

Australian Standard[®]

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

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



This Australian Standard® was prepared by Committee IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of the Council of Standards Australia on 10 March 2011.
This Standard was published on 28 March 2011.

The following are represented on Committee IT-006:

- Australia Safety Critical Systems Association
 - Australian Computer Society
 - Australian Petroleum Production and Exploration Association
 - Consult Australia
 - Consumers Federation of Australia
 - Engineers Australia
 - Institute of Chemical Engineers Australia
 - Institute of Instrumentation, Control and Automation Australia
 - Process Control Society
 - The University of Queensland
 - Workplace Health and Safety Queensland
 - WorkSafe Victoria
-

This Standard was issued in draft form for comment as DR AS 61508.2.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard[®]

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

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

Originated as AS 61508.2—2001.
Second edition 2011.

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9797 2

PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation, to supersede AS 61508.2—2001.

The objective of this revision is to adopt the current edition of IEC 61508-2.

This Standard is identical with, and has been reproduced from IEC 61508-2 Ed.2.0 (2010), *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*.

As this Standard is reproduced from an international standard, the following applies:

- (a) Its number appears on the cover and title page while the international standard number appears only on the cover.
- (b) In the source text ‘part of the IEC 61508 series’ should read ‘this Australian Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>		<i>Australian Standard</i>	
IEC		AS	
60947	Low-voltage switchgear and control gear	60947	Low-voltage switchgear and control gear
60947-5-1	Part 5-1: Control circuit devices and switching elements— Electromechanical control circuit devices	60947.5.1	Part 5.1: Control circuit devices and switching elements— Electromechanical control circuit devices
61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
61508-1	Part 1: General requirements	61508.1	Part 1: General requirements
61508-3	Part 3: Software requirements	61508.3	Part 3: Software requirements
61508-4	Part 4: Definitions and abbreviations	61508.4	Part 4: Definitions and abbreviations
61508-7	Part 7: Overview of techniques and measures	61508.7	Part 7: Overview of techniques and measures

Only international references that have been adopted as Australian Standards have been listed.

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the annex to which they apply. A ‘normative’ annex is an integral part of a Standard, whereas an ‘informative’ annex is only for information and guidance.

CONTENTS

	<i>Page</i>
1 Scope.....	9
2 Normative references	12
3 Definitions and abbreviations.....	12
4 Conformance to this standard	12
5 Documentation	13
6 Management of functional safety	13
7 E/E/PE system safety lifecycle requirements	13
7.1 General	13
7.1.1 Objectives and requirements – general.....	13
7.1.2 Objectives	13
7.1.3 Requirements	13
7.2 E/E/PE system design requirements specification	17
7.2.1 Objective	17
7.2.2 General	17
7.2.3 E/E/PE system design requirements specification.....	18
7.3 E/E/PE system safety validation planning	19
7.3.1 Objective	19
7.3.2 Requirements	19
7.4 E/E/PE system design and development.....	19
7.4.1 Objective	20
7.4.2 General requirements	20
7.4.3 Synthesis of elements to achieve the required systematic capability.....	22
7.4.4 Hardware safety integrity architectural constraints	23
7.4.5 Requirements for quantifying the effect of random hardware failures	32
7.4.6 Requirements for the avoidance of systematic faults	34
7.4.7 Requirements for the control of systematic faults.....	35
7.4.8 Requirements for system behaviour on detection of a fault	35
7.4.9 Requirements for E/E/PE system implementation	36
7.4.10 Requirements for proven in use elements	38
7.4.11 Additional requirements for data communications	39
7.5 E/E/PE system integration	40
7.5.1 Objective	40
7.5.2 Requirements	40
7.6 E/E/PE system operation and maintenance procedures	41
7.6.1 Objective	41
7.6.2 Requirements	41
7.7 E/E/PE system safety validation	42
7.7.1 Objective	42
7.7.2 Requirements	42
7.8 E/E/PE system modification.....	43
7.8.1 Objective	43
7.8.2 Requirements	43
7.9 E/E/PE system verification	44
7.9.1 Objective	44

7.9.2 Requirements	44
8 Functional safety assessment.....	46
Annex A (normative) Techniques and measures for E/E/PE safety-related systems – control of failures during operation.....	47
Annex B (normative) Techniques and measures for E/E/PE safety-related systems – avoidance of systematic failures during the different phases of the lifecycle	62
Annex C (normative) Diagnostic coverage and safe failure fraction	71
Annex D (normative) Safety manual for compliant items	74
Annex E (normative) Special architecture requirements for integrated circuits (ICs) with on-chip redundancy	76
Annex F (informative) Techniques and measures for ASICs – avoidance of systematic failures	81
Bibliography.....	89
 Figure 1 – Overall framework of the IEC 61508 series	11
Figure 2 – E/E/PE system safety lifecycle (in realisation phase).....	14
Figure 3 – ASIC development lifecycle (the V-Model).....	15
Figure 4 – Relationship between and scope of IEC 61508-2 and IEC 61508-3	15
Figure 5 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements, see 7.4.4.2.3)	28
Figure 6 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprised of two subsystems X & Y, see 7.4.4.2.4).....	30
Figure 7 – Architectures for data communication.....	40
 Table 1 – Overview – realisation phase of the E/E/PE system safety lifecycle.....	16
Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem	26
Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem	27
Table A.1 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction	49
Table A.2 – Electrical components	51
Table A.3 – Electronic components	51
Table A.4 – Processing units	52
Table A.5 – Invariable memory ranges	52
Table A.6 – Variable memory ranges	53
Table A.7 – I/O units and interface (external communication).....	53
Table A.8 – Data paths (internal communication)	54
Table A.9 – Power supply	54
Table A.10 – Program sequence (watch-dog).....	55
Table A.11 – Clock	55
Table A.12 – Communication and mass-storage	55
Table A.13 – Sensors	56
Table A.14 – Final elements (actuators).....	56
Table A.15 – Techniques and measures to control systematic failures caused by hardware design	58

