

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

Part 1: General requirements

The European Standard EN 61508-1:2001 has the status of a British Standard

ICS 25.040.40; 29.020

National foreword

This British Standard is the official English language version of EN 61508-1:2001. It is identical with IEC 61508-1:1998 including corrigendum May 1999.

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

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

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

Cross-references

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

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

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

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 59 and a back cover.

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

Amendments issued since publication

Amd. No.	Date	Comments
10631 Corrigendum No.1	August 1999	Incorporation of IEC Corrigendum May 1999
13779	15 March 2002	Implementation of the European Standard

This British Standard, having been prepared under the direction of the Electrotechnical Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 June 1999

© BSI 15 March 2002

ISBN 0 580 32719 1

EUROPEAN STANDARD

EN 61508-1

NORME EUROPÉENNE

EUROPÄISCHE NORM

December 2001

ICS 13.110;25.040;29.020;35.240.50

English version

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

Part 1: General requirements
(IEC 61508-1:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
Partie 1: Prescriptions générales
(CEI 61508-1:1998 + corrigendum 1999)

Funktionale Sicherheit
sicherheitsbezogener elektrischer/
elektronischer/programmierbarer
elektronischer Systeme
Teil 1: Allgemeine Anforderungen
(IEC 61508-1:1998 + Corrigendum 1999)

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

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

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

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

CENELEC

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

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

© 2001 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 61508-1:2001 E



Documents
Document Sharing Hub

Foreword

The text of the International Standard IEC 61508-1:1998 including its corrigendum May 1999, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61508-1 on 2001-07-03 without any modification.

The following dates were fixed:

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

Annexes designated "normative" are part of the body of the standard.

Annexes designated "informative" are given for information only.

In this standard, annex ZA is normative and annexes A, B and C are informative.

Annex ZA has been added by CENELEC.

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

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

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

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

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

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

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

Endorsement notice

The text of the International Standard IEC 61508-1:1998 including its corrigendum May 1999 was approved by CENELEC as a European Standard without any modification.

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

IEC 61355:1997 NOTE Harmonized as EN 61355:1997 (not modified).

CONTENTS

	Page
INTRODUCTION	6
Clause	
1 Scope	8
2 Normative references	11
3 Definitions and abbreviations.....	11
4 Conformance to this standard.....	12
5 Documentation.....	12
5.1 Objectives.....	12
5.2 Requirements	13
6 Management of functional safety	14
6.1 Objectives.....	14
6.2 Requirements	14
7 Overall safety lifecycle requirements	16
7.1 General.....	16
7.2 Concept	25
7.3 Overall scope definition.....	25
7.4 Hazard and risk analysis	26
7.5 Overall safety requirements.....	28
7.6 Safety requirements allocation	29
7.7 Overall operation and maintenance planning	35
7.8 Overall safety validation planning	36
7.9 Overall installation and commissioning planning	37
7.10 Realisation: E/E/PES.....	38
7.11 Realisation: other technology	38
7.12 Realisation: external risk reduction facilities	38
7.13 Overall installation and commissioning	39
7.14 Overall safety validation	39
7.15 Overall operation, maintenance and repair.....	40
7.16 Overall modification and retrofit.....	43
7.17 Decommissioning or disposal	45
7.18 Verification.....	46
8 Functional safety assessment.....	47
8.1 Objective	47
8.2 Requirements	47

Annexes

Annex A (informative) Example documentation structure	50
A.1 General	50
A.2 Safety lifecycle document structure	51
A.3 Physical document structure	54
A.4 List of documents.....	56
Annex B (informative) Competence of persons.....	57
B.1 Objective	57
B.2 General considerations	57
Annex C (informative) Bibliography	58
Annex ZA (normative) Normative references to international publications with their corresponding European publications	59

Tables

1 Overall safety lifecycle: overview	20
2 Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in low demand mode of operation	33
3 Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in high demand or continuous mode of operation.....	33
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))	49
5 Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phase 9 - includes all phases of E/E/PES and software safety lifecycles (see figures 2, 3 and 4))	49
A.1 Example documentation structure for information related to the overall safety lifecycle	52
A.2 Example documentation structure for information related to the E/E/PES safety lifecycle	53
A.3 Example documentation structure for information related to the software safety lifecycle	54

