

Australian Standard[®]

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

Part 1: General requirements



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 61508.1.

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Standards may also be withdrawn.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 1: General requirements

Originated as AS 61508.1—1999.
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 9796 5

PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation, to supersede AS 61508.1—1999.

The objective of this revision is to adopt the current edition of IEC 61508-1.

This Standard is identical with, and has been reproduced from IEC 61508-1 Ed.2.0 (2010), *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1: General requirements*.

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 ‘this International Standard’ 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	
61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
61508-2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	61508.2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
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
Guide 104	The preparation of safety publications and the use of basic safety publications and group safety publications	—	
ISO/IEC			
Guide 51	Guidelines for their inclusion in standards	—	

The term ‘informative’ has been used in this Standard to define the application of the annex to which it applies. An ‘informative’ annex is for information only.

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
5.1 Objectives	13
5.2 Requirements	13
6 Management of functional safety.....	14
6.1 Objectives	14
6.2 Requirements	14
7 Overall safety lifecycle requirements	17
7.1 General	17
7.1.1 Introduction	17
7.1.2 Objectives and requirements – general	20
7.1.3 Objectives	25
7.1.4 Requirements	25
7.2 Concept.....	25
7.2.1 Objective	25
7.2.2 Requirements	26
7.3 Overall scope definition	26
7.3.1 Objectives	26
7.3.2 Requirements	26
7.4 Hazard and risk analysis	27
7.4.1 Objectives	27
7.4.2 Requirements	27
7.5 Overall safety requirements	28
7.5.1 Objective	29
7.5.2 Requirements	29
7.6 Overall safety requirements allocation.....	30
7.6.1 Objectives	30
7.6.2 Requirements	31
7.7 Overall operation and maintenance planning	35
7.7.1 Objective	35
7.7.2 Requirements	35
7.8 Overall safety validation planning.....	37
7.8.1 Objective	37
7.8.2 Requirements	37
7.9 Overall installation and commissioning planning.....	38
7.9.1 Objectives	38
7.9.2 Requirements	38
7.10 E/E/PE system safety requirements specification	38
7.10.1 Objective	39
7.10.2 Requirements	39
7.11 E/E/PE safety-related systems – realisation	41

7.11.1	Objective	41
7.11.2	Requirements	41
7.12	Other risk reduction measures – specification and realisation.....	41
7.12.1	Objective	41
7.12.2	Requirements	41
7.13	Overall installation and commissioning.....	41
7.13.1	Objectives	41
7.13.2	Requirements	42
7.14	Overall safety validation.....	42
7.14.1	Objective	42
7.14.2	Requirements	42
7.15	Overall operation, maintenance and repair	43
7.15.1	Objective	43
7.15.2	Requirements	43
7.16	Overall modification and retrofit	46
7.16.1	Objective	46
7.16.2	Requirements	47
7.17	Decommissioning or disposal.....	48
7.17.1	Objective	48
7.17.2	Requirements	48
7.18	Verification	49
7.18.1	Objective	49
7.18.2	Requirements	49
8	Functional safety assessment	50
8.1	Objective	50
8.2	Requirements	50
Annex A (informative)	Example of a documentation structure.....	54
Bibliography		60
Figure 1	– Overall framework of the IEC 61508 series	11
Figure 2	– Overall safety lifecycle	18
Figure 3	– E/E/PE system safety lifecycle (in realisation phase)	19
Figure 4	– Software safety lifecycle (in realisation phase)	19
Figure 5	– Relationship of overall safety lifecycle to the E/E/PE system and software safety lifecycles.....	20
Figure 6	– Allocation of overall safety requirements to E/E/PE safety-related systems and other risk reduction measures.....	32
Figure 7	– Example of operations and maintenance activities model	45
Figure 8	– Example of operation and maintenance management model	46
Figure 9	– Example of modification procedure model.....	48
Figure A.1	– Structuring information into document sets for user groups	59
Table 1	– Overall safety lifecycle – overview.....	21
Table 2	– Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation	33
Table 3	– Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation	34

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 2))	53
Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 9 and 10, including all phases of E/E/PE system and software safety lifecycles (see Figures 2, 3 and 4))	53
Table A.1 – Example of a documentation structure for information related to the overall safety lifecycle	56
Table A.2 – Example of a documentation structure for information related to the E/E/PE system safety lifecycle.....	57
Table A.3 – Example of a documentation structure for information related to the software safety lifecycle	58

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;
- sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in
 - a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5} ;
 - a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h⁻¹];

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

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

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

AUSTRALIAN STANDARD

Functional safety of electrical/electronic/programmable electronic safety-related systems**Part 1:****General requirements****1 Scope**

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

1.2 In particular, this standard

- a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic elements;

NOTE 1 In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this standard may be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.3 of IEC 61508-4).