Table A.16 – Techniques and measures to control systematic failures caused by environmental stress or influences	59
Table A.17 – Techniques and measures to control systematic operational failures	60
Table A.18 – Effectiveness of techniques and measures to control systematic failures	61
Table B.1 – Techniques and measures to avoid mistakes during specification of E/E/PE system design requirements (see 7.2)	63
Table B.2 – Techniques and measures to avoid introducing faults during E/E/PE system design and development (see 7.4)	64
Table B.3 – Techniques and measures to avoid faults during E/E/PE system integration (see 7.5).....	65
Table B.4 – Techniques and measures to avoid faults and failures during E/E/PE system operation and maintenance procedures (see 7.6).....	66
Table B.5 – Techniques and measures to avoid faults during E/E/PE system safety validation (see 7.7)	67
Table B.6 – Effectiveness of techniques and measures to avoid systematic failures.....	68
Table E.1 – Techniques and measures that increase β_{B-IC}	79
Table E.2 – Techniques and measures that decrease β_{B-IC}	80
Table F.1 – Techniques and measures to avoid introducing faults during ASIC's design and development – full and semi-custom digital ASICs (see 7.4.6.7).....	83
Table F.2 – Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD) (see 7.4.6.7)	86

INTRODUCTION

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

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of product and application sector international standards based on the IEC 61508 series.

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

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

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

This International Standard

- considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE systems are used to perform safety functions;
- has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
- enables product and application sector international standards, dealing with E/E/PE safety-related systems, to be developed; the development of product and application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
- provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
- adopts a risk-based approach by which the safety integrity requirements can be determined;
- introduces safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

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

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;
- a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5} ;
- a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h⁻¹];

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

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

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;
- introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe. However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

AUSTRALIAN 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 the IEC 61508 series

- 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, that contains at least one electrical, electronic or programmable electronic element;
- c) applies to all elements within an E/E/PE safety-related system (including sensors, actuators and the operator interface);
- d) specifies how to refine the E/E/PE system safety requirements specification, developed in accordance with IEC 61508-1 (comprising the E/E/PE system safety functions requirements specification and the E/E/PE system safety integrity requirements specification), into the E/E/PE system design requirements specification;
- e) specifies the 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/PE system safety lifecycle model) except software, which is dealt with in IEC 61508-3 (see Figures 2 to 4). These requirements include the application of techniques and measures that 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 4.

- i) does not apply for medical equipment in compliance with the IEC 60601 series.

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 3.4.3 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone standards. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

1.3 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 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.

1.4 Figure 1 shows the overall framework of the IEC 61508 series 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.

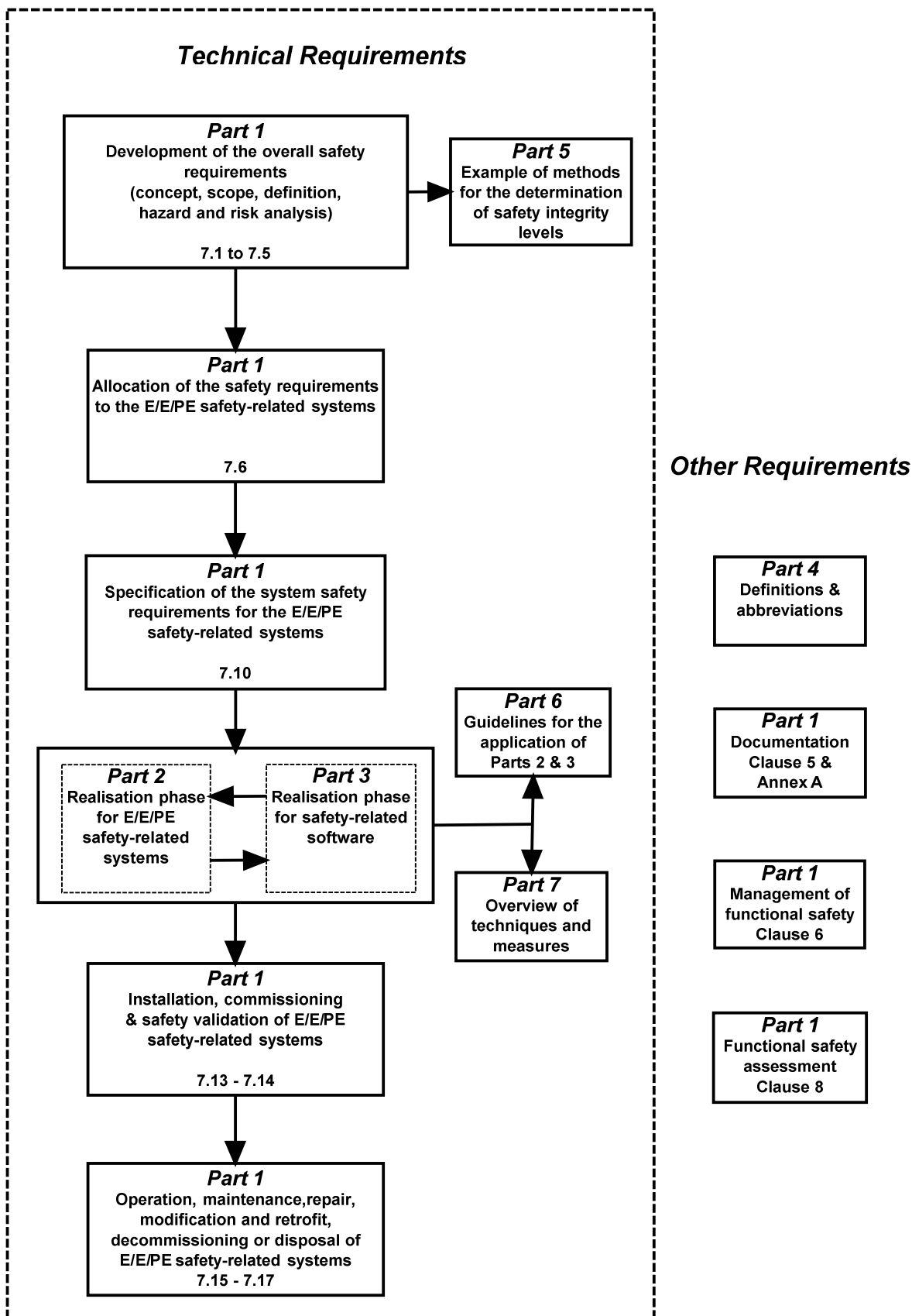


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

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

IEC 60947-5-1, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

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

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

IEC 61508-4: 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

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

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

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

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

EN 50205, *Relays with forcibly guided (mechanically linked) contacts*

3 Definitions and abbreviations

For the purposes of this document, 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/PE system 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/PE system 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/PE system 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/PE system 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/PE system safety lifecycle.