Figures

1 Overall framework of this standard	10
2 Overall safety lifecycle.....	17
3 E/E/PES safety lifecycle (in realisation phase)	18
4 Software safety lifecycle (in realisation phase).....	18
5 Relationship of overall safety lifecycle to E/E/PES and software safety lifecycles.....	19
6 Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities	32
7 Example operations and maintenance activities model.....	42
8 Example operation and maintenance management model.....	43
9 Example modification procedure model	45
A.1 Structuring information into document sets for user groups.....	55
A.2 Structuring information for large complex systems and small low complexity systems	55

INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make 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 components (electrical/electronic/programmable electronic systems (E/E/PESs)) that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of application sector standards.

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

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

This International Standard

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

- uses safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;
- adopts a risk-based approach for the determination of the safety integrity level requirements;
- sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in
 - a low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand,
 - a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

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

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

Part 1: General requirements

1 Scope

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

1.2 In particular, this standard

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

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 3.4.4 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 possible hazards caused by failures of the safety functions to be performed by E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself (for example electric shock etc);
- d) does not cover E/E/PE systems where
- a single E/E/PE system is capable of providing the necessary risk reduction, and
 - the required safety integrity of the E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).
- e) 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 – See 3.1.1 and 7.3.1.2 of IEC 61508-4.

- f) considers E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;
- g) 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 3 – The early phases of the overall safety lifecycle include, of necessity, consideration of other technology (as well as the E/E/PE safety-related systems) and external risk reduction facilities, in order that the safety requirements specification for the E/E/PE safety-related systems can be developed in a systematic, risk-based manner.

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 the consideration of any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

- h) 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;
- i) provides general requirements for E/E/PE safety-related systems where no application sector standards exist;
- j) 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.

1.3 This part of IEC 61508 specifies the general requirements that are applicable to all parts. Other parts of IEC 61508 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 Parts 1, 2, 3 and 4 of this standard are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 of part 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*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications.

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 – In the USA and Canada, until the proposed process sector implementation of IEC 61508 is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) (see reference [8] in annex C) can be applied to the process sector instead of IEC 61508.

1.5 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-1 plays in the achievement of functional safety for E/E/PE safety-related systems.