NOTE 2 Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4), human factor requirements related to the design of E/E/PE safety-related systems are not considered in detail in this standard.

- b) is generically-based and applicable to all E/E/PE safety-related systems irrespective of the application;
- c) covers the achievement of a tolerable risk through the application of E/E/PE safety-related systems, but does not cover hazards arising from the E/E/PE equipment itself (for example electric shock);
- d) applies to all types of E/E/PE safety-related systems, including protection systems and control systems;
- e) does not cover E/E/PE systems where
 - a single E/E/PE system is capable on its own of meeting the tolerable risk, and
 - the required safety integrity of the safety functions of the single E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).
- f) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE 3 See 3.1.1 of IEC 61508-4.

- g) considers E/E/PE safety-related systems and other risk reduction measures, in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;
- h) uses an overall safety lifecycle model as the technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;

NOTE 4 Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it could also provide a technical framework for considering any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

- i) does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application). The technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards;
- j) provides general requirements for E/E/PE safety-related systems where no product or application sector international standards exist;
- k) requires malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases;

NOTE 5 Other IEC/ISO standards address this subject in depth; see ISO/IEC/TR 19791 and IEC 62443 series.

- l) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems (see k) above);
- m) does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system;
- n) does not apply for medical equipment in compliance with the IEC 60601 series.

1.3 This part of the IEC 61508 series of standards includes general requirements that are applicable to all parts. Other parts of the IEC 61508 series concentrate on more specific topics:

- parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (for hardware and software);
- part 4 gives definitions and abbreviations that are used throughout this standard;
- part 5 provides guidelines on the application of part 1 in determining safety integrity levels, by showing example methods;
- part 6 provides guidelines on the application of parts 2 and 3;
- part 7 contains an overview of techniques and measures.

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

NOTE One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

1.5 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-1 plays in the achievement of functional safety for E/E/PE safety-related systems.