7.1.3 Requirements

7.1.3.1 The E/E/PE system safety lifecycle that shall be used in claiming conformance with this standard is that specified in Figure 2. A detailed V-model of the ASIC development lifecycle for the design of ASICs (see IEC 61508-4, 3.2.15) is shown in Figure 3. If another E/E/PE system safety lifecycle or ASIC development lifecycle is used, it shall be specified as part of the management of functional safety activities (see Clause 6 of IEC 61508-1), and all the objectives and requirements of each subclause of IEC 61508-2 shall be met.

NOTE 1 The relationship between and scope for IEC 61508-2 and IEC 61508-3 are shown in Figure 4.

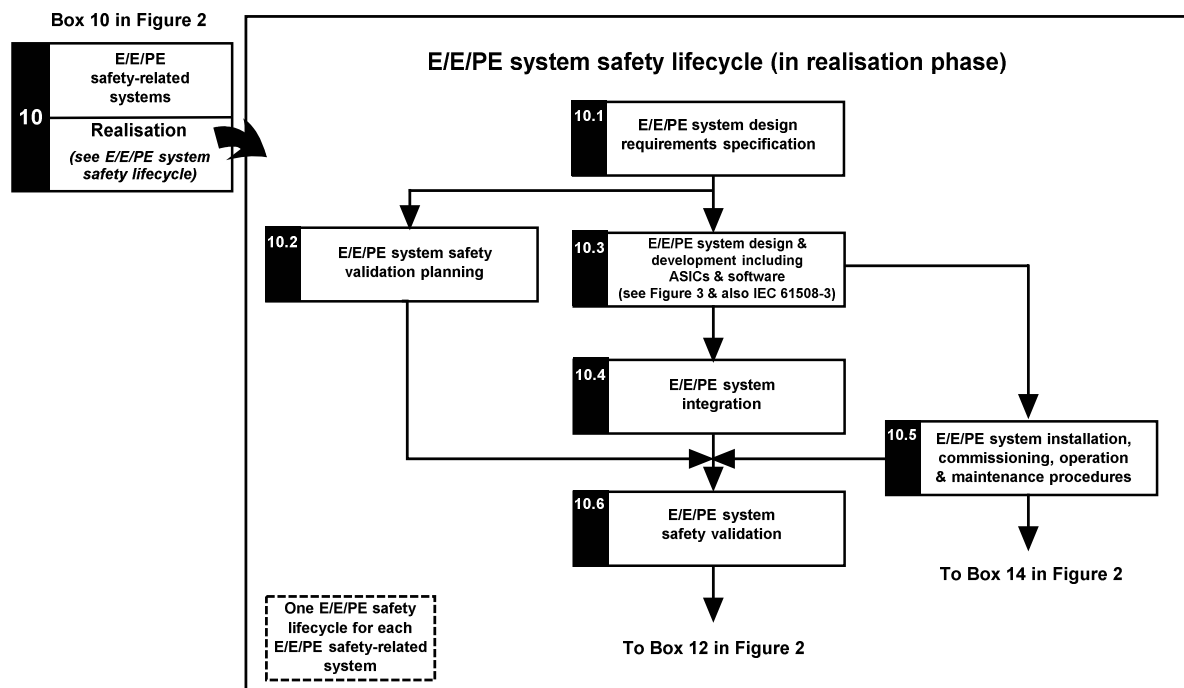
NOTE 2 There are significant similarities between the ASIC and the software design processes. IEC 61508-3 recommends the V-model for designing safety-related software. The V-model requires a clearly structured design process and a modular software structure for avoiding and controlling systematic faults. The ASIC development lifecycle for the design of ASICs in Figure 3 follows this model. At first the requirements for the ASIC specification are derived from the system requirements. ASIC architecture, ASIC design and module design follow. The results of each step on the left-hand side of the V become the input to the next step, and are also fed back to the preceding step for iteration where appropriate, until the final code is created. This code is verified against the corresponding design through post-layout simulation, module testing, module integration testing and verification of the complete ASIC. The results of any step may necessitate a revision to any of the preceding steps. Finally, the ASIC is validated after its integration into the E/E/PE safety-related system.

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/PE system safety lifecycle phases.

7.1.3.3 Each phase of the E/E/PE system 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 as part of the management of functional safety activities (see Clause 6 of IEC 61508-1), the outputs of each phase of the E/E/PE system safety lifecycle shall be documented (see Clause 5 of IEC 61508-1).

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



NOTE 1 See also IEC 61508-6, A.2 b).

NOTE 2 This figure shows only those phases of the E/E/PE system safety lifecycle that are within the realisation phase of the overall safety lifecycle. The complete E/E/PE system safety lifecycle will also contain instances, specific to the E/E/PE safety-related system, of the subsequent phases of the overall safety lifecycle (Boxes 12 to 16 in Figure 2 of IEC 61508-1).