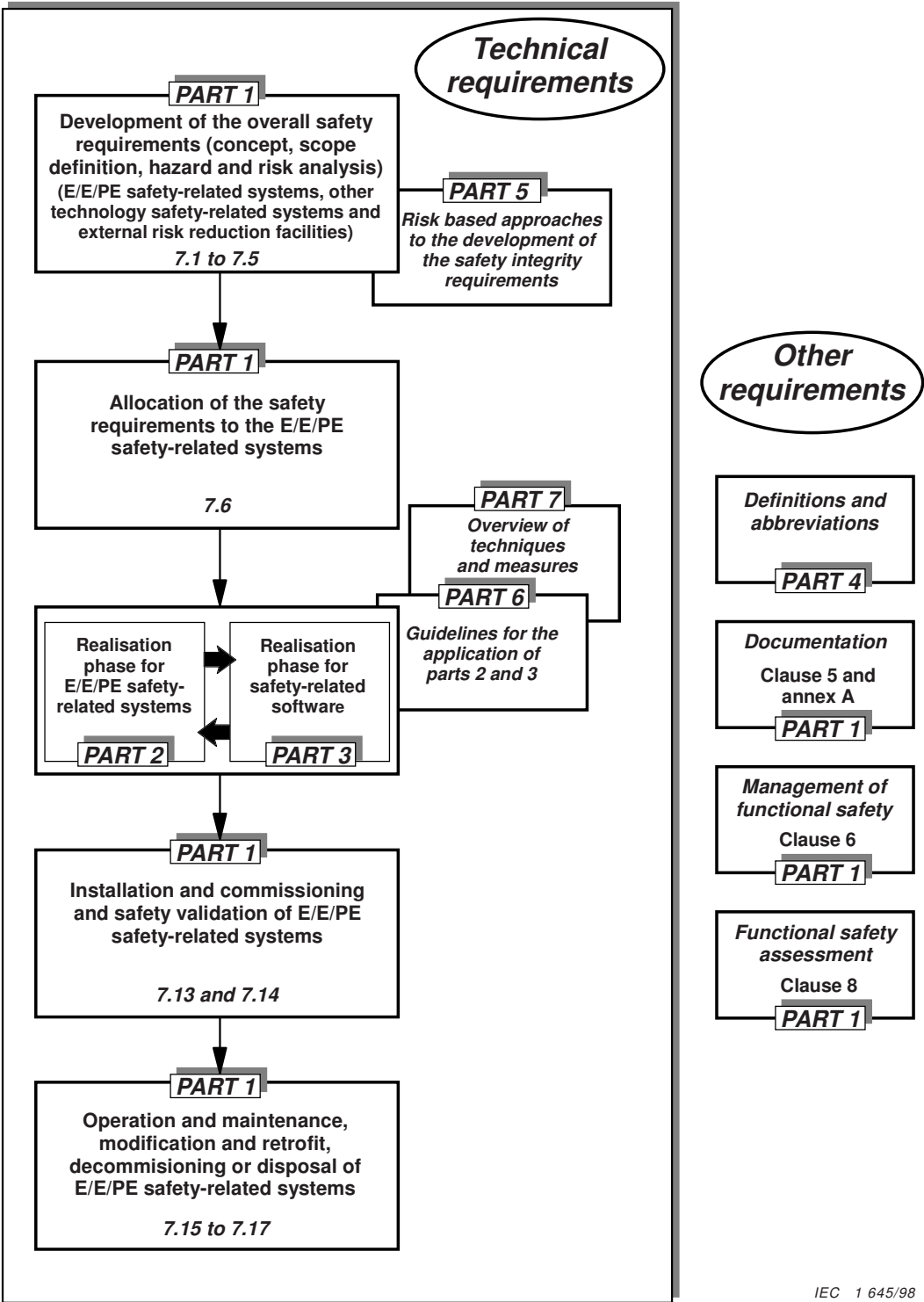


Figure 1 – Overall framework of this standard

2 Normative references

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

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

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

IEC 61508-2, — *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electrical/programmable electronic safety-related systems* ¹⁾

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

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

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

IEC 61508-6, — *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3* ¹⁾

IEC 61508-7, — *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures* ²⁾

3 Definitions and abbreviations

For the purposes of this standard, the definitions and abbreviations given in part 4 apply.

²⁾ To be published.

4 Conformance to this standard

4.1 To conform to this standard it shall be demonstrated that the 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.

NOTE – It is not generally possible to single out any one factor that determines the degree to which a requirement is to be satisfied (degree of rigour). It will be dependent upon a number of factors which, themselves, may depend upon the specific overall, E/E/PES or software safety lifecycle phase and activity. The factors will include:

- nature of the hazards;
- consequence and risk reduction;
- safety integrity level;
- type of implementation technology;
- size of systems;
- number of teams involved;
- physical distribution;
- novelty of design.

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 3.4.4 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 application sector 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 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 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/PES 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 [4] in annex C.

5.2 Requirements

5.2.1 The documentation shall contain sufficient information, for each phase of the overall, E/E/PES 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 Unless justified in the functional safety planning or specified in the application sector standard, the information to be documented shall be as stated in the various clauses of this standard.

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 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, approved and be under the control of 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 management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.

6.1.2 The second objective of the requirements of this clause is to specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.

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 normally be specified as part of the information provided by the supplier of the E/E/PE safety-related system.