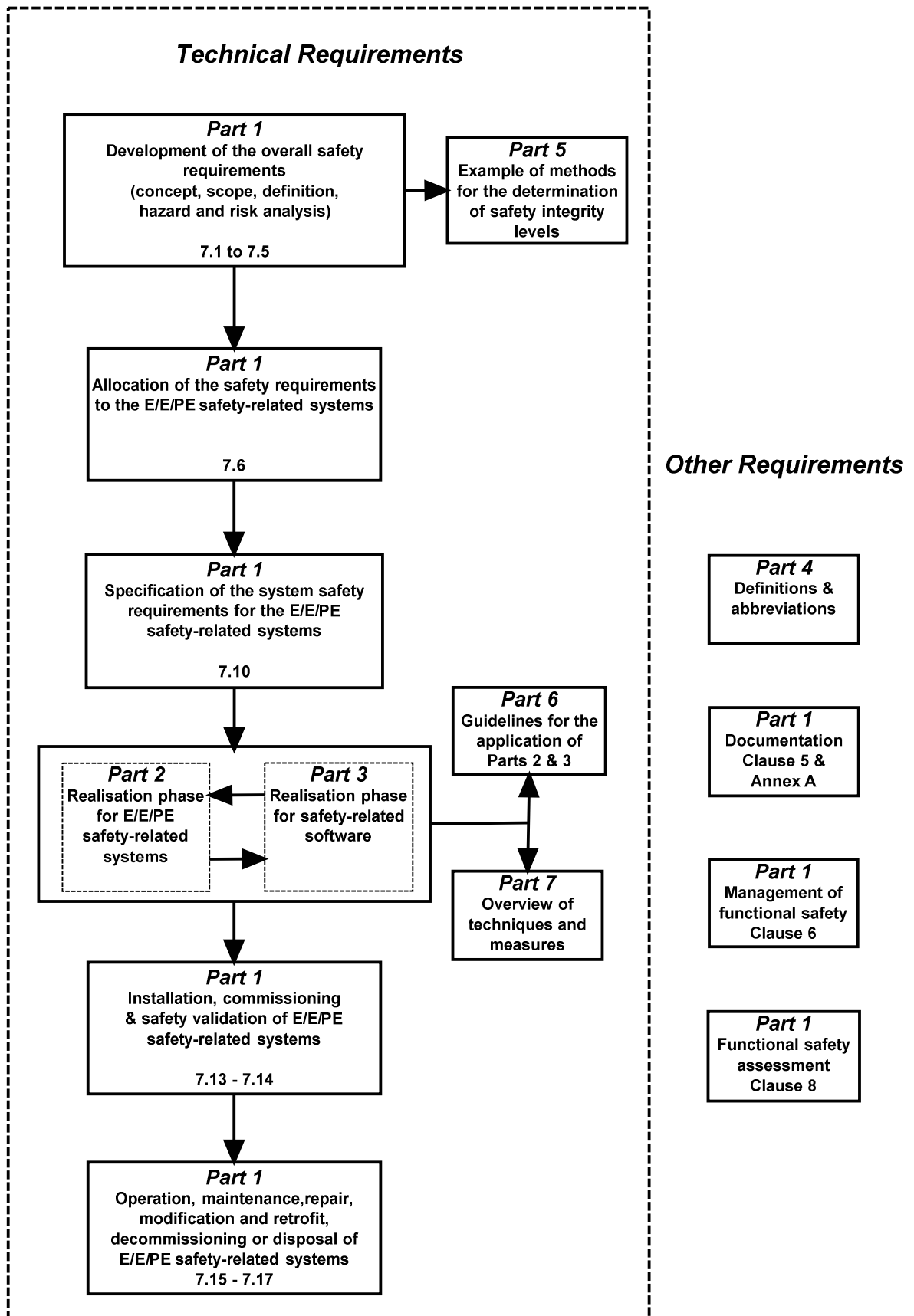


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

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

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

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

3 Definitions and abbreviations

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

4 Conformance to this standard

4.1 To conform to this standard it shall be demonstrated that all the relevant requirements have been satisfied to the required criteria specified (for example safety integrity level) and therefore, for each clause or subclause, all the objectives have been met.

4.2 This standard specifies the requirements for E/E/PE safety-related systems and has been developed to meet the full range of complexity associated with such systems. However, for low complexity E/E/PE safety-related systems (see 3.4.3 of IEC 61508-4), where dependable field experience exists which provides the necessary confidence that the required safety integrity can be achieved, the following options are available:

- in product and application sector international standards implementing the requirements of IEC 61508-1 to IEC 61508-7, certain requirements may be unnecessary and exemption from compliance with such requirements is acceptable;
- if this standard is used directly for those situations where no product or application sector international standard exists, certain of the requirements specified in this standard may be unnecessary and exemption from compliance with such requirements is acceptable providing this is justified.

4.3 Product or application sector international standards for E/E/PE safety-related systems developed within the framework of this standard shall take into account the requirements of ISO/IEC Guide 51 and IEC Guide 104.

5 Documentation

5.1 Objectives

5.1.1 The first objective of the requirements of this clause is to specify the necessary information to be documented in order that all phases of the overall, E/E/PE system and software safety lifecycles can be effectively performed.

5.1.2 The second objective of the requirements of this clause is to specify the necessary information to be documented in order that the management of functional safety (see Clause 6), verification (see 7.18) and the functional safety assessment (see Clause 8) activities can be effectively performed.

NOTE 1 The documentation requirements in this standard are concerned, essentially, with information rather than physical documents. The information need not be contained in physical documents unless this is explicitly declared in the relevant subclause.

NOTE 2 Documentation may be available in different forms (for example on paper, film, or any data medium to be presented on screens or displays).

NOTE 3 See Annex A concerning possible documentation structures.

NOTE 4 See reference [7] in the Bibliography.

5.2 Requirements

5.2.1 The documentation shall contain sufficient information, for each phase of the overall, E/E/PE system and software safety lifecycles completed, necessary for effective performance of subsequent phases and verification activities.