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

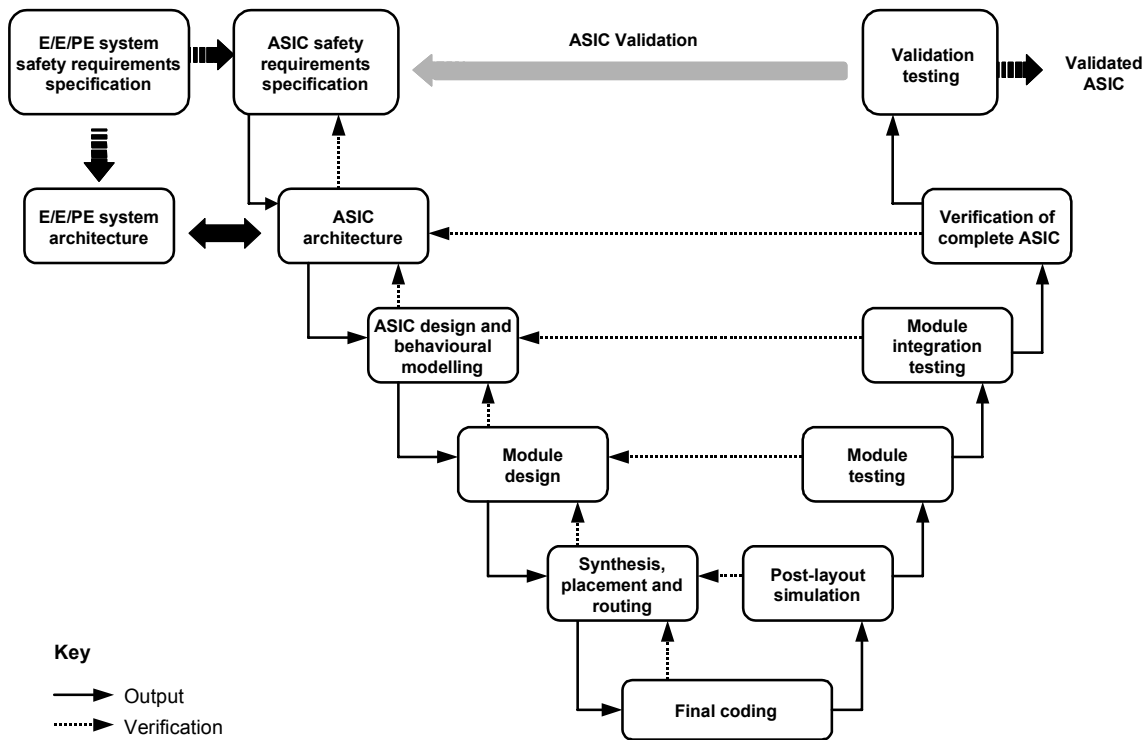


Figure 3 – ASIC development lifecycle (the V-Model)

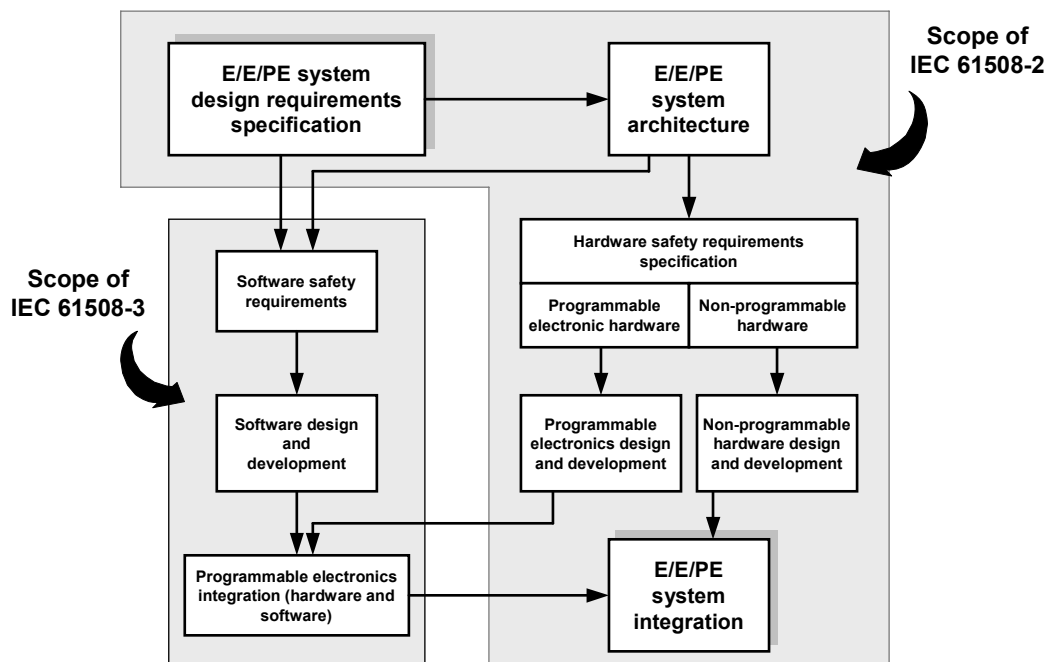


Figure 4 – Relationship between and scope of IEC 61508-2 and IEC 61508-3

Table 1 – Overview – realisation phase of the E/E/PE system safety lifecycle

Safety lifecycle phase or activity		Objectives	Scope	Requirements sub-clause	Inputs	Outputs
Figure 2 box number	Title					
10.1	E/E/PE system design requirements specification	To specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements (see 7.10.2 of IEC 61508-1)	E/E/PE safety-related system	7.2.2	E/E/PE system safety requirements specification (see IEC 61508-1, 7.10)	E/E/PE system design requirements specification, describing the equipment and architectures for the E/E/PE system
10.2	E/E/PE system safety validation planning	To plan the validation of the safety of the E/E/PE safety-related system	E/E/PE safety-related system	7.3.2	E/E/PE system safety requirements specification and E/E/PE system design requirements specification	Plan for the safety validation of the E/E/PE safety-related systems
10.3	E/E/PE system design & development including ASICs & software (see Figure 3 & also IEC 61508-3)	To design and develop the E/E/PE safety-related system (including ASICs if appropriate) to meet the E/E/PE system design requirements specification (with respect to the safety functions requirements and the safety integrity requirements (see 7.2))	E/E/PE safety-related system	7.4.2 to 7.4.11	E/E/PE system design requirements specification	Design of the E/E/PE safety related systems in conformance with the E/E/PE system design requirements specification Plan for the E/E/PE system integration test PE system architectural information as an input to the software requirements specification
10.4	E/E/PE system integration	To integrate and test the E/E/PE safety-related system	E/E/PE safety-related system	7.5.2	E/E/PE system design E/E/PE system integration test plan Programmable electronics hardware and software	Fully functioning E/E/PE safety-related systems in conformance with the E/E/PE system design Results of E/E/PE system integration tests
10.5	E/E/PE system installation, commissioning, operation and maintenance procedures	To develop procedures to ensure that the required functional safety of the E/E/PE safety-related system is maintained during operation and maintenance	E/E/PE safety-related system EUC	7.6.2	E/E/PE system design requirements specification E/E/PE system design	E/E/PE system installation, commissioning, operation and maintenance procedures for each individual E/E/PE system
10.6	E/E/PE system safety validation	To validate that the E/E/PE safety-related system meets, in all respects, the requirements for safety in terms of the required safety functions and safety integrity	E/E/PE safety-related system	7.7.2	E/E/PE system safety requirements specification and E/E/PE system design requirements specification 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/PE system safety validation