6.2 Requirements

6.2.1 Those organizations or individuals that have overall responsibility for one or more phases of the overall, E/E/PES or software safety lifecycles shall, in respect of those phases for which they have overall responsibility, specify all management and technical activities that are necessary to ensure that the E/E/PE safety-related systems achieve and maintain the required functional safety. In particular, the following should be considered:

- a) the policy and strategy for achieving functional safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organization to ensure a culture of safe working;
- b) identification of the persons, departments and organizations which are responsible for carrying out and reviewing the applicable overall, E/E/PES or software safety lifecycle phases (including, where relevant, licensing authorities or safety regulatory bodies);
- c) the overall, E/E/PES or software safety lifecycle phases to be applied;
- d) the way in which information is to be structured and the extent of the information to be documented (see clause 5);
- e) the selected measures and techniques used to meet the requirements of a specified clause or subclause (see IEC 61508-2, IEC 61508-3 and 61508-6);
- f) the functional safety assessment activities (see clause 8);

- g) the procedures for ensuring prompt follow-up and satisfactory resolution of recommendations relating to E/E/PE safety-related systems arising from
 - hazard and risk analysis (see 7.4);
 - functional safety assessment (see clause 8);
 - verification activities (see 7.18);
 - validation activities (see 7.8 and 7.14);
 - configuration management (see 6.2.1 o), 7.16 and IEC 61508-2 and IEC 61508-3);
- h) the procedures for ensuring that applicable parties involved in any of the overall, E/E/PES or software safety lifecycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified:
 - the training of staff in diagnosing and repairing faults and in system testing;
 - the training of operations staff;
 - the retraining of staff at periodic intervals;

NOTE 1 – Annex B provides guidelines on the competence requirements of those involved in any overall, E/E/PES or software safety lifecycle activity.

- i) the procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations made to minimise the probability of a repeat occurrence;
- j) the procedures for analysing operations and maintenance performance. In particular procedures for
 - recognising systematic faults which could jeopardise functional safety, including procedures used during routine maintenance which 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;
- k) requirements for periodic functional safety audits in accordance with this subclause including
 - the frequency of the functional safety audits;
 - consideration as to the level of independence required for those responsible for the audits;
 - the documentation and follow-up activities;
- l) the procedures for initiating modifications to the safety-related systems (see 7.16.2.2);
- m) the required approval procedure and authority for modifications;
- n) the procedures for maintaining accurate information on potential hazards and safety-related systems;
- o) the procedures for configuration management of the E/E/PE safety-related systems during the overall, E/E/PES and software safety lifecycle phases; in particular the following should be specified:
 - the stage at which formal configuration control is to be implemented;
 - the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);
 - the procedures for preventing unauthorized items from entering service;

NOTE 2 – For more details on configuration management see references [6] and [7] in annex C.

- p) where appropriate, the provision of training and information for the emergency services.

6.2.2 The activities specified as a result of 6.2.1 shall be implemented and progress monitored.

6.2.3 The requirements developed as a result of 6.2.1 shall be formally reviewed by the organizations concerned, and agreement reached.

6.2.4 All those specified as responsible for management of functional safety activities shall be informed of the responsibilities assigned to them.

6.2.5 Suppliers providing products or services to an organization having overall responsibility for one or more phases of the overall, E/E/PES 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.

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 level for 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.