NOTE What constitutes sufficient information will be dependent upon a number of factors, including the complexity and size of the E/E/PE safety-related systems and the requirements relating to the specific application.

5.2.2 The documentation shall contain sufficient information required for the management of functional safety (Clause 6).

NOTE See notes to 5.1.2.

5.2.3 The documentation shall contain sufficient information required for the implementation of a functional safety assessment, together with the information and results derived from any functional safety assessment.

NOTE See notes to 5.1.2.

5.2.4 The information to be documented shall be as stated in the various clauses of this standard unless justified or shall be as specified in the product or application sector international standard relevant to the application

5.2.5 The availability of documentation shall be sufficient for the duties to be performed in respect of the clauses of this standard.

NOTE Only the information necessary to undertake a particular activity, required by this standard, need be held by each relevant party.

5.2.6 The documentation shall:

- be accurate and concise;
- be easy to understand by those persons having to make use of it;
- suit the purpose for which it is intended;
- be accessible and maintainable.

5.2.7 The documentation or set of information shall have titles or names indicating the scope of the contents, and some form of index arrangement so as to allow ready access to the information required in this standard.

5.2.8 The documentation structure may take account of company procedures and the working practices of specific product or application sectors.

5.2.9 The documents or set of information shall have a revision index (version numbers) to make it possible to identify different versions of the document.

5.2.10 The documents or set of information shall be so structured as to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document or set of information.

NOTE The physical structure of the documentation will vary depending upon a number of factors such as the size of the system, its complexity and organizational requirements.

5.2.11 All relevant documents shall be revised, amended, reviewed and approved under an appropriate document control scheme.

NOTE Where automatic or semi-automatic tools are used for the production of documentation, specific procedures may be necessary to ensure effective measures are in place for the management of versions or other control aspects of the documents.

6 Management of functional safety

6.1 Objectives

6.1.1 The first objective of the requirements of this clause is to specify the responsibilities in the management of functional safety of those who have responsibility for an E/E/PE safety-related system, or for one or more phases of the overall E/E/PE system and software safety lifecycles.

6.1.2 The second objective of the requirements of this clause is to specify the activities to be carried out by those with responsibilities in the management of functional safety.

NOTE The organizational measures dealt with in this clause provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of functional safety of the E/E/PE safety-related systems. The technical requirements necessary for maintaining functional safety will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.

6.2 Requirements

6.2.1 An organisation with responsibility for an E/E/PE safety-related system, or for one or more phases of the overall, E/E/PE system or software safety lifecycle, shall appoint one or more persons to take overall responsibility for:

- the system and for its lifecycle phases;
- coordinating the safety-related activities carried out in those phases;
- the interfaces between those phases and other phases carried out by other organisations;
- carrying out the requirements of 6.2.2 to 6.2.11 and 6.2.13;
- coordinating functional safety assessments (see 6.2.12 b) and Clause 8) – particularly where those carrying out the functional safety assessment differ between phases – including communication, planning, and integrating the documentation, judgements and recommendations;
- ensuring that functional safety is achieved and demonstrated in accordance with the objectives and requirements of this standard.

NOTE Responsibility for safety-related activities, or for safety lifecycle phases, may be delegated to other persons, particularly those with relevant expertise, and different persons could be responsible for different activities and requirements. However, the responsibility for coordination, and for overall functional safety, should reside in one or a small number of persons with sufficient management authority.

6.2.2 The policy and strategy for achieving functional safety shall be specified, together with the means for evaluating their achievement, and the means by which they are communicated within the organization.

6.2.3 All persons, departments and organizations responsible for carrying out activities in the applicable overall, E/E/PE system or software safety lifecycle phases (including persons responsible for verification and functional safety assessment and, where relevant, licensing authorities or safety regulatory bodies) shall be identified, and their responsibilities shall be fully and clearly communicated to them.

6.2.4 Procedures shall be developed for defining what information is to be communicated, between relevant parties, and how that communication will take place.

NOTE See Clause 5 for documentation requirements.