Table 1 (continued)

Safety lifecycle phase or activity		Objectives	Scope	Requirements sub-clause	Inputs	Outputs
Figure 2 box number	Title					
–	E/E/PE system modification	To make corrections, enhancements or adaptations to the E/E/PE safety-related system, ensuring that the required safety integrity is achieved and maintained	E/E/PE safety-related system	7.8.2	E/E/PE system design requirements specification	Results of E/E/PE system modification
–	E/E/PE system 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 system	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/PE system functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related system	E/E/PE safety-related system	8	Plan for E/E/PE system functional safety assessment	Results of E/E/PE system functional safety assessment

7.2 E/E/PE system design requirements specification

NOTE This phase is Box 10.1 of Figure 2.

7.2.1 Objective

The objective of the requirements of this subclause is to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

NOTE The E/E/PE system design requirements specification is normally derived from the E/E/PE system safety requirements specification by decomposing the safety functions and allocating parts of the safety function to subsystems (for example groups of sensors, logic solvers or actuators). The requirements for the subsystems may be included in the E/E/PE system design requirements specification or may be separate and referenced from the E/E/PE system design requirements specification. Subsystems may be further decomposed into elements and architectures to satisfy the design and development requirements of 7.4. The requirements for these elements may be included in the requirements for the subsystems or may be separate and referenced from the subsystem requirements.

7.2.2 General

7.2.2.1 The specification of the E/E/PE system design requirements shall be derived from the E/E/PE system safety requirements, specified in 7.10 of IEC 61508-1.

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). See also 7.4.2.3.

7.2.2.2 The specification of the E/E/PE system design requirements shall be expressed and structured in such a way that they are:

- clear, precise, unambiguous, verifiable, testable, maintainable and feasible;
- written to aid comprehension by those who are likely to utilise the information at any phase of the E/E/PE safety lifecycle; and
- traceable to the E/E/PE system safety requirements specification.

7.2.3 E/E/PE system design requirements specification

7.2.3.1 The specification of the E/E/PE system design requirements shall contain design requirements relating to safety functions (see 7.2.3.2) and design requirements relating to safety integrity (see 7.2.3.3).

7.2.3.2 The specification of the E/E/PE system design requirements shall contain details of all the hardware and software necessary to implement the required safety functions, as specified by the E/E/PE system safety functions requirements specification (see 7.10.2.6 of IEC 61508-1). The specification shall include, for each safety function:

- a) requirements for the subsystems and requirements for their hardware and software elements as appropriate;
- b) requirements for the integration of the subsystems and their hardware and software elements to meet the E/E/PE system safety functions requirements specification;
- c) throughput performance that enables response time requirements to be met;
- d) accuracy and stability requirements for measurements and controls;
- e) E/E/PE safety-related system and operator interfaces;
- f) interfaces between the E/E/PE safety-related systems and any other systems (either within, or outside, the EUC);
- g) all 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) of the E/E/PE safety-related systems;
- h) the significance of all hardware/software interactions and, where relevant, any required constraints between the hardware and the software;

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

- i) any limiting and constraint conditions for the E/E/PE safety-related systems and their associated elements, for example timing constraints or constraints due to the possibility of common cause failures;
- j) any specific requirements related to the procedures for starting-up and restarting the E/E/PE safety-related systems.

7.2.3.3 The specification of the E/E/PE system design requirements shall contain details, relevant to the design, to achieve the safety integrity level and the required target failure measure for the safety function, as specified by the E/E/PE system safety integrity requirements specification (see 7.10.2.7 of IEC 61508-1), including:

- a) the architecture of each subsystem required to meet the architectural constraints on the hardware safety integrity (see 7.4.4);
- b) all relevant reliability modelling parameters such as the required proof testing frequency of all hardware elements necessary to achieve the target failure measure;

NOTE 1 Information on the specific application cannot be understated (see 7.10.2.1 of IEC 61508-1). 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.

- c) the actions taken in the event of a dangerous failure being detected by diagnostics;
- d) the requirements, constraints, functions and facilities to enable the proof testing of the E/E/PE hardware to be undertaken;
- e) the capabilities of equipment used to meet the extremes of all environmental conditions (e.g. temperature, humidity, mechanical, electrical) that are specified as required during the E/E/PE system safety lifecycle including manufacture, storage, transport, testing, installation, commissioning, operation and maintenance;
- f) the electromagnetic immunity levels that are required (see IEC/TS 61000-1-2: 2008);

NOTE 2 The required immunity levels may vary for different elements of the safety-related system, depending on physical location and power supply arrangements.

NOTE 3 Guidance may be found in EMC product standards, but it is important to recognise that higher immunity levels, or additional immunity requirements, than those specified in such standards may be necessary for particular locations or when the equipment is intended for use in harsher, or different, electromagnetic environments.

g) the quality assurance/quality control measures necessary to safety management (see 6.2.5 of IEC 61508-1);

7.2.3.4 The E/E/PE system design requirements specification shall be completed in detail as the design progresses and updated as necessary after modification.

7.2.3.5 For the avoidance of mistakes during the development of the specification for the E/E/PE system design requirements, an appropriate group of techniques and measures according to Table B.1 shall be used.

7.2.3.6 The implications imposed on the architecture by the E/E/PE system design requirements shall be considered.

NOTE This should include the consideration of the simplicity of the implementation to achieve the required safety integrity level (including architectural considerations and apportionment of functionality to configuration data or to the embedded system).

7.3 E/E/PE system safety validation planning

NOTE This phase is Box 10.2 of Figure 2. It will normally be carried out in parallel with E/E/PE system 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 system.

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 system satisfies the E/E/PE system safety requirements specification (see 7.10 of IEC 61508-1) and the E/E/PE system design requirements specification (see 7.2).

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

- a) all of the requirements defined in the E/E/PE system safety requirements specification and the E/E/PE system design 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 electromagnetic immunity tests for elements of safety-related systems is given in IEC/TS 61000-1-2.

g) policies for resolving validation failure.