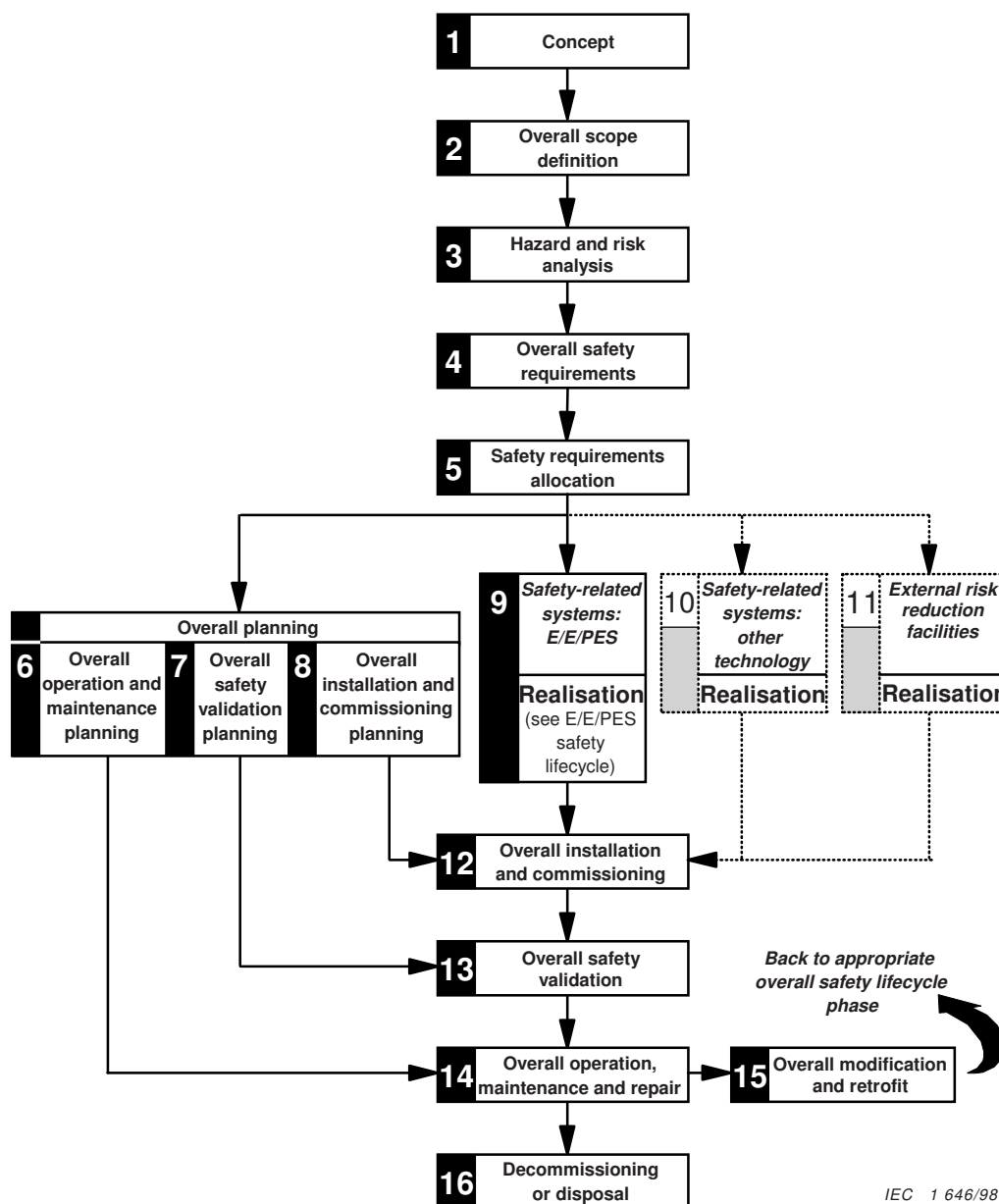
7.1.1.2 The overall safety lifecycle encompasses the following risk reduction measures:

- E/E/PE safety-related systems;
- other technology safety-related systems;
- external risk reduction facilities.

7.1.1.3 The portion of the overall safety lifecycle dealing with E/E/PE safety-related systems is expanded and shown in figure 3. This is termed the E/E/PES safety lifecycle and forms the technical framework for IEC 61508-2. The software safety lifecycle is shown in figure 4 and forms the technical framework for IEC 61508-3. The relationship of the overall safety lifecycle to the E/E/PES and software safety lifecycles for safety-related systems is shown in figure 5.

7.1.1.4 The overall, E/E/PES 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/PES 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/PES or software safety lifecycles. This has been done in order to reduce the complexity of the overall, E/E/PES and software safety lifecycle figures. These activities, where required, will need to be applied at the relevant phases of the overall, E/E/PES 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/PES and software safety lifecycle phases.

NOTE 2 – The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 – IEC 61508-2 and IEC 61508-3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

Figure 2 – Overall safety lifecycle