6.2.5 Procedures shall be developed for ensuring prompt follow-up and satisfactory resolution of recommendations relating to E/E/PE safety-related systems, including those arising from:

- a) hazard and risk analysis (see 7.4);
- b) functional safety assessment (see Clause 8);
- c) verification activities (see 7.18);
- d) validation activities (see 7.8 and 7.14);
- e) configuration management (see 6.2.10, 7.16, IEC 61508-2 and IEC 61508-3);
- f) incident reporting and analysis (see 6.2.6).

6.2.6 Procedures shall be developed for ensuring that all detected hazardous events are analysed, and that recommendations are made to minimise the probability of a repeat occurrence.

6.2.7 Requirements for periodic functional safety audits shall be specified, including:

- a) the frequency of the functional safety audits;
- b) the level of independence of those carrying out the audits;
- c) the necessary documentation and follow-up activities.

6.2.8 Procedures shall be developed for:

- a) initiating modifications to the E/E/PE safety-related systems (see 7.16.2.2);
- b) obtaining approval and authority for modifications.

6.2.9 Procedures shall be developed for maintaining accurate information on hazards and hazardous events, safety functions and E/E/PE safety-related systems.

6.2.10 Procedures shall be developed for configuration management of the E/E/PE safety-related systems during the overall, E/E/PE system and software safety lifecycle phases, including in particular:

- a) the point, in respect of specific phases, at which formal configuration control is to be implemented;
- b) the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);
- c) the procedures for preventing unauthorized items from entering service.

6.2.11 Training and information for the emergency services shall be provided where appropriate.

6.2.12 Those individuals who have responsibility for one or more phases of the overall, E/E/PE system or software safety lifecycles shall, in respect of those phases for which they have responsibility and in accordance with the procedures defined in 6.2.1 to 6.2.11, specify all management and technical activities that are necessary to ensure the achievement, demonstration and maintenance of functional safety of the E/E/PE safety-related systems, including:

- a) the selected measures and techniques used to meet the requirements of a specified clause or subclause (see IEC 61508-2, IEC 61508-3 and IEC 61508-6);
- b) the functional safety assessment activities, and the way in which the achievement of functional safety will be demonstrated to those carrying out the functional safety assessment (see Clause 8);

NOTE Appropriate procedures for functional safety assessment should be used to define

- the selection of an appropriate organisation, person or persons, at the appropriate level of independence;
 - the drawing up, and making changes to, terms of reference for functional safety assessments;
 - the change of those carrying out the functional safety assessment at any point during the lifecycle of a system;
 - the resolution of disputes involving those carrying out functional safety assessments.
- c) the procedures for analysing operations and maintenance performance, in particular for
 - recognising systematic faults that could jeopardise functional safety, including procedures used during routine maintenance that detect recurring faults;
 - assessing whether the demand rates and failure rates during operation and maintenance are in accordance with assumptions made during the design of the system.

6.2.13 Procedures shall be developed to ensure that all persons with responsibilities defined in accordance with 6.2.1 and 6.2.3 (i.e. including all persons involved in any overall, E/E/PE system or software lifecycle activity, including activities for verification, management of functional safety and functional safety assessment), shall have the appropriate competence (i.e. training, technical knowledge, experience and qualifications) relevant to the specific duties that they have to perform. Such procedures shall include requirements for the refreshing, updating and continued assessment of competence.

6.2.14 The appropriateness of competence shall be considered in relation to the particular application, taking into account all relevant factors including:

- a) the responsibilities of the person;
- b) the level of supervision required;
- c) the potential consequences in the event of failure of the E/E/PE safety-related systems – the greater the consequences, the more rigorous shall be the specification of competence;
- d) the safety integrity levels of the E/E/PE safety-related systems – the higher the safety integrity levels, the more rigorous shall be the specification of competence;
- e) the novelty of the design, design procedures or application – the newer or more untried these are, the more rigorous shall be the specification of competence;
- f) previous experience and its relevance to the specific duties to be performed and the technology being employed – the greater the required competence, the closer the fit shall be between the competences developed from previous experience and those required for the specific activities to be undertaken;
- g) the type of competence appropriate to the circumstances (for example qualifications, experience, relevant training and subsequent practice, and leadership and decision-making abilities);
- h) engineering knowledge appropriate to the application area and to the technology;
- i) safety engineering knowledge appropriate to the technology;

- j) knowledge of the legal and safety regulatory framework;
- k) relevance of qualifications to specific activities to be performed.

NOTE Reference [8] in the Bibliography contains an example method for managing competence for E/E/PE safety-related systems.

6.2.15 The competence of all persons with responsibilities defined in accordance with 6.2.1 and 6.2.3 shall be documented.

6.2.16 The activities specified as a result of 6.2.2 to 6.2.15 shall be implemented and monitored.

6.2.17 Suppliers providing products or services to an organization having overall responsibility for one or more phases of the overall, E/E/PE system or software safety lifecycles (see 6.2.1), shall deliver products or services as specified by that organization and shall have an appropriate quality management system.

6.2.18 Activities relating to the management of functional safety shall be applied at the relevant phases of the overall, E/E/PE system and software safety lifecycles (see 7.1.1.5).

7 Overall safety lifecycle requirements

7.1 General

7.1.1 Introduction

7.1.1.1 In order to deal in a systematic manner with all the activities necessary to achieve the required safety integrity for the safety functions carried out by the E/E/PE safety-related systems, this standard adopts an overall safety lifecycle (see Figure 2) as the technical framework.

NOTE The overall safety lifecycle should be used as a basis for claiming conformance to this standard, but a different overall safety lifecycle can be used to that given in Figure 2, providing the objectives and requirements of each clause of this standard are met.

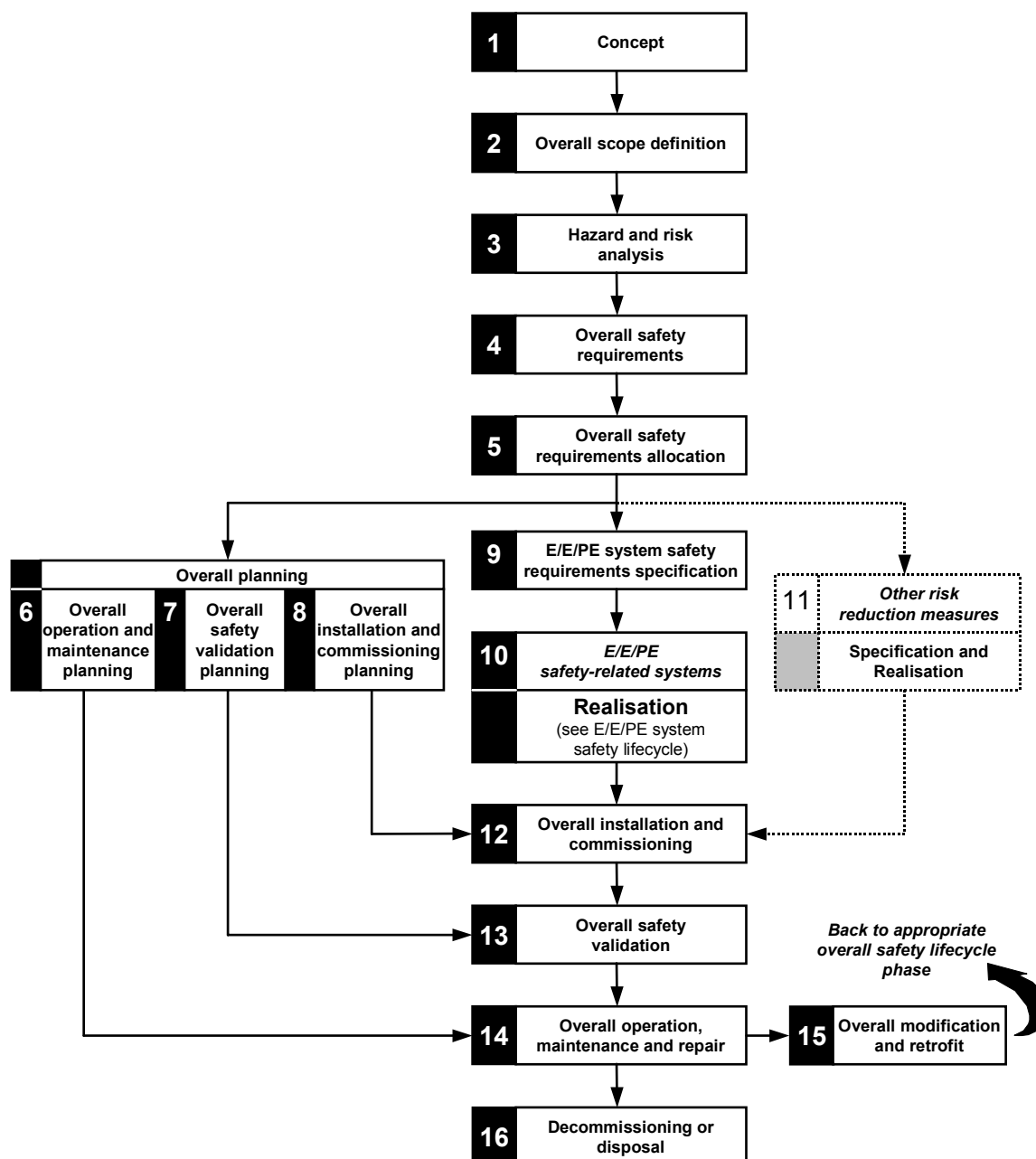
7.1.1.2 The overall safety lifecycle encompasses the following means for meeting the tolerable risk:

- E/E/PE safety-related systems;
- other risk reduction measures.

7.1.1.3 The E/E/PE safety-related systems realisation phase from the overall safety lifecycle is expanded and shown in Figure 3. This part of the E/E/PE system safety lifecycle forms the technical framework for IEC 61508-2. The part of the software safety lifecycle shown in Figure 4 forms the technical framework for IEC 61508-3. The relationship of the overall safety lifecycle to the E/E/PE system and software safety lifecycles for safety-related systems is shown in Figure 5.

7.1.1.4 The overall, E/E/PE system and software safety lifecycle figures (Figures 2 to 4) are simplified views of reality and as such do not show all the iterations relating to specific phases or between phases. Iteration, however, is an essential and vital part of development through the overall, E/E/PE system and software safety lifecycles.

7.1.1.5 Activities relating to the management of functional safety (Clause 6), verification (7.18) and functional safety assessment (Clause 8) are not shown on the overall, E/E/PE system or software safety lifecycles. This has been done in order to reduce the complexity of the lifecycle figures. These activities, where required, will need to be applied at the relevant phases of the overall, E/E/PE system and software safety lifecycles.



NOTE 1 Activities relating to **verification**, **management of functional safety** and **functional safety assessment** are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.

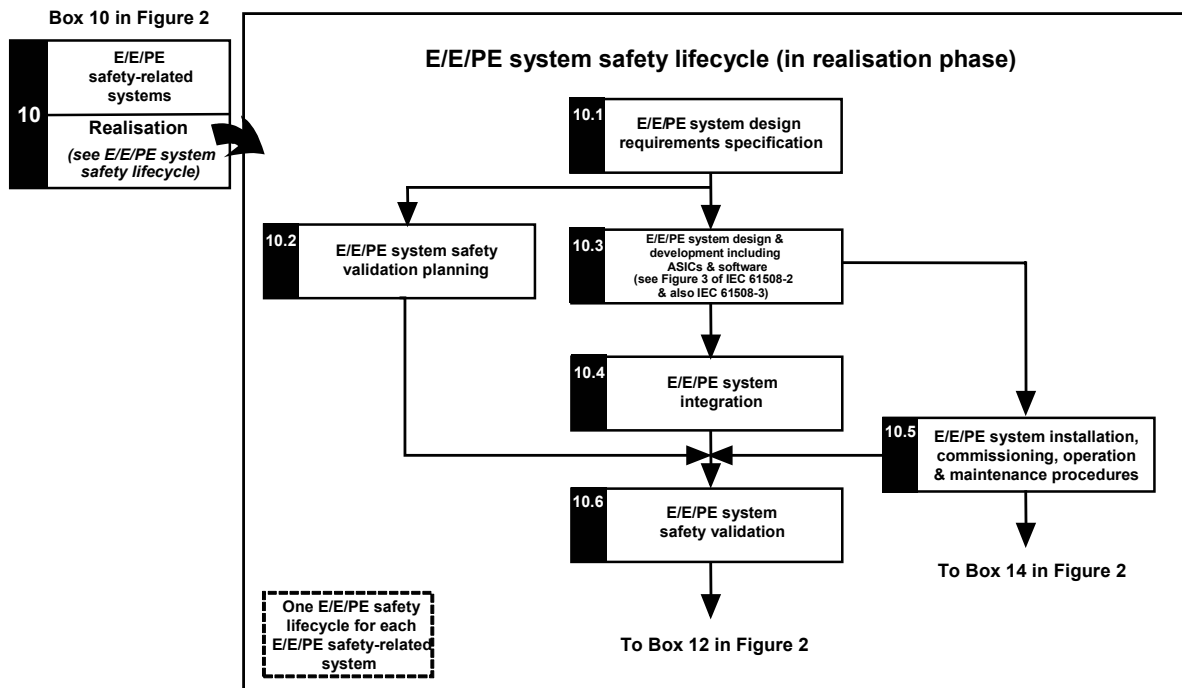
NOTE 2 The phase represented by Box 11 is outside the scope of this standard.

NOTE 3 IEC 61508-2 and IEC 61508-3 deal with Box 10 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of Boxes 13, 14 and 15.

NOTE 4 See Table 1 for a description of the objectives and scope of the phases represented by each box.

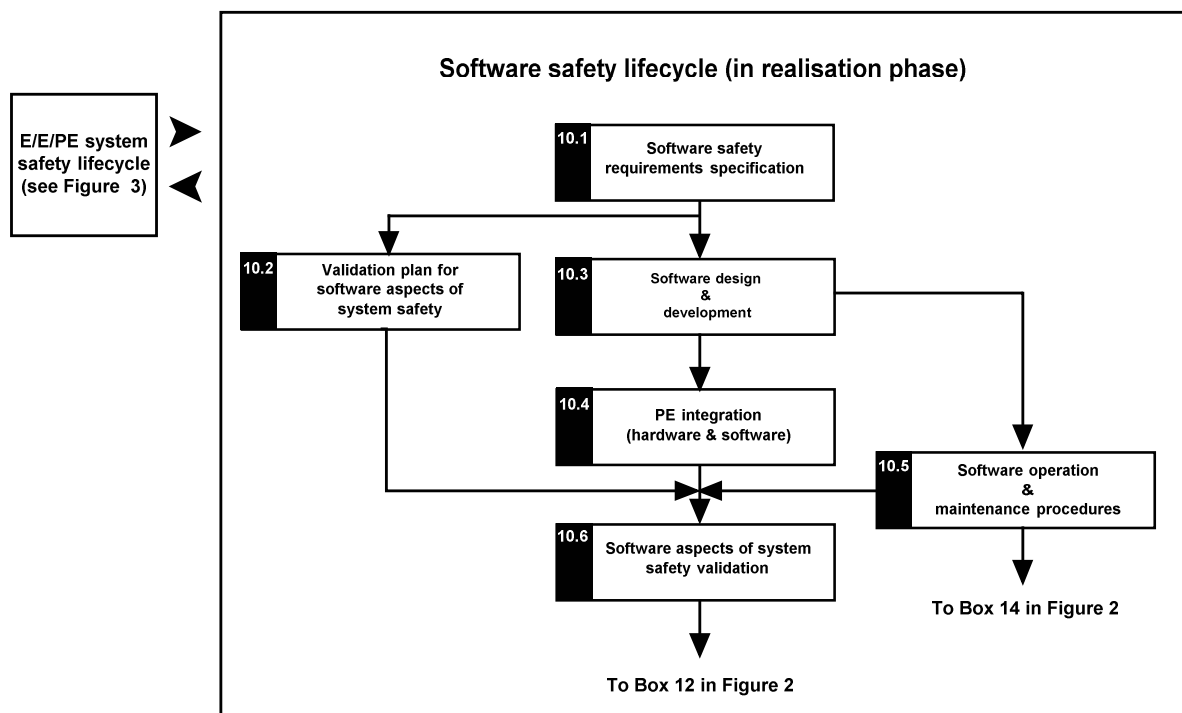
NOTE 5 The technical requirements necessary for overall operation, maintenance, repair, modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.

Figure 2 – Overall safety lifecycle



NOTE 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).

Figure 3 – E/E/PE system safety lifecycle (in realisation phase)



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

Figure 4 – Software safety lifecycle (in realisation phase)