7.4 E/E/PE system design and development

NOTE This phase is Box 10.3 of Figure 2. It will normally be carried out in parallel with E/E/PE system safety validation planning (see 7.3).

7.4.1 Objective

The objective of the requirements of this subclause is to design and develop the E/E/PE safety-related system (including ASICs if appropriate, see IEC 61508-4, 3.2.15) to meet the E/E/PE system design requirements specification (with respect to the safety functions requirements and the 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/PE system design requirements specification (see 7.2.3), taking into account all the requirements of 7.2.3.

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, ASICs, embedded software, application software, data etc.), shall meet all of the requirements a) to e) as follows:

- a) the requirements for hardware safety integrity comprising;
 - the architectural constraints on hardware safety integrity (see 7.4.4), and
 - the requirements for quantifying the effect of random failures (see 7.4.5);
- b) the special architecture requirements for ICs with on-chip redundancy (see Annex E), where relevant, unless justification can be given that the same level of independence between different channels is achieved by applying a different set of measures;
- c) the requirements for systematic safety integrity (systematic capability), which can be met by achieving one of the following compliance routes:
 - Route 1_S: compliance with the requirements for the avoidance of systematic faults (see 7.4.6 and IEC 61508-3) and the requirements for the control of systematic faults (see 7.4.7 and IEC 61508-3), or
 - Route 2_S: compliance with the requirements for evidence that the equipment is proven in use (see 7.4.10), or
 - Route 3_S (pre-existing software elements only): compliance with the requirements of IEC 61508-3, 7.4.2.12;

NOTE The “S” subscript in the above routes designates systematic safety integrity to distinguish it from Route 1_H, and Route 2_H for hardware safety integrity.
- d) the requirements for system behaviour on detection of a fault (see 7.4.8);
- e) the requirements for data communication processes (see 7.4.11).

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).

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/PE system 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.

EXAMPLE Addressing foreseeable failure modes, that may undermine independence, and their failure rates, use of FMECA or dependant failure analysis.

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 system 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 system 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 that 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 system 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 7.5.2).

NOTE 1 A subsystem may be considered to comprise a single element or any group of elements. See IEC 61508-4 for definitions. 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 7.4.9.3 and 7.4.9.4).

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 or element functionality, capacity and performance on to the new requirement or the verified subsystem or element 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 or element is overly complicated or has unused features and if protection against unintended functions cannot be obtained.

7.4.2.12 When the initial design of the E/E/PE safety-related system has been completed, an analysis shall be undertaken to determine whether any reasonably foreseeable failure of the E/E/PE safety-related system could cause a hazardous situation or place a demand on

other risk control measure. If any reasonably foreseeable failure could have either of these effects, then the first priority shall be to change the design of the E/E/PE safety-related system to avoid such failure modes. If this cannot be done, then measures shall be taken to reduce the likelihood of such failure modes to a level commensurate with the target failure measure. These measures shall be subject to the requirements of this standard.

NOTE The intention of this clause is to identify failure modes of the E/E/PE safety-related system that place a demand on other risk control measures. There may be cases where the failure rate of the specified failure modes cannot be reduced and either a new safety function will be required or the SIL of the other safety functions reconsidered taking into account the failure rate.

7.4.2.13 De-rating (see IEC 61508-7) should be considered for all hardware components. Justification for operating any hardware elements at their limits shall be documented (see IEC 61508-1, Clause 5).

NOTE Where de-rating is appropriate, a de-rating factor of approximately two-thirds is typical.

7.4.2.14 Where the design of an E/E/PE safety-related system includes one or more ASICs to implement a safety function, an ASIC development lifecycle (see 7.1.3.1) shall be used.

7.4.3 Synthesis of elements to achieve the required systematic capability

7.4.3.1 To meet the requirements for systematic safety integrity, the designated safety-related E/E/PE system may, in the circumstances described in this section, be partitioned into elements of different systematic capability.

NOTE 1 The systematic capability of an element determines the potential for systematic faults of that element to lead to a failure of the safety function. The concept of systematic capability of an element is applicable to both hardware and software elements.

NOTE 2 Subclause 7.6.2.7 of IEC 61508-1 recognises the value of independence and diversity at the level of a safety function and the E/E/PE safety related systems to which it could be allocated. These concepts can also be applied at the detailed design level where an assembly of elements implementing a safety function can potentially achieve a better systematic performance than the individual elements.

7.4.3.2 For an element of systematic capability SC N ($N=1, 2, 3$), where a systematic fault of that element does not cause a failure of the specified safety function but does so only in combination with a second systematic fault of another element of systematic capability SC N, the systematic capability of the combination of the two elements can be treated as having a systematic capability of SC ($N + 1$) providing that sufficient independence exists between the two elements (see 7.4.3.4).

NOTE The independence of elements can be assessed only when the specific application of the elements is known in relation to the defined safety functions.

7.4.3.3 The systematic capability that can be claimed for a combination of elements each of systematic capability SC N can at most be SC ($N+1$). A SC N element may be used in this way only once. It is not permitted to achieve SC ($N+2$) and higher by successively building assemblies of SC N elements.

7.4.3.4 Sufficient independence, in the design between elements and in the application of elements, shall be justified by common cause failure analysis to show that the likelihood of interference between elements and between the elements and the environment is sufficiently low in comparison with the safety integrity level of the safety function under consideration.

NOTE 1 For systematic capability, with respect to hardware design, realisation, operation and maintenance, possible approaches to the achievement of sufficient independence include:

- functional diversity: use of different approaches to achieve the same results;
- diverse technologies: use of different types of equipment to achieve the same results);
- common parts/services: ensuring that there are no common parts or services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;
- common procedures: ensuring that there are no common operational, maintenance or test procedures.

NOTE 2 Independence of application means that elements will not adversely interfere with each other's execution behaviour such that a dangerous failure would occur.

NOTE 3 For independence of software elements see 7.4.2.8 and 7.4.2.9 of IEC 61508-3.

7.4.4 Hardware safety integrity architectural constraints

NOTE 1 The equation, relating to the hardware safety integrity constraints, are specified in Annex C and the safety integrity constraints are summarized in Table 2 and Table 3

NOTE 2 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.

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 safety integrity constraints which shall be achieved by implementing one of two possible routes (to be implemented at system or subsystem level):

- Route 1_H based on hardware fault tolerance and safe failure fraction concepts; or,
- Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

Application standards based on the IEC 61508 series may indicate the preferred Route (i.e. Route 1_H or Route 2_H).

NOTE 3 The "H" subscript in the above routes designates hardware safety integrity to distinguish it from Route 1_S, Route 2_S and Route 3_S for systematic safety integrity.

7.4.4.1 General requirements

7.4.4.1.1 With respect to the hardware fault tolerance requirements

- a) a hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function (for further clarification see Note 1 and Table 2 and Table 3). 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) when determining the hardware fault tolerance achieved, 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 2).

NOTE 1 The constraints on hardware safety integrity have been included in order to achieve a sufficiently robust architecture, taking into account the level of element and subsystem complexity (see 7.4.4.1.1 and 7.4.4.1.2). The highest allowable safety integrity level for the safety function implemented by the E/E/PE safety-related system, derived through applying these requirements, is the maximum that is permitted to be claimed for the safety function even though, in some cases reliability calculations show that a higher safety integrity level could be achieved. It should also be noted that even if the hardware fault tolerance is achieved for all subsystems, a reliability calculation will still be necessary to demonstrate that the specified target failure measure has been achieved and this may require that the hardware fault tolerance be increased to meet design requirements.

NOTE 2 The hardware fault tolerance requirements apply to the subsystem architecture that is used under normal operating conditions. The hardware 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 should have been previously evaluated (for example MTTR compared to the probability of a demand).

NOTE 3 Certain faults may be excluded because if an element 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 that uses the element.

NOTE 4 The choice of the route is application and sector dependent and the following should be considered when selecting the Route:

- a safe failure of one function may create a new hazard or be an additional cause for an existing hazard;
- redundancy may not be practicable for all functions;

- repair is not always possible or rapid (e.g. not feasible within a time that is negligible compared to the proof test interval).

NOTE 5 Special architecture requirements for ICs with on-chip redundancy are given in Annex E.

7.4.4.1.2 An element 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 element under fault conditions can be completely determined; and
- c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.9.3 to 7.4.9.5).

7.4.4.1.3 An element 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 element under fault conditions cannot be completely determined; or
- c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.9.3 to 7.4.9.5).

NOTE This means that if at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.

7.4.4.1.4 When estimating the safe failure fraction of an element, intended to be used in a subsystem having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if:

- the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or,
- when operating in high demand mode of operation, the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.

7.4.4.1.5 When estimating the safe failure fraction of an element which,

- has a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation; or,
- is implementing a safety function, or part of a safety function, operating in low demand mode of operation,

credit shall only be taken for the diagnostics if the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

7.4.4.2 Route 1_H

7.4.4.2.1 To determine the maximum safety integrity level that can be claimed, with respect to a specified safety function, the following procedure shall be followed:

- 1) Define the subsystems making up the E/E/PE safety-related system.
- 2) For each subsystem determine the safe failure fraction for all elements in the subsystem separately (i.e. on an individual element basis with each element having a hardware fault tolerance of 0). In the case of redundant element configurations, the SFF may be calculated by taking into consideration the additional diagnostics that may be available (e.g. by comparison of redundant elements).
- 3) For each element, use the achieved safe failure fraction and hardware fault tolerance of 0 to determine the maximum safety integrity level that can be claimed from column 2 of Table 2 (for Type A elements) and column 2 of Table 3 (for Type B elements).

- 4) Use the method in 7.4.4.2.3 and 7.4.4.2.4 for determining the maximum safety integrity level that can be claimed for the subsystem.
- 5) The maximum safety integrity level that can be claimed for an E/E/PE safety-related system shall be determined by the subsystem that has achieved the lowest safety integrity level.

7.4.4.2.2 For application to subsystems comprising elements that meet the specific requirements detailed below, as an alternative to applying the requirements of 7.4.4.2.1 2) to 7.4.4.2.1 4), the following is applicable:

- 1) the subsystem is comprised of more than one element; and
- 2) the elements are of the same type; and
- 3) all the elements have achieved safe failure fractions that are in the same range (see Note 1 below) specified in Tables 2 or 3; then the following procedure may be followed,
 - a) determine the safe failure fraction of all individual elements. In the case of redundant element configurations, the SFF may be calculated by taking into consideration the additional diagnostics that may be available (e.g. by comparison of redundant elements);
 - b) determine the hardware fault tolerance of the subsystem;
 - c) determine the maximum safety integrity level that can be claimed for the subsystem if the elements are type A from Table 2;
 - d) determine the maximum safety integrity level that can be claimed for the subsystem if the elements are type B from Table 3.

NOTE 1 The range indicated in 3) above refers to Tables 2 and 3 where the safe failure fraction is classified into one of four ranges (i.e. (<60 %); (60 % to <90 %); (90% to <99 %) and (≥ 99 %)). All SFFs would need to be in the same range (e.g. all in the range (90 % to <99 %)).

EXAMPLE 1 To determine the maximum allowable safety integrity level that has been achieved, for the specified safety function, by a subsystem having a hardware fault tolerance of 1, where an element safety function is implemented through parallel elements, the following approach may be adopted providing the subsystem meets the requirements of 7.4.4.2.2. In this example, all the elements are type B and the safe failure fractions of the elements are in the (90 % to < 99 %) range.

From Table 3, it can be seen by inspection, that for a hardware fault tolerance equal to 1, with safe failure fractions of both elements in the (90 % to <99 %) range, the maximum allowable safety integrity level for the specified safety function is SIL 3.

EXAMPLE 2 To determine the required hardware fault tolerance for a subsystem, for the specified safety function, where an element safety function is implemented through parallel elements, the following approach may be adopted providing the subsystem meets the requirements of 7.4.4.2.2. In this example, all the elements are type A and the safe failure fractions of the elements are in the (60 % to <90 % range). The safety integrity level of the safety function is SIL 3.

From Table 2, it can be seen by inspection, that to meet the requirement of SIL 3, the required hardware fault tolerance needs to equal 1. This means that two elements in parallel are necessary.

Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 This table, in association with 7.4.4.2.1 and 7.4.4.2.2, is used for the determination of the maximum SIL that can be claimed for a subsystem: given the fault tolerance of the subsystem and the SFF to the elements used.

- For general application to any subsystem see 7.4.4.2.1.
- For application to subsystems comprising elements that meet the specific requirements of 7.4.4.2.2. To claim that a subsystem meets a specified SIL directly from this table it will be necessary to meet all the requirements in 7.4.4.2.2.

NOTE 2 The table, in association with 7.4.4.2.1 and 7.4.4.2.2, can also be used:

- For the determination of the hardware fault tolerance requirements for a subsystem given the required SIL of the safety function and the SFFs of the elements to be used.
- For the determination of the SFF requirements for elements given the required SIL of the safety function and the hardware fault tolerance of the subsystem.

NOTE 3 The requirements in 7.4.4.2.3 and 7.4.4.2.4 are based on the data specified in this table and Table 3.

NOTE 4 See Annex C for details of how to calculate safe failure fraction.

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 This table, in association with 7.4.4.2.1 and 7.4.4.2.2, is used for the determination of the maximum SIL that can be claimed for a subsystem given the fault tolerance of the subsystem and the SFF to the elements used.

- For general application to any subsystem see 7.4.4.2.1.
- For application to subsystems comprising elements that meet the specific requirements of 7.4.4.2.2. To claim that a subsystem meets a specified SIL directly from this table it will be necessary to meet all the requirements in 7.4.4.2.2.

NOTE 2 The table, in association with 7.4.4.2.1 and 7.4.4.2.2, can also be used:

- For the determination of the hardware fault tolerance requirements for a subsystem given the required SIL of the safety function and the SFFs of the elements to be used.
- For the determination of the SFF requirements for elements given the required SIL of the safety function and the hardware fault tolerance of the subsystem.

NOTE 3 The requirements in 7.4.4.2.3 and 7.4.4.2.4 are based on the data specified in this table and Table 2.

NOTE 4 See Annex C for details of how to calculate safe failure fraction.

NOTE 5 When using 7.4.4.2.1 for the combination of type B elements, with a hardware fault tolerance of 1, in which both elements have a safe failure fraction of less than 60 %, the maximum allowable safety integrity level for a safety function carried out by the combination is SIL 1.

7.4.4.2.3 In an E/E/PE safety-related subsystem where a number of element safety functions are implemented through a serial combination of elements (such as in Figure 5), the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by the element that has achieved the lowest safety integrity level for the achieved safe failure fraction for a hardware fault tolerance of 0. To illustrate the method, assume an architecture as indicated in Figure 5 and see example below.

EXAMPLE (see Figure 5): Assume an architecture where a number of element safety functions are performed by a subsystem comprising a single channel of elements 1, 2 and 3 and the elements meet the requirements of Tables 2 and 3 as follows:

- Element 1 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1;
- Element 2 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;
- Element 3 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1;
- Both element 1 and element 3 restrict the maximum SIL that can be claimed, for the achieved hardware fault tolerance and safe failure fraction to just SIL 1.

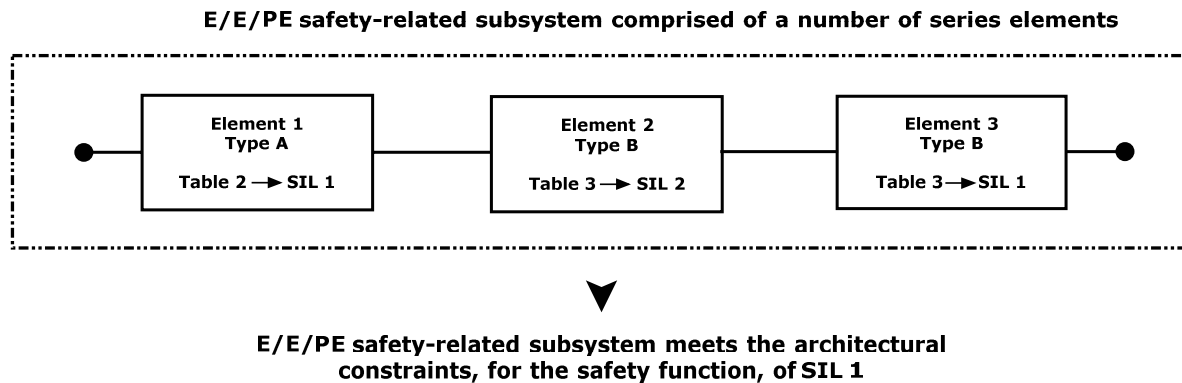


Figure 5 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements, see 7.4.4.2.3)

7.4.4.2.4 In an E/E/PE safety-related subsystem where an element safety function is implemented through a number of channels (combination of parallel elements) having a hardware fault tolerance of N, the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by:

- a) grouping the serial combination of elements for each channel and then determining the maximum safety integrity level that can be claimed for the safety function under consideration for each channel (see 7.4.4.2.3); and
- b) selecting the channel with the highest safety integrity level that has been achieved for the safety function under consideration and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of the subsystem.

To illustrate the method, assume architecture as indicated in Figure 6 and see example below.

NOTE 1 N is the hardware fault tolerance of the combination of parallel elements (see 7.4.4.1.1).

NOTE 2 See example below regarding the application of this subclause.

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 two subsystems, X and Y, where subsystem X consists of elements 1, 2, 3 and 4, and subsystem Y consists of a single element 5, as shown in Figure 6. The use of parallel channels in subsystem X ensures that elements 1 and 2 implement the part of the safety function required of subsystem X independently from elements 3 and 4, and vice-versa. The safety function will be performed:

- in the event of a fault in either element 1 or element 2 (because the combination of elements 3 and 4 is able to perform the required part of the safety function); or
- in the event of a fault in either element 3 or element 4 (because the combination of elements 1 and 2 is able to perform the required part of the safety function).

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

For subsystem X, in respect of the specified safety function under consideration, each element meets the requirements of Tables 2 and 3 as follows:

- Element 1 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 3;
- Element 2 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;
- Element 3 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;
- Element 4 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1.

Elements are combined to give a maximum hardware safety integrity level for the safety function under consideration, for subsystem X as follows: