BS EN 61508-1:2010

BSI Standards Publication

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

Part 1: General requirements

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 61508-1:2010. It is identical to IEC 61508-1:2010. It supersedes BS EN 61508-1:2002 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 56233 4

ICS 13.260; 25.040.40; 29.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2010.

Amendments issued since publication

Amd. No.	Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61508-1

May 2010

ICS 13.110; 25.040; 29.020

Supersedes EN 61508-1:2001

English version

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

(IEC 61508-1:2010)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 1: Exigences générales
(CEI 61508-1:2010)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme -Teil 1: Allgemeine Anforderungen
(IEC 61508-1:2010)

This European Standard was approved by CENELEC on 2010-05-01. 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, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 61508-1:2010 E

Foreword

The text of document 65A/548/FDIS, future edition 2 of IEC 61508-1, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61508-1 on 2010-05-01.

This European Standard supersedes EN 61508-1:2001.

It has the status of a basic safety publication according to IEC Guide 104.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

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)	2011-02-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-05-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61508-1:2010 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

[1] IEC 61511 series	NOTE	Harmonized in EN 61511 series (not modified).
[2] IEC 62061	NOTE	Harmonized as EN 62061.
[3] IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
[5] IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
[6] IEC 61508-7:2010	NOTE	Harmonized as EN 61508-7:2010 (not modified).
[10] IEC 60300-3-1:2003	NOTE	Harmonized as EN 60300-3-1:2004 (not modified).
[15] IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1.
[17] IEC 61355 series	NOTE	Harmonized in EN 61355 series (not modified).
[18] IEC 60601 series	NOTE	Harmonized in EN 60601 series (partially modified).
[20] IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
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	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010
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	-	-

CONTENTS

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.

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.

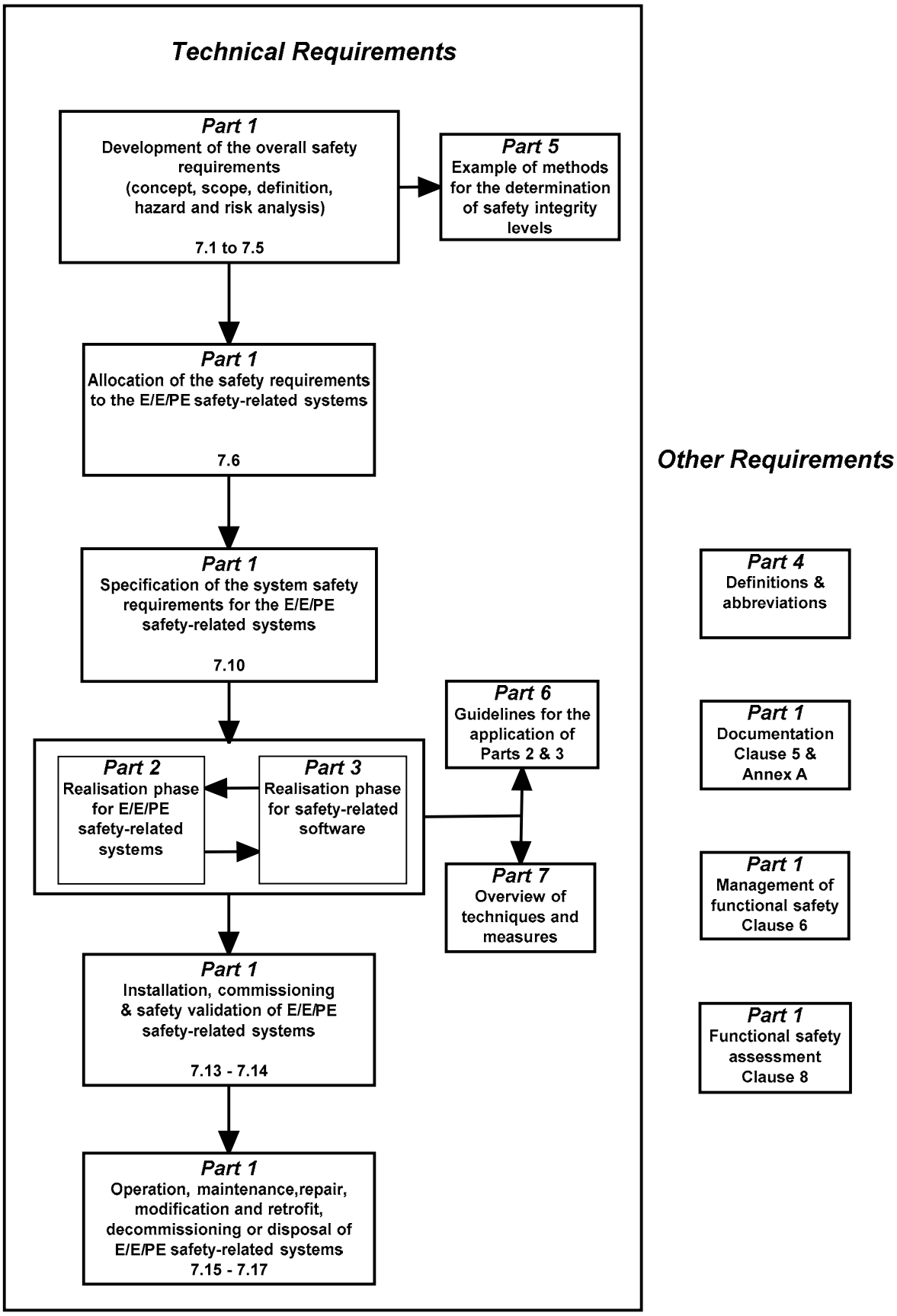


Figure 1 – Overall framework of the IEC 61508 series

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:

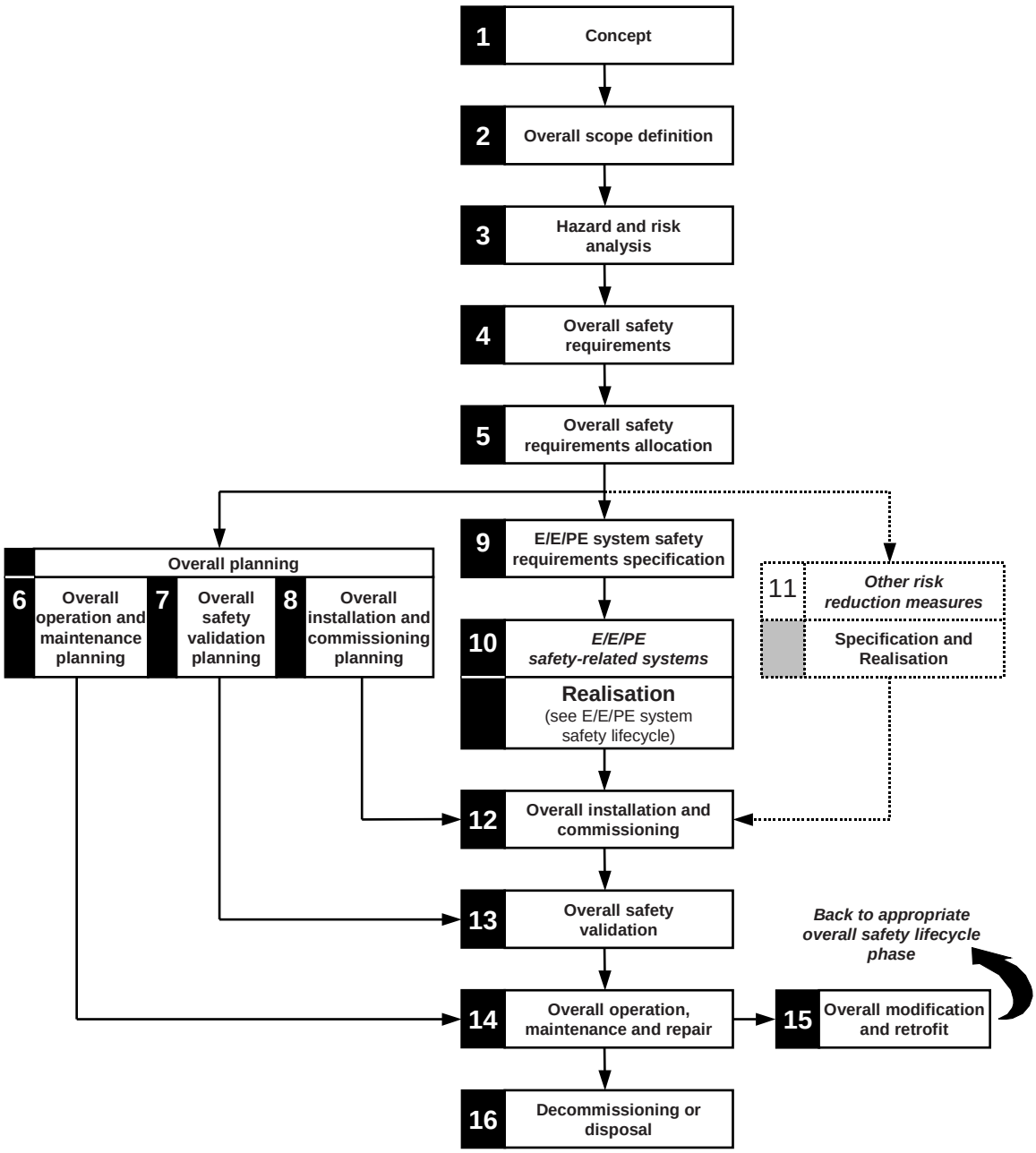
– E/E/PE safety-related systems;

– 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.

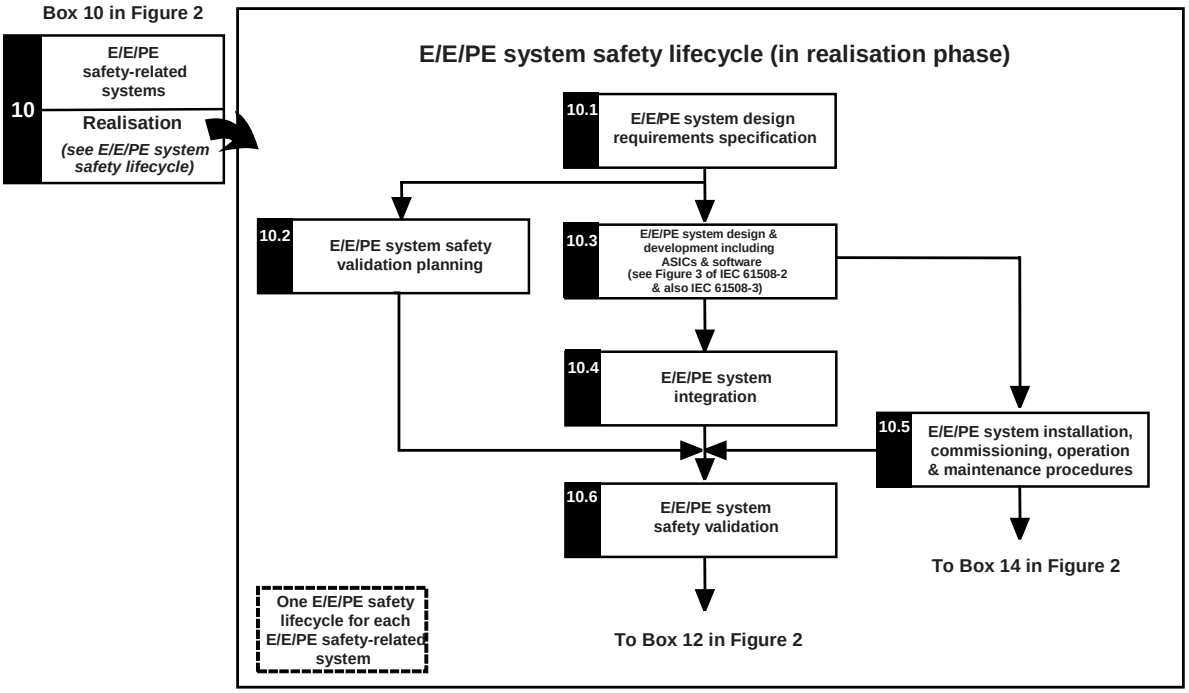
NOTE 2 The phase represented by Box 11 is outside the scope of this standard.

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.

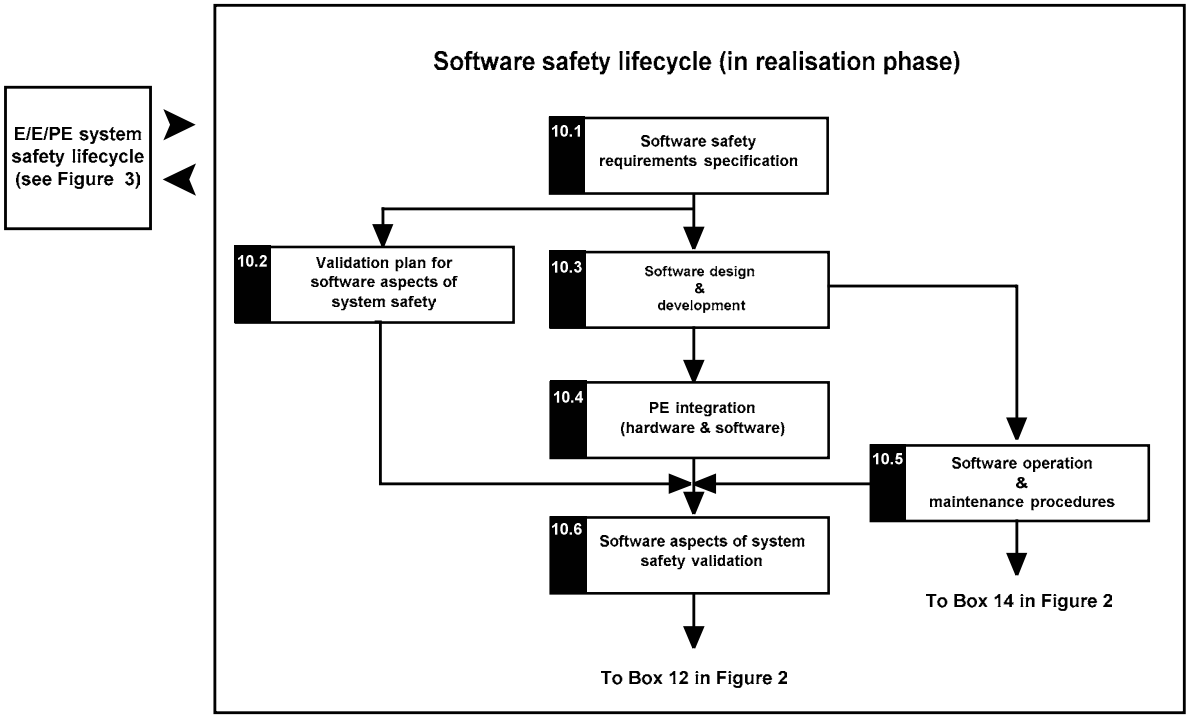
NOTE 5 The technical requirements necessary for overall operation, maintenance, repair, modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.

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)

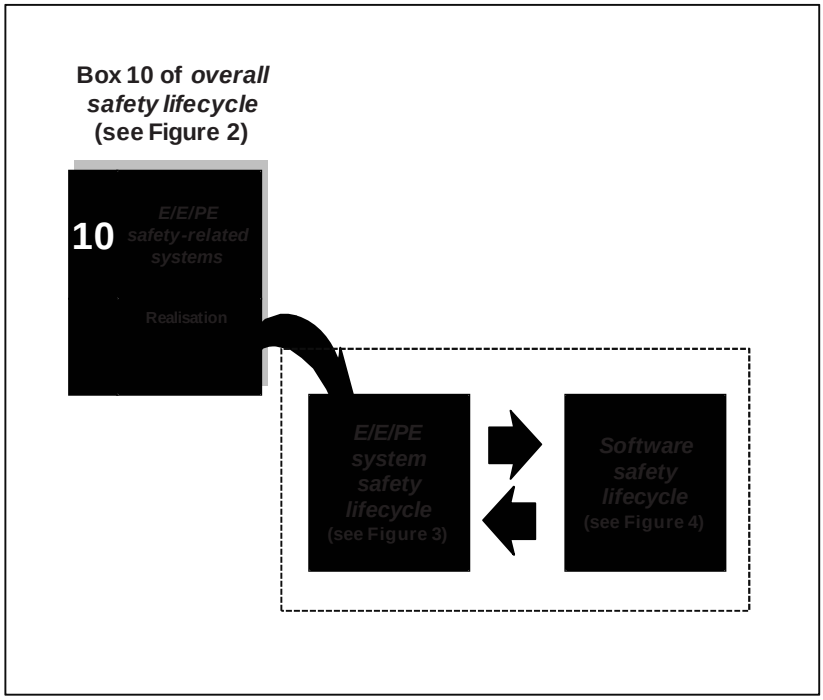


Figure 5 – Relationship of overall safety lifecycle to the E/E/PE system and software safety lifecycles

7.1.2 Objectives and requirements – general

7.1.2.1 The objectives and requirements for the overall safety lifecycle phases are contained in 7.2 to 7.17. The objectives and requirements for the E/E/PE system and software safety lifecycle phases are contained in IEC 61508-2 and IEC 61508-3 respectively.

NOTE 7.2 to 7.17 relate to specific boxes (phases) in Figure 2. The specific box is referenced in notes to these subclauses.

7.1.2.2 For all phases of the overall safety lifecycle, Table 1 indicates:

– the objectives to be achieved;
– the scope of the phase;
– the reference to the subclause containing the requirements;
– the required inputs to the phase;
– the outputs required to comply with the requirements.

Table 1 – Overall safety lifecycle – overview

Safety lifecycle phase		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	**Title**					
1	**Concept**	7.2.1: To develop a level of understanding of the EUC and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.	EUC and its environment (physical, legislative etc.).	7.2.2	All relevant information necessary to meet the requirements of the subclause.	Information concerning the EUC, its environment and hazards.
2	**Overall scope definition**	7.3.1: To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.).	EUC and its environment.	7.3.2	Information concerning the EUC, its environment and hazards.	Defined scope of the hazard and risk analysis.
3	**Hazard and risk analysis**	7.4.1: To determine the hazards, hazardous events and hazardous situations relating to the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse (see 3.1.14 of IEC 61508-4); To determine the event sequences leading to the hazardous events; To determine the EUC risks associated with the hazardous events.	The scope will be dependent upon the phase reached in the overall, E/E/PE system and software safety lifecycles (since it may be necessary for more than one hazard and risk analysis to be carried out). For the preliminary hazard and risk analysis, the scope will be as defined by the output of the overall scope definition.	7.4.2	Defined scope of the hazard and risk analysis.	Description of, and information relating to, the hazard and risk analysis.
4	**Overall safety require-ments**	7.5.1: To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems and other risk reduction measures, in order to achieve the required functional safety.	As defined by the output of the overall scope definition.	7.5.2	Description of, and information relating to, the hazard and risk analysis.	Specification of the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.

Table 1 *(continued)*

Safety lifecycle phase		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	**Title**					
5	**Overall safety require-ments allocation**	7.6.1: To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety-related systems and other risk reduction measures; To allocate a safety integrity level to each safety function to be carried out by an E/E/PE safety-related system.	As defined by the output of the overall scope definition.	7.6.2	Specification of the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	Information on the allocation of the overall safety functions, their target failure measures, and associated safety integrity levels Assumptions made concerning other risk reduction measures that need to be managed throughout the life of the EUC (see 7.6.2.13).
6	**Overall operation and mainte-nance planning**	7.7.1: To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.7.2	Information on the allocation of the overall safety functions, their target failure measures, and associated safety integrity levels Assumptions made concerning other risk reduction measures that need to be managed throughout the life of the EUC (see 7.6.2.13).	A plan for operating and maintaining the E/E/PE safety-related systems.
7	**Overall safety validation planning**	7.8.1: To develop a plan for the overall safety validation of the E/E/PE safety-related systems.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.8.2	Information and results of the overall safety requirements allocation.	A plan for the overall safety validation of the E/E/PE safety-related systems.
8	**Overall installa-tion and commis-sioning planning**	7.9.1: To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved; To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved.	EUC and the EUC control system; E/E/PE safety-related systems.	7.9.2	Information and results of the overall safety requirements allocation.	A plan for the installation of the E/E/PE safety-related systems; A plan for the commissioning of the E/E/PE safety-related systems.

Table 1 *(continued)*

Safety lifecycle phase		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	**Title**					
9	**E/E/PE system safety require-ments specifi-cation**	7.10.1: To define the E/E/PE system safety requirements, in terms of the E/E/PE system safety functions requirements and the E/E/PE system safety integrity requirements, in order to achieve the required functional safety.	E/E/PE safety-related systems	7.10.2	Information and results of the overall safety requirements allocation.	Specification of the E/E/PE system safety requirements.
10	**E/E/PE safety-related systems: realisation**	7.11.1 and parts 2 and 3: To create E/E/PE safety-related systems conforming to the specification for the E/E/PE system safety requirements (comprising the specification for the E/E/PE system safety functions requirements and the specification for the E/E/PE system safety integrity requirements).	E/E/PE safety-related systems.	7.11.2, IEC 61508-2 and IEC 61508-3	Specification of the E/E/PE system safety requirements.	Realisation of each E/E/PE safety-related system according to the E/E/PE system safety requirements specification.
11	**Other risk reduction measures: specifi-cation and realisation**	7.12.1: To create other risk reduction measures to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other risk reduction measures.	7.12.2	Other risk reduction measures safety requirements specification (outside the scope and not considered further in this standard).	Realisation of each other risk reduction measure according to the safety requirements for that measure.
12	**Overall installa-tion and commis-sioning**	7.13.1: To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems.	EUC and the EUC control system; E/E/PE safety-related systems.	7.13.2	A plan for the installation of the E/E/PE safety-related systems; A plan for the commis-sioning of the E/E/PE safety-related systems.	Fully installed E/E/PE safety-related systems; Fully commissioned E/E/PE safety-related systems.
13	**Overall safety validation**	7.14.1: To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.	EUC and the EUC control system; E/E/PE safety-related systems.	7.14.2	Overall safety validation plan for the E/E/PE safety-related systems; Information and results of the overall safety requirements allocation.	Confirmation that all the E/E/PE safety-related systems meet the specification for the overall safety requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems.

Table 1 *(continued)*

Safety lifecycle phase		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	**Title**					
14	**Overall operation, mainte-nance and repair**	7.15.1: To ensure the functional safety of the E/E/PE safety-related systems is maintained to the specified level; To ensure that the technical requirements, necessary for the overall operation, maintenance and repair of the E/E/PE safety-related systems, are specified and provided to those responsible for the future operation and maintenance of the E/E/PE safety-related systems.	EUC and the EUC control system; E/E/PE safety-related systems.	7.15.2	Overall operation and maintenance plan for the E/E/PE safety-related systems.	Continuing achievement of the required functional safety for the E/E/PE safety-related systems; Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems.
15	**Overall modifica-tion and retrofit**	7.16.1: To define the procedures that are necessary to ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.	EUC and the EUC control system; E/E/PE safety-related systems.	7.16.2	Request for modification or retrofit under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems, both during and after the modification and retrofit phase has taken place; Chronological documentation of modification and retrofit of the E/E/PE safety-related systems.
16	**Decom-mis-sioning or disposal**	7.17.1: To define the procedures that are necessary to ensure that the functional safety for the E/E/PE safety-related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC.	EUC and the EUC control system; E/E/PE safety-related systems.	7.17.2	Request for decommis-sioning or disposal under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems both during and after the decommis-sioning or disposal activities; Chronological documentation of the decommis-sioning or disposal activities.

7.1.3 Objectives

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

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

NOTE See Clause 5 for documentation requirements and Annex A for an example documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific product or application sectors.

7.1.4 Requirements

7.1.4.1 The overall safety lifecycle that shall be used as the basis for claiming conformance to this standard is that specified in Figure 2. If another overall safety lifecycle is used, it shall be specified as part of the management of functional safety activities (see Clause 6) and all the objectives and requirements in each clause or subclause in this standard shall be met.

NOTE The parts of the E/E/PE system safety lifecycle and the software safety lifecycle that form the realisation phase of the overall safety lifecycle are specified in IEC 61508-2 and IEC 61508-3 respectively.

7.1.4.2 The requirements for the management of functional safety (see Clause 6) shall run in parallel with the overall safety lifecycle phases.

7.1.4.3 Unless justified, each phase of the overall safety lifecycle shall be applied and the requirements met.

7.1.4.4 Each phase of the overall safety lifecycle shall be divided into elementary activities with the scope, inputs and outputs specified for each phase.

7.1.4.5 The scope and inputs for each overall safety lifecycle phase shall be as specified in Table 1 unless justified as part of the management of functional safety activities (see Clause 6) or specified in the product or application sector international standard.

7.1.4.6 The outputs from each phase of the overall safety lifecycle shall be those specified in Table 1 unless justified as part of the management of functional safety activities (see Clause 6) or specified in the product or application sector international standard.

7.1.4.7 The outputs from each phase of the overall safety lifecycle shall meet the objectives and requirements specified for each phase (see 7.2 to 7.17).

7.1.4.8 The verification requirements that shall be met for each overall safety lifecycle phase are specified in 7.18.

7.2 Concept

NOTE This phase is Box 1 of Figure 2.

7.2.1 Objective

The objective of the requirements of this subclause is to develop a level of understanding of the EUC and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.

7.2.2 Requirements

7.2.2.1 A thorough familiarity shall be acquired of the EUC, its required control functions and its physical environment.

7.2.2.2 The likely sources of hazards, hazardous situations and harmful events shall be determined.

7.2.2.3 Information about the determined hazards shall be obtained (for example, duration, intensity, toxicity, exposure limit, mechanical force, explosive conditions, reactivity, flammability etc.).

7.2.2.4 Information about the current safety regulations (national and international) shall be obtained.

7.2.2.5 Hazards, hazardous situations and harmful events due to interaction with other equipment or systems (installed or to be installed) of the EUC shall be considered together with other EUCs (installed or to be installed)

7.2.2.6 The information and results acquired in 7.2.2.1 to 7.2.2.5 shall be documented.

7.3 Overall scope definition

NOTE This phase is Box 2 of Figure 2.

7.3.1 Objectives

7.3.1.1 The first objective of the requirements of this subclause is to determine the boundary of the EUC and the EUC control system.

7.3.1.2 The second objective of the requirements of this subclause is to specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.).

7.3.2 Requirements

7.3.2.1 The boundary of the EUC and the EUC control system shall be defined so as to include all equipment and systems (including humans where appropriate) that are associated with relevant hazards and hazardous events.

NOTE Several iterations between overall scope definition and hazard and risk analysis may be necessary.

7.3.2.2 The physical equipment, including the EUC and the EUC control system, to be included in the scope of the hazard and risk analysis shall be specified.

NOTE See references [9] and [10] in the Bibliography.

7.3.2.3 The external events to be taken into account in the hazard and risk analysis shall be specified.

7.3.2.4 The equipment and systems that are associated with the hazards and hazardous events shall be specified.

7.3.2.5 The type of initiating events that need to be considered (for example component failures, procedural faults, human error, dependent failure mechanisms that can cause hazardous events) shall be specified.

7.3.2.6 The information and results acquired in 7.3.2.1 to 7.3.2.5 shall be documented.

7.4 Hazard and risk analysis

NOTE This phase is Box 3 of Figure 2.

7.4.1 Objectives

7.4.1.1 The first objective of the requirements of this subclause is to determine the hazards, hazardous events and hazardous situations relating to the EUC and the EUC control system (in all modes of operation) for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse (see 3.1.14 of IEC 61508-4);

7.4.1.2 The second objective of the requirements of this subclause is to determine the event sequences leading to the hazardous events determined in 7.4.1.1.

7.4.1.3 The third objective of the requirements of this subclause is to determine the EUC risks associated with the hazardous events determined in 7.4.1.1.

NOTE 1 This subclause is necessary in order that the safety requirements for the E/E/PE safety-related systems are based on a systematic risk-based approach. This cannot be done unless the EUC and the EUC control system are considered.

NOTE 2 In application areas where valid assumptions can be made about the risks associated with the hazardous events and their consequences, the analysis required in this subclause (and 7.5) may be carried out by the developers of application sector versions of this standard, and may be embedded in simplified graphical requirements. Examples of such methods are given in IEC 61508-5, Annexes E and G.

7.4.2 Requirements

7.4.2.1 A hazard and risk analysis shall be undertaken which shall take into account information from the overall scope definition phase (see 7.3). If decisions are taken at later stages in the overall, E/E/PE system or software safety lifecycle phases that may change the basis on which the earlier decisions were taken, then a further hazard and risk analysis shall be undertaken.

NOTE 1 For guidance see references [9] and [10] in the Bibliography.

NOTE 2 As an example of the need to continue hazard and risk analysis deep into the overall safety lifecycle, consider the analysis of an EUC that incorporates a safety-related valve. A hazard and risk analysis may determine two event sequences, that include valve fails closed and valve fails open, leading to hazardous events. However, when the detailed design of the EUC control system controlling the valve is analyzed, a new failure mode, valve oscillates, may be discovered which introduces a new event sequence leading to a hazardous event.

7.4.2.2 Consideration shall be given to the elimination or reduction of the hazards.

NOTE Although not within the scope of this standard, it is of primary importance that identified hazards of the EUC are eliminated at source, for example by the application of inherent safety principles and the application of good engineering practice.

7.4.2.3 The hazards, hazardous events and hazardous situations of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions, reasonably foreseeable misuse and malevolent or unauthorised action). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC. If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out.

NOTE 1 For reasonably foreseeable misuse see 3.1.14 of IEC 61508-4.

NOTE 2 For guidance on hazard identification including guidance on representation and analysis of human factor issues, see reference [11] in the bibliography.

NOTE 3 For guidance on security risks analysis, see IEC 62443 series.

NOTE 4 Malevolent or unauthorised action covers security threats.

NOTE 5 The hazard and risk analysis should also consider whether the activation of a safety function due to a demand or spurious action will give rise to a new hazard. In such a situation it may be necessary to develop a new safety function in order to deal with this hazard.

7.4.2.4 The event sequences leading to the hazardous events determined in 7.4.2.3 shall be determined.

NOTE 1 The event sequences should be considered taking into account safety policy and risk management decisions.

NOTE 2 It is normally worthwhile to consider if any of the event sequences can be eliminated by modifications to the process design or equipment used.

7.4.2.5 The likelihood of the hazardous events for the conditions specified in 7.4.2.3 shall be evaluated.

7.4.2.6 The consequences associated with the hazardous events determined in 7.4.2.3 shall be determined.

7.4.2.7 The EUC risk shall be evaluated, or estimated, for each determined hazardous event.

7.4.2.8 The requirements of 7.4.2.1 to 7.4.2.7 can be met by the application of either qualitative or quantitative hazard and risk analysis techniques (see IEC 61508-5).

7.4.2.9 The appropriateness of the techniques, and the extent to which the techniques will need to be applied, will depend on a number of factors, including:

– the specific hazards and the consequences;
– the complexity of the EUC and the EUC control system;
– the application sector and its accepted good practices;
– the legal and safety regulatory requirements;
– the EUC risk;
– the availability of accurate data upon which the hazard and risk analysis is to be based.

7.4.2.10 The hazard and risk analysis shall consider the following:

– each determined hazardous event and the components that contribute to it;
– the consequences and likelihood of the event sequences with which each hazardous event is associated;
– the tolerable risk for each hazardous event;
– the measures taken to reduce or remove hazards and risks;
– the assumptions made during the analysis of the risks, including the estimated demand rates and equipment failure rates; any credit taken for operational constraints or human intervention shall be detailed.

7.4.2.11 The information and results that constitute the hazard and risk analysis shall be documented.

7.4.2.12 The information and results that constitute the hazard and risk analysis shall be maintained for the EUC and the EUC control system throughout the overall safety lifecycle, from the hazard and risk analysis phase to the decommissioning or disposal phase.

NOTE The maintenance of the information, arising from the results of the hazard and risk analysis phase, is a key means of tracking the progress on outstanding hazard and risk analysis issues.

7.5 Overall safety requirements

NOTE This phase is Box 4 of Figure 2.

7.5.1 Objective

The objective of the requirements of this subclause is to develop the specification for the overall safety requirements, in terms of the overall safety functions requirements and overall safety integrity requirements, for the E/E/PE safety-related systems and other risk reduction measures, in order to achieve the required functional safety.

NOTE In application areas where valid assumptions can be made about the risks, likely hazards, harmful events and their consequences, the analysis required in this subclause (and 7.4) may be carried out by the developers of application sector versions of this standard, and may be embedded in simplified graphical requirements. Examples of such methods are given in IEC 61508-5, Annexes E and F.

7.5.2 Requirements

7.5.2.1 A set of all necessary overall safety functions shall be developed based on the hazardous events derived from the hazard and risk analysis. This shall constitute the specification for the overall safety functions requirements.

NOTE 1 It will be necessary to create an overall safety function for each hazardous event.

NOTE 2 The overall safety functions to be performed will not, at this stage, be specified in technology-specific terms since the method and technology of implementation of the overall safety functions will not be known until later. During the allocation of overall safety requirements (see 7.6), the description of the safety functions may need to be modified to reflect the specific method of implementation.

EXAMPLE Prevent temperature in vessel X rising above 250 °C and prevent speed of drive Y exceeding 3 000 r/min are examples of overall safety functions.

7.5.2.2 If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements.

NOTE Guidance is given in IEC 62443 series.

7.5.2.3 For each overall safety function, a target safety integrity requirement shall be determined that will result in the tolerable risk being met. Each requirement may be determined in a quantitative and/or qualitative manner. This shall constitute the specification for the overall safety integrity requirements.

NOTE 1 The specification of the overall safety integrity requirements is an interim stage towards the determination of the target failure measures and associated safety integrity levels for the safety functions to be implemented by the E/E/PE safety-related systems. Some of the qualitative methods used to determine the safety integrity levels (see IEC 61508-5, Annexes E and F) progress directly from the risk parameters to the safety integrity levels. In such cases, the safety integrity requirements are implicitly rather than explicitly stated because they are incorporated in the method itself.

NOTE 2 The EUC risk can be reduced either by reducing the consequences of the hazardous event (this is preferred), or by reducing the rate of hazardous events of the EUC and the EUC control system (see 7.5.2.4 below).

NOTE 3 The required reduction in frequency of the hazardous event can be achieved by additional measures comprising E/E/PE safety-related system(s) and/or other risk reduction measures including other technology safety-related systems or managed measures such as escape, occupancy or exposure time.

NOTE 4 In order to satisfy tolerable risk criteria, it may be necessary when determining the target safety integrity for each safety function to take into account that individuals may be exposed to risks from other sources.

NOTE 5 For situations where an application sector international standard exists that includes appropriate methods for directly determining the safety integrity requirements, then such standards may be used to meet the requirements of this subclause.

7.5.2.4 The overall safety integrity requirements shall be specified in terms of either

– the risk reduction required to achieve the tolerable risk, or

– the tolerable hazardous event rate so as to meet the tolerable risk.

7.5.2.5 If, in assessing the EUC risk, the average frequency of dangerous failures of a single EUC control system function is claimed as being lower than 10^{-5} dangerous failures per hour

then the EUC control system shall be considered to be a safety-related control system subject to the requirements of this standard.

NOTE For example, if a rate of dangerous failure between 10^{-6} and 10^{-5} dangerous failures per hour is claimed for the EUC control system, then the EUC control system is regarded as an E/E/PE safety-related system and the requirements appropriate to safety integrity level 1 would need to be met.

7.5.2.6 Where failures of the EUC control system place a demand on one or more E/E/PE safety-related systems and/or other risk reduction measures, and where the intention is not to designate the EUC control system as a safety-related system, the following requirements shall apply:

a) the rate of dangerous failure claimed for the EUC control system shall be supported by data acquired through one of the following:
   – actual operating experience of the EUC control system in a similar application;
   – a reliability analysis carried out to a recognised procedure;
   – an industry database of reliability of generic equipment;
b) the rate of dangerous failure that can be claimed for the EUC control system shall be no lower than 10^{-5} dangerous failures per hour;

NOTE 1 See 7.5.2.5.

c) all reasonably foreseeable dangerous failure modes of the EUC control system shall be taken into account in developing the specification for the overall safety requirements;
d) the EUC control system shall be independent from the E/E/PE safety-related systems and other risk reduction measures.

NOTE 2 Providing the safety-related systems have been designed to provide adequate safety integrity, taking into account the normal demand rate from the EUC control system, it will not be necessary to designate the EUC control system as a safety-related system (and, therefore, its functions will not be designated as safety functions within the context of this standard). In some applications, particularly where very high safety integrity is required, it may be appropriate to reduce the demand rate by designing the EUC control system to have a lower than normal failure rate. In such cases, if the failure rate claimed is less than the higher limit target safety integrity for safety integrity level 1 (see Table 3), then the control system will become safety-related and the requirements in this standard will apply.

NOTE 3 See 7.6.2.7 for meaning of independent.

7.5.2.7 If the requirements of 7.5.2.6 a) to d) inclusive cannot be met, then the EUC control system shall be designated as a safety-related system. The safety integrity level of functions of the EUC control system shall be determined by the rate of dangerous failure that is claimed for the EUC control system in accordance with Table 3 (see Note 3 of 7.6.2.9). In such cases, the requirements in this standard, relevant to the allocated safety integrity level, shall apply to the EUC control system.

NOTE See 7.5.2.5 and also 7.6.2.10.

7.6 Overall safety requirements allocation

NOTE This phase is Box 5 of Figure 2.

7.6.1 Objectives

7.6.1.1 The first objective of the requirements of this subclause is to allocate the overall safety functions, contained in the specification for the overall safety requirements (both the overall safety functions requirements and the overall safety integrity requirements), to the designated E/E/PE safety-related systems and other risk reduction measures.

NOTE Other risk reduction measures are considered of necessity, since the allocation to E/E/PE safety-related systems cannot be done unless these are taken into account.

7.6.1.2 The second objective of the requirements of this subclause is to allocate a target failure measure and an associated safety integrity level to each safety function to be carried out by an E/E/PE safety-related system.

7.6.2 Requirements

7.6.2.1 The designated safety-related systems that are to be used to achieve the required functional safety shall be specified. The tolerable risk may be met by

– E/E/PE safety-related systems; and/or

– other risk reduction measures.

NOTE This standard is applicable only if the tolerable risk is met at least in part by an E/E/PE safety-related system.

7.6.2.2 In allocating overall safety functions to the designated E/E/PE safety-related systems and other risk reduction measures, the skills and resources available during all phases of the overall safety lifecycle shall be considered.

NOTE 1 The full implications of using safety-related systems employing complex technology are often underestimated. For example, the implementation of complex technology requires a higher level of competence at all phases, from specification up to operation and maintenance. The use of other, simpler, technology solutions may be equally effective and may have several advantages because of the reduced complexity.

NOTE 2 The availability of skills and resources for operation and maintenance, and the operating environment, may be critical to achieving the required functional safety in actual operation.

7.6.2.3 Each overall safety function, with its associated overall safety integrity requirement developed according to 7.5, shall be allocated to one or more of the designated E/E/PE safety-related systems and/or other risk reduction measures, so that the tolerable risk for the safety function is achieved. This allocation is iterative, and if it is found that the tolerable risk cannot be achieved, then the specifications for the EUC control system, the designated E/E/PE safety-related systems and the other risk reduction measures shall be modified and the allocation repeated.

NOTE 1 The decision to allocate a specific overall safety function across one or more E/E/PE safety-related systems or other risk reduction measures will depend on a number of factors, but particularly on its overall safety integrity requirement. The more onerous the safety integrity requirement, the more likely the function will be shared by more than one E/E/PE safety-related system and/or other risk reduction measure.

NOTE 2 Figure 6 indicates the approach to overall safety requirements allocation.

7.6.2.4 The allocation indicated in 7.6.2.3 shall be done in such a way that all overall safety functions are allocated and target failure measures are defined for each safety function (subject to the requirements specified in 7.6.2.10).

7.6.2.5 The safety integrity requirements for each safety function shall be specified in terms of either

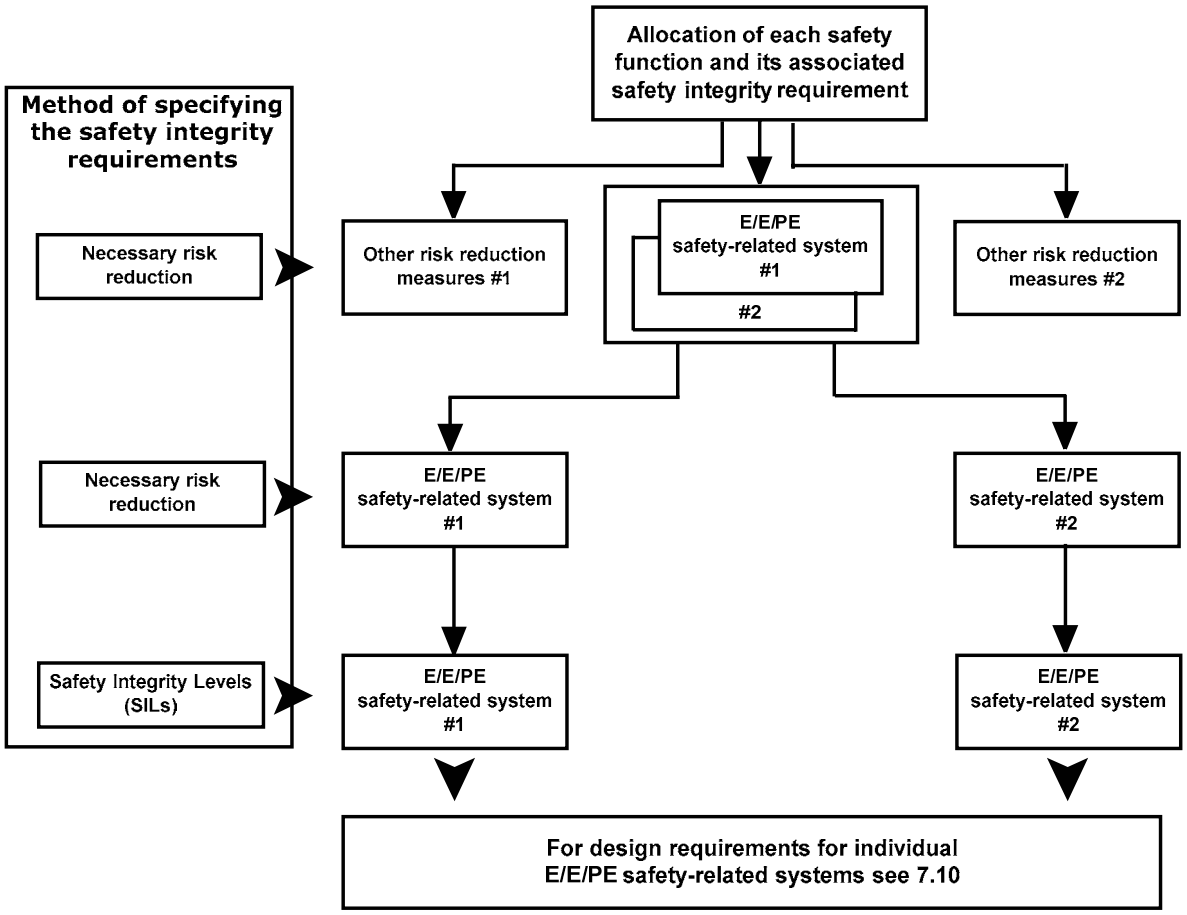
– the average probability of a dangerous failure on demand of the safety function, for a low demand mode of operation, or

– the average frequency of a dangerous failure of the safety function [h^{-1}] for a high demand or a continuous mode of operation.

7.6.2.6 The allocation of the safety integrity requirements shall be carried out using appropriate techniques for the combination of probabilities.

NOTE 1 Safety requirements allocation may be carried out in a qualitative and/or quantitative manner.

NOTE 2 Where a number of E/E/PE safety related systems and/or other risk reduction measures are necessary to achieve the tolerable risk, the actual risk achieved will depend on the systemic dependencies between the E/E/PE safety related systems and/or other risk reduction measures (see A.5.4 of IEC 61508-5 for more details of dependencies and how they can be analysed).



NOTE 1 Overall safety integrity requirements are associated with each overall safety function before allocation (see 7.5.2.3).

NOTE 2 An overall safety function may be allocated across more than one safety-related system.

Figure 6 – Allocation of overall safety requirements to E/E/PE safety-related systems and other risk reduction measures

7.6.2.7 The allocation shall proceed taking into account the possibility of common cause failures. If the EUC control system, E/E/PE safety-related systems and other risk reduction measures are to be treated as independent for the allocation, they shall:

– be independent such that the likelihood of simultaneous failures between two or more of these different systems or measures is sufficiently low in relation to the required safety integrity;

– be functionally diverse (i.e. use totally different approaches to achieve the same results);

– be based on diverse technologies (i.e. use different types of equipment to achieve the same results);

NOTE 1 It is recognised that, however diverse the technology, in the case of high safety integrity systems with particularly severe consequences in the event of failure, special precautions will have to be taken against low probability common cause events, for example aircraft crashes and earthquakes.

– not share common parts, services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;

– not share common operational, maintenance or test procedures.

NOTE 2 This standard is specifically concerned with the implementation of the safety requirements allocated to the E/E/PE safety-related systems, and requirements are specified as to how this shall be done. The implementation of safety requirements allocated to other risk reduction measures is therefore not considered in detail in this standard.

Within common cause analysis, limiting and constraint conditions for the realisation of E/E/PE safety-related systems such as the aspect of necessary separation of different channels of an E/E/PE system, subsystem or element, for example by space, shall be checked – this may not allow for example for two channels/microprocessors on one board or for on-chip redundancy (see IEC 61508-2, Annex E).

7.6.2.8 If not all of the requirements in 7.6.2.7 can be met then the E/E/PE safety-related systems and the other risk reduction measures shall not be treated as independent for the purposes of the safety allocation. Instead, the allocation shall take into account relevant common cause failures between the EUC control system, the E/E/PE safety-related systems and the other risk reduction measures.

NOTE 1 For further information on analysing dependent failures see references [13] and [14] in the Bibliography.

NOTE 2 Sufficient independence is established by showing that the probability of a dependent failure is sufficiently low for the E/E/PE safety-related systems in comparison with the overall safety integrity requirements (see 7.6.2.7).

NOTE 3 As indicated in 7.6.2.3, the allocation is iterative and, if an analysis that includes common cause failures indicates that the tolerable risk cannot be achieved based on initial assumptions, then design changes will be needed (for further guidance see A.5.4 of IEC 61508-5).

7.6.2.9 When the allocation has sufficiently progressed, the safety integrity requirements, for each safety function allocated to the E/E/PE safety-related system(s), shall be specified in terms of the safety integrity level in accordance with Table 2 or Table 3 and shall indicate whether the target failure measure is, either:

– the average probability of dangerous failure on demand of the safety function, (PFD_{avg}), for a low demand mode of operation (Table 2), or

– the average frequency of a dangerous failure of the safety function [h^{-1}], (PFH), for a high demand mode of operation (Table 3), or

– the average frequency of a dangerous failure of the safety function [h^{-1}], (PFH), for a continuous mode of operation (Table 3).

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE 1 See 3.5.16 of IEC 61508-4 for definitions of the terms: “low demand mode of operation”, “high demand mode of operation” and “continuous mode of operation”.

NOTE 2 See IEC 61508-5 for guidance on modes of operation relating the target failure measures to the hazard and risk analysis.

NOTE 3 Tables 2 and 3 relate the target failure measures, as allocated to a safety function carried out by an E/E/PE safety-related system, to the safety integrity level. It is accepted that it will not be possible to predict quantitatively the safety integrity of all aspects of E/E/PE safety-related systems. Qualitative techniques, measures and judgements will have to be made with respect to the precautions considered necessary to ensure that the target failure measures are achieved. This is particularly true in the case of systematic safety integrity (see 3.5.6 of IEC 61508-4) where qualitative techniques and judgements have to be made with respect to the precautions considered necessary to achieve the required systematic safety integrity, for the specified safety integrity level (see IEC 61508-2, 7.4.2.2 c), 7.4.3, 7.4.6, 7.4.7 and IEC 61508-3).

NOTE 4 For hardware safety integrity it is necessary to apply quantified reliability estimation techniques in order to assess whether the target safety integrity, as determined by the risk assessment, has been achieved, taking into account random hardware failures (see IEC 61508-2, 7.4.5).

NOTE 5 When the safety integrity level has been determined using a qualitative method (for example a qualitative risk graph), either Table 2 or Table 3, as appropriate, gives the quantitative failure measures that set the limits for hardware safety integrity.

NOTE 6 The safety integrity that can be claimed when two or more E/E/PE safety-related systems are used may be better than that indicated in Table 2 providing that adequate levels of independence are achieved. For example, this would be relevant if the specified safety function was to carried out by two E/E/PE safety-related systems where adequate levels of independence between the two E/E/PE safety-related systems had been achieved.

NOTE 7 For an E/E/PE safety-related system operating in high demand or continuous mode of operation which is required to operate for a defined mission time during which no repair can take place, the required safety integrity level for a safety function can be derived as follows. Determine the required probability of failure of the safety function during the mission time and divide this by the mission time, to give a required frequency of failure per hour, then use Table 3 to derive the required safety integrity level.

7.6.2.10 For an E/E/PE safety-related system that implements safety functions of different safety integrity levels, unless it can be shown there is sufficient independence of implementation between these particular safety functions, those parts of the safety-related hardware and software where there is insufficient independence of implementation shall be treated as belonging to the safety function with the highest safety integrity level. Therefore, the requirements applicable to the highest relevant safety integrity level shall apply to all those parts.

NOTE See also IEC 61508-2, 7.4.2.4 and IEC 61508-3, 7.4.2.8.

7.6.2.11 In cases where the allocation process results in the requirement for an E/E/PE safety-related system implementing a SIL 4 safety function then the following shall apply:

a) There shall be a reconsideration of the application to determine if any of the risk parameters can be modified so that the requirement for a SIL 4 safety function is avoided. The review shall consider whether:

- additional safety-related systems or other risk reduction measures, not based on E/E/PE safety-related systems, could be introduced;
- the severity of the consequence could be reduced;
- the likelihood of the specified consequence could be reduced.

b) If after further consideration of the application, it is decided to implement the SIL 4 safety function then a further risk assessment shall be carried out using a quantitative method that takes into consideration potential common cause failures between the E/E/PE safety-related system and:
   - any other systems whose failure would place a demand on it; and,
   - any other safety-related systems.

7.6.2.12 No single safety function in an E/E/PE safety-related system shall be allocated a target safety integrity lower than specified in Tables 2 and 3. That is, for 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 the safety function 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 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.

7.6.2.13 The information and results of the overall safety requirements allocation acquired in 7.6.2.1 to 7.6.2.12, together with any assumptions and justifications made (including assumptions concerning the other risk reduction measures that need to be managed throughout the life of the EUC), shall be documented.

NOTE For each E/E/PE safety-related system, there should be sufficient information on the safety functions and their associated safety integrity levels. This information will form the basis of the safety requirements for the E/E/PE safety-related systems specified in 7.10.

7.7 Overall operation and maintenance planning

NOTE 1 This phase is Box 6 of Figure 2.

NOTE 2 An example of an operation and maintenance activities model is shown in Figure 7 hereinafter.

NOTE 3 An example of an operations and maintenance management model is shown in Figure 8 hereinafter.

NOTE 4 The requirements of 7.7.2 are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 5 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.7.1 Objective

The objective of the requirements of this subclause is to develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.

7.7.2 Requirements

7.7.2.1 A plan shall be prepared that shall specify the following:

a) the routine actions that need to be carried out to maintain the required functional safety of the E/E/PE safety-related systems;

b) the actions and constraints that are necessary (for example during start-up, normal operation, routine testing, foreseeable disturbances, faults and shutdown) to prevent an

unsafe state, to reduce the demands on the E/E/PE safety-related system, or reduce the consequences of the harmful events;

NOTE 1 The following constraints, conditions and actions are relevant to E/E/PE safety-related systems:

1) constraints on the EUC operation during a fault of the E/E/PE safety-related systems;
2) constraints on the EUC operation during maintenance of the E/E/PE safety-related systems;
3) when constraints on the EUC operation may be removed;
4) the procedures for returning to normal operation;
5) the procedures for confirming that normal operation has been achieved;
6) the circumstances under which the safety functions implemented by the E/E/PE safety-related system may be by-passed for start-up, for special operation or for testing;
7) the procedures to be followed before, during and after by-passing E/E/PE safety-related systems, including permit to work procedures and authority levels.

c) the documentation that needs to be maintained showing results of functional safety audits and tests;

d) the documentation that needs to be maintained on all hazardous events and all incidents with the potential to create a hazardous event;

e) the scope of the maintenance activities (as distinct from the modification activities);

f) the actions to be taken in the event of hazardous events occurring;

g) the contents of the chronological documentation of operation and maintenance activities (see 7.15).

NOTE 2 The majority of E/E/PE safety-related systems have some failure modes that can be revealed only by testing during routine maintenance. In such cases, if testing is not carried out at sufficient frequency, the safety integrity requirements for the E/E/PE safety-related system will not be achieved.

NOTE 3 This subclause applies to a supplier of software who is required to provide information and procedures with the software product that will allow the user to ensure the required functional safety during the operation and maintenance of a safety-related system. This includes preparing procedures for any software modification that could come about as a consequence of an operational or maintenance requirement (see also 7.6 of IEC 61508-3). Implementing these procedures is covered by 7.8 of IEC 61508-3. Preparing procedures for future software changes that will come about as a consequence of a modification requirement for a safety-related system are dealt with in 7.6 of IEC 61508-3. Implementing those procedures is covered by 7.8 of IEC 61508-2.

NOTE 4 Account should be taken of the operation and maintenance procedures developed to meet the requirements in IEC 61508-2 and IEC 61508-3.

7.7.2.2 The plan shall ensure, that if any subsystem of an E/E/PE safety related system with a hardware fault tolerance of zero is taken off-line for testing, the continuing safety of the EUC shall be maintained by additional measures and constraints. The safety integrity provided by the additional measures and constraints shall be at least equal to the safety integrity provided by the E/E/PE safety-related system during normal operation. In the case of any subsystem of an E/E/PE safety related system with a hardware fault tolerance greater than zero then at least one channel of the E/E/PE safety-related system shall remain in operation during testing and the testing shall be completed within the MTTR assumed in the calculations carried out to determine compliance with the target failure measure.

NOTE For hardware fault tolerance see; 7.4.4.1 of IEC 61508-2.

7.7.2.3 The routine maintenance activities that are carried out to detect unrevealed faults shall be determined by a systematic analysis.

NOTE If unrevealed faults are not detected, they may

a) in the case of E/E/PE safety-related systems or other risk reduction measures, lead to a failure to operate on demand;

b) in the case of non-safety-related systems, lead to demands on the E/E/PE safety-related systems or other risk reduction measures.

7.7.2.4 The plan for maintaining the E/E/PE safety-related systems shall be agreed upon with those responsible for the operation and maintenance of

– the E/E/PE safety-related systems;
– the other risk reduction measures; and
– the non-safety-related systems that have the potential to place demands on the E/E/PE safety-related systems or other risk reduction measures.

7.8 Overall safety validation planning

NOTE 1 This phase is Box 7 of Figure 2.

NOTE 2 The requirements of this subclause are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 3 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.8.1 Objective

The objective of the requirements of this subclause is to develop a plan for the overall safety validation of the E/E/PE safety-related systems

7.8.2 Requirements

7.8.2.1 A plan shall be developed that shall include the following:

a) details of when the validation shall take place;
b) details of those who shall carry out the validation;
c) specification of the relevant modes of the EUC operation with their relationship to the E/E/PE safety-related system, including where applicable
   – preparation for use, including setting and adjustment;
   – start up;
   – teach;
   – automatic;
   – manual;
   – semi-automatic;
   – steady state of operation;
   – re-setting;
   – shut down;
   – maintenance;
   – reasonably foreseeable abnormal conditions;
d) specification of the E/E/PE safety-related systems that need to be validated for each mode of EUC operation before commissioning commences;
e) the technical strategy for the validation (for example analytical methods, statistical tests, etc.);
f) the measures, techniques and procedures that shall be used for confirming that the allocation of safety functions has been carried out correctly; this shall include confirmation that each safety function conforms
   – with the specification for the overall safety functions requirements, and
   – to the specification for the overall safety integrity requirements;
g) specific reference to each element contained in the outputs from 7.5 and 7.6;
h) the required environment in which the validation activities are to take place (for example, for tests this would include calibrated tools and equipment);
i) the pass and fail criteria;

j) the policies and procedures for evaluating the results of the validation, particularly failures.

NOTE In planning the overall validation, account should be taken of the work planned for E/E/PE system safety validation and software safety validation as required by IEC 61508-2 and IEC 61508-3. It is important to ensure that all the interactions between two or more E/E/PE safety-related systems and/or other risk reduction measures are considered and that all safety functions (as specified in the outputs of 7.5) have been achieved.

7.8.2.2 The information from 7.8.2.1 shall be documented and shall constitute the plan for the overall safety validation of the E/E/PE safety-related systems.

7.9 Overall installation and commissioning planning

NOTE 1 This phase is Box 8 of Figure 2.

NOTE 2 The requirements of this subclause are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 3 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.9.1 Objectives

7.9.1.1 The first objective of the requirements of this subclause is to develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved.

7.9.1.2 The second objective of the requirements of this subclause is to develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved.

7.9.2 Requirements

7.9.2.1 A plan for the installation of the E/E/PE safety-related systems shall be developed, specifying

a) the installation schedule;

b) those responsible for different parts of the installation;

c) the procedures for the installation;

d) the sequence in which the various elements are integrated;

e) the criteria for declaring all or parts of the E/E/PE safety-related systems ready for installation and for declaring installation activities complete;

f) procedures for the resolution of failures and incompatibilities.

7.9.2.2 A plan for the commissioning of the E/E/PE safety-related systems shall be developed, specifying:

a) the commissioning schedule;

b) those responsible for different parts of the commissioning;

c) the procedures for the commissioning;

d) the relationships to the different steps in the installation;

e) the relationships to the validation.

7.9.2.3 The overall installation and commissioning planning shall be documented.

7.10 E/E/PE system safety requirements specification

NOTE This phase is Box 9 of Figure 2.

7.10.1 Objective

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

7.10.2 Requirements

7.10.2.1 The E/E/PE system safety requirements specification shall be derived from the allocation of safety requirements specified in 7.6 together with all relevant information related to the application. This information shall be made available to the E/E/PE safety-related system developer.

7.10.2.2 The E/E/PE system safety requirements specification shall contain requirements for the safety functions and their associated safety integrity levels.

NOTE The objective is to describe, in terms not specific to the equipment, the safety functions and their required functional safety performance. The specification can then be verified against the outputs of the overall safety requirements and the overall safety requirements allocation phases, and used as a basis of the realisation of the E/E/PE system (see 7.2 of IEC 61508-2). Equipment designers can use the specification as a basis for selecting the equipment and architecture.

7.10.2.3 The E/E/PE system safety requirements specification shall be made available to the developer of the E/E/PE safety-related system.

7.10.2.4 The E/E/PE system safety requirements specification shall be expressed and structured in such a way that it

a) is clear, precise, unambiguous, verifiable, testable, maintainable and feasible;
b) is written to aid comprehension by those who are likely to utilise the information at any stage of the E/E/PE system safety lifecycle;
c) is expressed in natural or formal language and/or logic, sequence or cause and effect diagrams that define the necessary safety functions with each safety function being individually defined.

7.10.2.5 The specification of the E/E/PE system safety requirements shall contain the requirements for the E/E/PE system safety functions (see 7.10.2.6) and the requirements for E/E/PE system safety integrity (see 7.10.2.7).

7.10.2.6 The E/E/PE system safety functions requirements specification shall contain:

a) a description of all the safety functions necessary to achieve the required functional safety, which shall, for each safety function,
   – provide comprehensive detailed requirements sufficient for the design and development of the E/E/PE safety-related systems,
   – include the manner in which the E/E/PE safety-related systems are intended to achieve or maintain a safe state for the EUC,
   – specify whether or not continuous control is required, and for what periods, in achieving or maintaining a safe state of the EUC, and
   – specify whether the safety function is applicable to E/E/PE safety-related systems operating in low demand, high demand or continuous modes of operation;
b) response time performance (i.e. the time within which it is necessary for the safety function to be completed);
c) E/E/PE safety-related system and operator interfaces that are necessary to achieve the required functional safety;
d) all information relevant to functional safety that may have an influence on the E/E/PE safety-related system design;

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

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

- preparation for use including setting and adjustment,
- start-up, teach, automatic, manual, semi-automatic, steady state of operation,
- steady state of non-operation, re-setting, shut-down, maintenance,
- reasonably foreseeable abnormal conditions;

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

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

7.10.2.7 The E/E/PE system safety integrity requirements specification shall contain:

a) the safety integrity level for each safety function and, when required, a specified value for the target failure measure;

NOTE 1 The specified value for the target failure measure can be derived using a quantitative method (see 7.5.2.3). Alternatively, when the safety integrity requirement has been developed using a qualitative method and expressed as a safety integrity level, then the target failure measure is derived from Table 2 or 3, as appropriate, according to the safety integrity level. In this case the specified target failure measure is the smallest average probability of failure or failure rate for the safety integrity level, unless a different value has been used to calibrate the method.

NOTE 2 In the case of a safety function operating in the low demand mode of operation, the target failure measure will be expressed in terms of the average probability of dangerous failure on demand, as determined by the safety integrity level of the safety function (see Table 2), unless there is a requirement in the E/E/PE system safety integrity requirements specification for the safety function to meet a specific target failure measure, rather than a specific safety integrity level. For example, when a target failure measure of $1{,}5 \times 10^{-2}$ (average probability of dangerous failure on demand) is specified in order to meet the required tolerable risk, then the average probability of dangerous failure on demand of the safety function due to random hardware failures will need to be equal to or less than $1{,}5 \times 10^{-2}$.

NOTE 3 In the case of a safety function operating in the high demand or the continuous mode of operation, the target failure measure will be expressed in terms of the average frequency of a dangerous failure [h^{-1}], as determined by the safety integrity level of the safety function (see Table 3), unless there is a requirement in the E/E/PE system safety integrity requirements specification for the safety function to meet a specific target failure measure, rather than a specific safety integrity level. For example, when a target failure measure of $1{,}5 \times 10^{-6}$ (average frequency of a dangerous failure [h^{-1}]) is specified in order to meet the required tolerable risk, then the average frequency of a dangerous failure of the safety function due to random hardware failures will need to be equal to or less than $1{,}5 \times 10^{-6}$ [h^{-1}].

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

c) the required duty cycle and lifetime;

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

NOTE 4 In developing the E/E/PE system safety requirements specification, the application in which the E/E/PE safety-related systems are to be used should be taken into consideration. This is particularly important for maintenance, where the specified proof test interval should not be less than can be reasonably expected for the particular application. For example, the time between services that can be realistically attained for mass-produced items used by the public is likely to be greater than in a more controlled application.

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

f) the electromagnetic immunity limits that are required to achieve functional safety. These limits should be derived taking into account both the electromagnetic environment and the required safety integrity levels (see IEC/TS 61000-1-2);

NOTE 5 Due to the nature and physics of electromagnetic phenomena no simple, evident and provable correlation can be established between the required immunity level and safety integrity level for nearly all cases of electromagnetic phenomena. Specifying effective immunity levels solely according to the required SIL is therefore not possible and reasonable in those cases. Alternative approaches may be used which, to some degree, specify

the required immunity level according to the required SIL but also involve special test arrangements or test performance criteria. See IEC/TS 61000-1-2.

NOTE 6 See also reference [15] in the Bibliography.

g) limiting and constraint conditions for the realisation of E/E/PE safety-related systems due to the possibility of common cause failures (see 7.6.2.7).

7.11 E/E/PE safety-related systems – realisation

NOTE This phase is Box 10 of Figure 2 and Boxes 10.1 to 10.6 of Figures 3 and 4.

7.11.1 Objective

The objective of the requirements of this subclause is to create E/E/PE safety-related systems conforming to the specification for the E/E/PE system safety requirements (comprising the specification for the E/E/PE system safety functions requirements and the specification for the E/E/PE system safety integrity requirements). (See IEC 61508-2 and IEC 61508-3).

7.11.2 Requirements

The requirements that shall be met are contained in IEC 61508-2 and IEC 61508-3.

7.12 Other risk reduction measures – specification and realisation

NOTE This phase is Box 11 of Figure 2.

7.12.1 Objective

The objective of the requirements of this subclause is to create other risk reduction measures to meet the safety functions requirements and safety integrity requirements specified for such systems.

7.12.2 Requirements

The specification to meet the safety functions requirements and safety integrity requirements for other risk reduction measures is not covered in this standard.

NOTE Other risk reduction measures are based on a technology other than electrical/electronic/programmable electronic (for example hydraulic, pneumatic etc.) or may be physical structures (for example a drain system, a fire wall or a bund). They have been included in the overall safety lifecycle to ensure that the risk reduction from E/E/PE safety related systems is determined in the context of the risk reduction from other risk reduction measures.

7.13 Overall installation and commissioning

NOTE 1 This phase is Box 12 of Figure 2.

NOTE 2 The requirements of this subclause are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 3 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.13.1 Objectives

7.13.1.1 The first objective of the requirements of this subclause is to install the E/E/PE safety-related systems.

7.13.1.2 The second objective of the requirements of this subclause is to commission the E/E/PE safety-related systems.

7.13.2 Requirements

7.13.2.1 Installation activities shall be carried out in accordance with the plan for the installation of the E/E/PE safety-related systems (see 7.9).

7.13.2.2 The information documented during installation shall include

– documentation of installation activities;
– resolution of failures and incompatibilities.

7.13.2.3 Commissioning activities shall be carried out in accordance with the plan for the commissioning of the E/E/PE safety-related systems.

7.13.2.4 The information documented during commissioning shall include

– documentation of commissioning activities;
– references to failure reports;
– resolution of failures and incompatibilities.

7.14 Overall safety validation

NOTE 1 This phase is Box 13 of Figure 2.

NOTE 2 The requirements of this subclause are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 3 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.14.1 Objective

The objective of the requirements of this subclause is to validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.

7.14.2 Requirements

7.14.2.1 Validation activities shall be carried out in accordance with the overall safety validation plan for the E/E/PE safety-related systems (see 7.8).

7.14.2.2 All equipment used for quantitative measurements as part of the validation activities shall be calibrated against a specification traceable to a national standard or to the vendor specification.

7.14.2.3 The information documented during validation shall include

– documentation in chronological form of the validation activities;
– the version of the specification for the overall safety requirements being used;
– the safety function being validated (by test or by analysis);
– tools and equipment used, along with calibration data;
– the results of the validation activities;
– configuration identification of the item under test, the procedures applied and the test environment;
– discrepancies between expected and actual results.

7.14.2.4 When discrepancies occur between expected and actual results, the analysis made, and the decisions taken on whether to continue the validation or issue a change request and return to an earlier part of the validation, shall be documented.

7.15 Overall operation, maintenance and repair

NOTE 1 This phase is Box 14 of Figure 2.

NOTE 2 The organizational measures dealt with in this subclause 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.

NOTE 3 The functional safety requirements during the maintenance and repair activities may be different from those required during operation.

NOTE 4 It should not be assumed that test procedures developed for initial installation and commissioning can be used without checking their validity and practicability in the context of on-line EUC operations.

NOTE 5 The requirements of this subclause are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 6 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.15.1 Objective

7.15.1.1 The first objective of the requirements of this subclause is to ensure the functional safety of the E/E/PE safety-related systems is maintained to the specified level.

7.15.1.2 The second objective of the requirements of this subclause is to ensure that the technical requirements, necessary for the overall operation, maintenance and repair of the E/E/PE safety-related systems, are specified and provided to those responsible for the future operation and maintenance of the E/E/PE safety-related systems.

7.15.2 Requirements

7.15.2.1 The following shall be implemented:

– the plan for operating and maintaining the E/E/PE safety-related systems (see 7.7);
– the operation, maintenance and repair procedures for the E/E/PE safety-related systems.

7.15.2.2 Implementation of the items specified in 7.15.2.1 shall include initiation of the following actions:

– the implementation of procedures;
– the following of maintenance schedules;
– the maintaining of documentation;
– the carrying out, periodically, of functional safety audits (see 6.2.7);
– the documenting of modifications that have been made to the E/E/PE safety-related systems.

NOTE 1 An example of an operation and maintenance activities model is shown in Figure 7.

NOTE 2 An example of an operations and maintenance management model is shown in Figure 8.

7.15.2.3 Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems shall be maintained which shall contain the following information:

– the results of functional safety audits and tests;

– documentation of the time and cause of demands on the E/E/PE safety-related systems (in actual operation), together with the performance of the E/E/PE safety-related systems when subject to those demands, and the faults found during routine maintenance;

– documentation of modifications that have been made to the EUC, to the EUC control system and to the E/E/PE safety-related systems.

7.15.2.4 The exact requirements for chronological documentation will be dependent on the specific product or application and shall, where relevant, be detailed in product and application sector international standards.

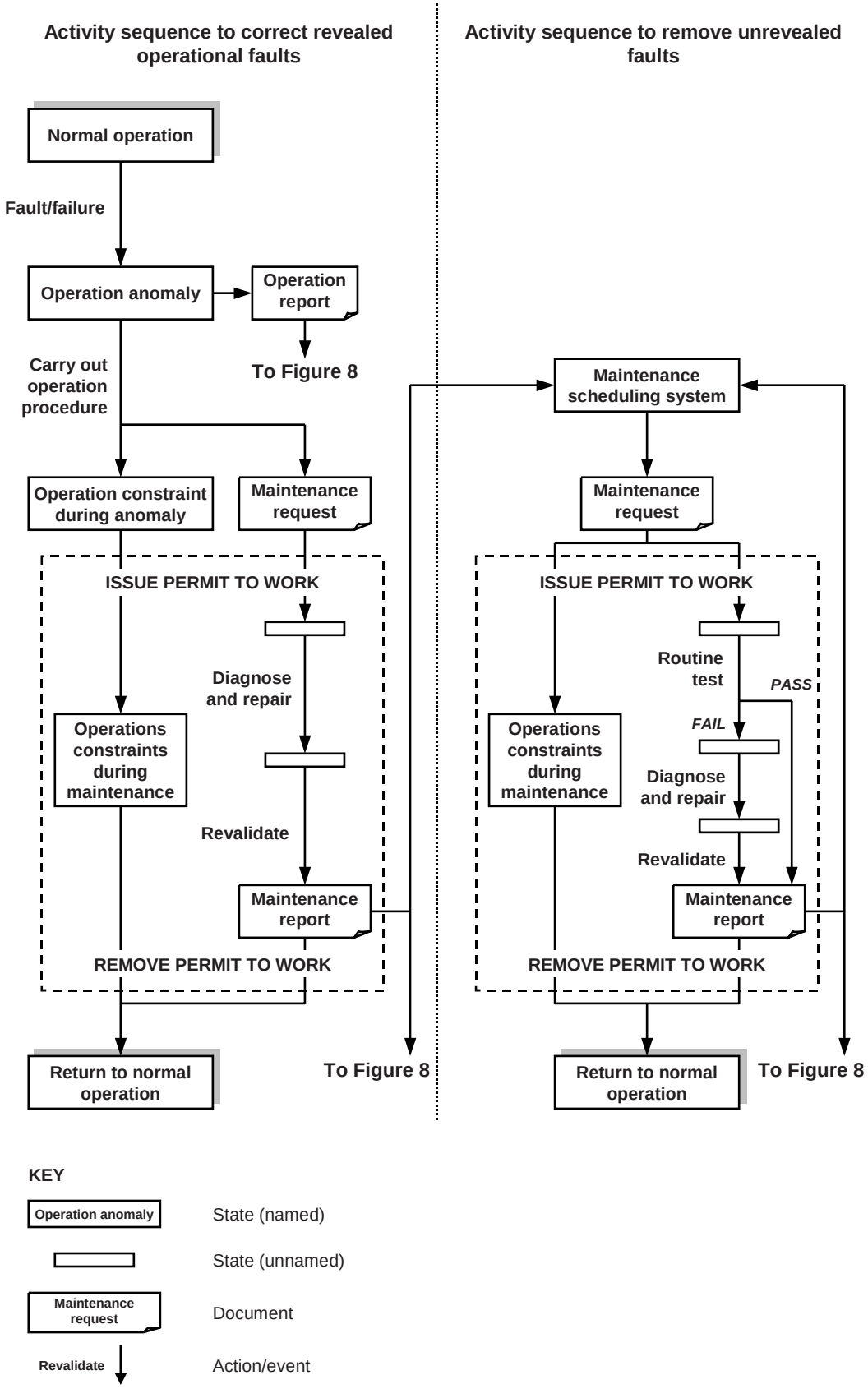


Figure 7 – Example of operations and maintenance activities model

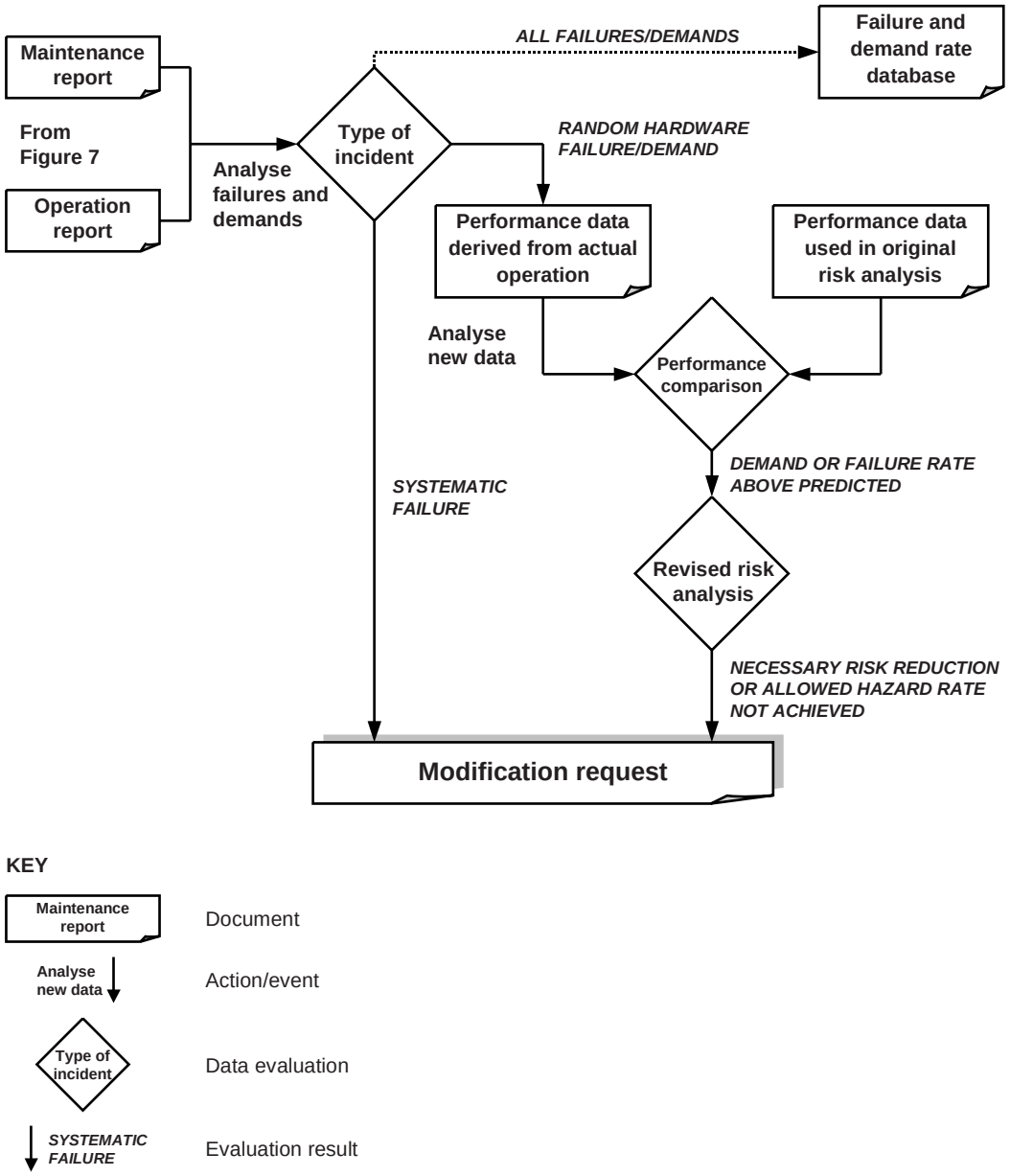


Figure 8 – Example of operation and maintenance management model

7.16 Overall modification and retrofit

NOTE 1 This phase is Box 15 of Figure 2.

NOTE 2 The organizational measures dealt with in this subclause 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.

NOTE 3 The requirements of this subclause are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 4 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.16.1 Objective

The objective of the requirements of this subclause is to define the procedures that are necessary to ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.

7.16.2 Requirements

7.16.2.1 Prior to carrying out any modification or retrofit activity, procedures shall be planned (see 6.2.8).

NOTE An example of a modification procedure model is shown in Figure 9.

7.16.2.2 The modification and retrofit phase shall be initiated only by the issue of an authorized request under the procedures for the management of functional safety (see 6.2.8). The request shall detail the following:

– the determined hazards that may be affected;
– the proposed change (both hardware and software);
– the reasons for the change.

NOTE The reason for the request for the modification could arise from, for example:

a) functional safety below that specified;
b) systematic fault experience;
c) new or amended safety legislation;
d) modifications to the EUC or its use;
e) modification to the overall safety requirements;
f) analysis of operations and maintenance performance, indicating that the performance is below target;
g) routine functional safety audits.

7.16.2.3 An impact analysis shall be carried out that shall include an assessment of the impact of the proposed modification or retrofit activity on the functional safety of any E/E/PE safety-related system. The assessment shall include a hazard and risk analysis sufficient to determine the breadth and depth to which subsequent overall, E/E/PE system or software safety lifecycle phases will need to be undertaken. The assessment shall also consider the impact of other concurrent modification or retrofit activities, and shall also consider the functional safety both during and after the modification and retrofit activities have taken place.

7.16.2.4 The results described in 7.16.2.3 shall be documented.

7.16.2.5 Authorization to carry out the required modification or retrofit activity shall be dependent on the results of the impact analysis.

7.16.2.6 All modifications that have an impact on the functional safety of any E/E/PE safety-related system shall initiate a return to an appropriate phase of the overall, E/E/PE system or software safety lifecycles. All subsequent phases shall then be carried out in accordance with the procedures specified for the specific phases in accordance with the requirements in this standard.

NOTE 1 It may be necessary to implement a full hazard and risk analysis which may generate a need for safety integrity levels that are different to those currently specified for the safety functions implemented by the E/E/PE safety-related systems.

NOTE 2 It should not be assumed that test procedures developed for initial installation and commissioning can be used without checking their validity and practicability in the context of on-line EUC operations.

7.16.2.7 Chronological documentation shall be established and maintained that shall document details of all modifications and retrofits, and shall include references to:

– the modification or retrofit request;
– the impact analysis;
– reverification and revalidation of data and results;
– all documents affected by the modification and retrofit activity.

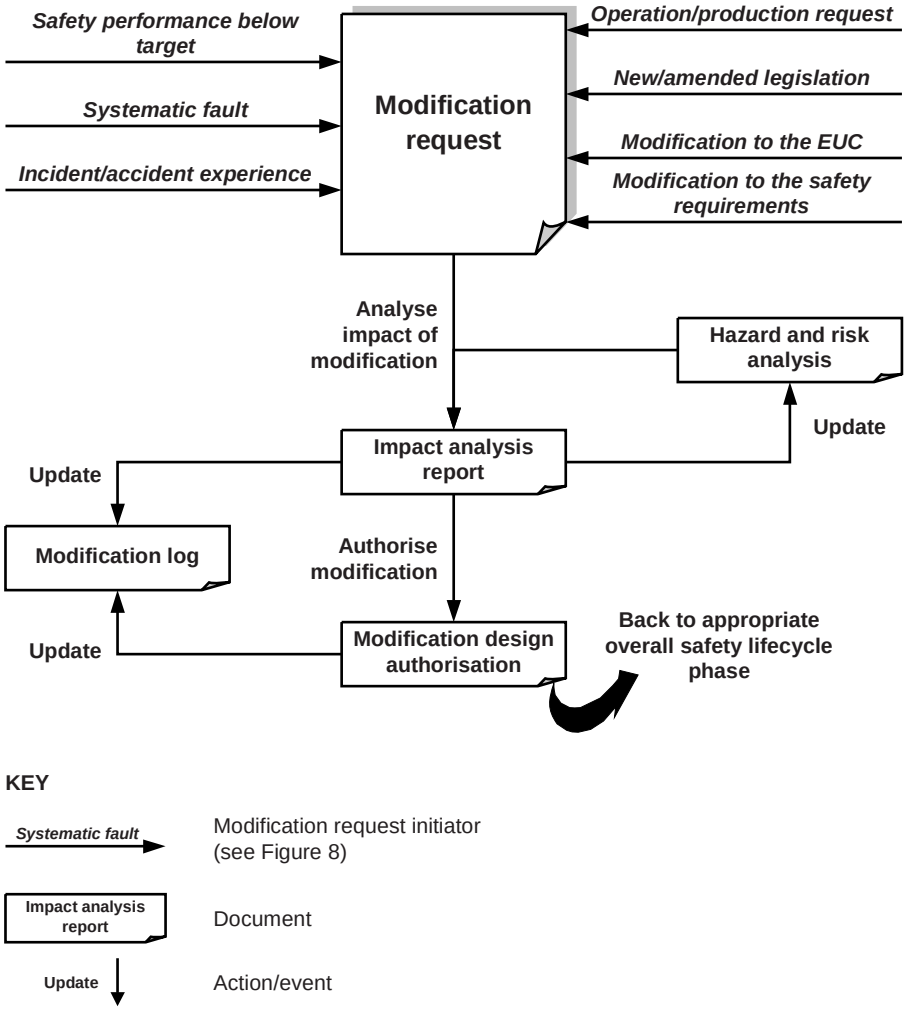


Figure 9 – Example of modification procedure model

7.17 Decommissioning or disposal

NOTE 1 This phase is Box 16 of Figure 2.

NOTE 2 The requirements of this subclause are specific to E/E/PE safety-related systems. They should be considered in the context of the other risk reduction measures, taking particular account of assumptions already made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

NOTE 3 In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures.

7.17.1 Objective

The objective of the requirements of this subclause is to define the procedures that are necessary to ensure that the functional safety for the E/E/PE safety-related systems is appropriate for the circumstances during and after the activities of decommissioning or disposing of the EUC.

7.17.2 Requirements

7.17.2.1 Prior to any decommissioning or disposal activity, an impact analysis shall be carried out that shall include an assessment of the impact of the proposed decommissioning or disposal activity on the functional safety of any E/E/PE safety-related system associated with the EUC. The impact analysis shall also consider adjacent EUCs and the impact on their E/E/PE safety-related systems. The assessment shall include a hazard and risk analysis sufficient to determine the necessary breadth and depth of subsequent overall, E/E/PE system or software safety lifecycle phases.

7.17.2.2 The results described in 7.17.2.1 shall be documented.

7.17.2.3 The decommissioning or disposal phase shall only be initiated by the issue of an authorized request under the procedures for the management of functional safety (see Clause 6).

7.17.2.4 Authorization to carry out the required decommissioning or disposal shall be dependent on the results of the impact analysis.

7.17.2.5 Prior to decommissioning or disposal taking place a plan shall be prepared that shall include procedures for:

– the closing down of the E/E/PE safety-related systems;
– dismantling the E/E/PE safety-related systems.

7.17.2.6 If any decommissioning or disposal activity has an impact on the functional safety of any E/E/PE safety-related system, this shall initiate a return to the appropriate phase of the overall, E/E/PE system or software safety lifecycles. All subsequent phases shall then be carried out in accordance with the procedures specified in this standard for the safety integrity levels of the safety functions implemented by the E/E/PE safety-related systems.

NOTE 1 It may be necessary to implement a full hazard and risk analysis which may generate a need for different safety integrity levels for the safety functions implemented by the E/E/PE safety-related systems.

NOTE 2 The functional safety requirements during the decommissioning or disposal phase may be different from those required during the operational phase.

7.17.2.7 Chronological documentation shall be established and maintained that shall document details of the decommissioning or disposal activities and shall include references to:

– the plan used for the decommissioning or disposal activities;
– the impact analysis.

7.18 Verification

7.18.1 Objective

The objective of the requirements of this subclause is to demonstrate, for each phase of the overall, E/E/PE system and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.

7.18.2 Requirements

7.18.2.1 For each phase of the overall, E/E/PE system and software safety lifecycles, a plan for the verification shall be established concurrently with the development for the phase.

7.18.2.2 The verification plan shall document or refer to the criteria, techniques, tools to be used in the verification activities.

7.18.2.3 The verification shall be carried out according to the verification plan.

NOTE Selection of techniques and measures for verification, and the degree of independence for the verification activities, will depend upon a number of factors and may be specified in product and application sector international standards.

The factors could include, for example

– size of project;
– degree of complexity;
– degree of novelty of design;
– degree of novelty of technology.

7.18.2.4 Information on the verification activities shall be collected and documented as evidence that the phase being verified has, in all respects, been satisfactorily completed.

8 Functional safety assessment

8.1 Objective

The objective of the requirements of this clause is to specify the activities necessary to investigate and arrive at a judgement on the adequacy of the functional safety achieved by the E/E/PE safety-related system(s) or compliant items (e.g. elements/subsystems)based on compliance with the relevant clauses of this standard.

8.2 Requirements

8.2.1 One or more persons shall be appointed to carry out one or more functional safety assessments in order to arrive at a judgement on the adequacy of:

– the functional safety achieved by the E/E/PE safety-related systems, within their particular environment, in respect to the relevant clauses of this standard;

– the compliance to the relevant clauses of this standard, achieved in the case of elements/subsystems.

8.2.2 Those carrying out a functional safety assessment shall have access to all persons involved in any overall, E/E/PE system or software safety lifecycle activity and all relevant information and equipment (both hardware and software).

NOTE It is recognised that access to those persons who where previously involved in a safety lifecycle phase may not be achievable and in such a case reliance has necessarily to be placed on those persons currently having relevant responsibilities.

8.2.3 A functional safety assessment shall be applied to all phases throughout the overall, E/E/PE system and software safety lifecycles, including documentation, verification and management of functional safety.

8.2.4 Those carrying out a functional safety assessment shall consider the activities carried out and the outputs obtained during each phase of the overall, E/E/PE system and software safety lifecycles and judge whether adequate functional safety has been achieved based on the objectives and requirements in this standard.

8.2.5 All relevant claims of compliance made by suppliers and other parties responsible for achieving functional safety shall be included in the functional safety assessment.

NOTE Such claims may be made for an operational system or for the contribution to functional safety of activities and/or equipment in each phase of the overall, E/E/PE system and software safety lifecycles.

8.2.6 A functional safety assessment may be carried out after each phase of the overall, E/E/PE system and software safety lifecycles, or after a number of safety lifecycle phases, subject to the overriding requirement that a functional safety assessment shall be undertaken prior to the determined hazards being present.

8.2.7 A functional safety assessment shall include assessment of the evidence that functional safety audit(s) have been carried out (either full or partial) relevant to its scope.

8.2.8 Each functional safety assessment shall consider at least the following:

– the work done since the previous functional safety assessment;

– the plans or strategy for implementing further functional safety assessments of the overall, E/E/PE system and software safety lifecycles;

– the recommendations of the previous functional safety assessments and the extent to which changes have been made to meet them.

8.2.9 Each functional safety assessment shall be planned. The plan shall specify all information necessary to facilitate an effective assessment, including:

– the scope of the functional safety assessment;
– the organisations involved;
– the resources required;
– those to undertake the functional safety assessment;
– the level of independence of those undertaking the functional safety assessment;
– the competence of each person involved in the functional safety assessment;
– the outputs from the functional safety assessment;
– how the functional safety assessment relates to, and shall be integrated with, other functional safety assessments where appropriate (see 6.2.1).

NOTE 1 In establishing the scope of each functional safety assessment, it will be necessary to specify the documents, and their revision status, that are to be used as inputs for each assessment activity.

NOTE 2 The plan can be made by either those responsible for functional safety assessment or those responsible for management of functional safety, or can be shared between them.

8.2.10 Prior to a functional safety assessment taking place, its plan shall be approved by those carrying it out and by those responsible for the management of functional safety.

8.2.11 At the conclusion of a functional safety assessment, those carrying out the assessment shall document, in accordance with the assessment's plans and terms of reference:

– the activities conducted;
– the findings made;
– the conclusions arrived at;
– a judgement on the adequacy of functional safety in accordance with the requirements of this standard;
– recommendations that arise from the assessment, including recommendations for acceptance, qualified acceptance or rejection.

8.2.12 The relevant outputs of the functional safety assessment of a compliant item shall be made available to those having responsibilities for any overall, E/E/PE system or software safety lifecycle activity including the designers and assessors of the E/E/PE safety-related system. The output of the assessment of the E/E/PE safety-related system shall be made available to the E/E/PE system integrator.

NOTE A compliant item is any item (e.g. an element) on which a claim is being made with respect the clauses of IEC 61508 series.

8.2.13 The output of the functional safety assessment of a compliant item shall include the following information to facilitate the re-use of the assessment results in the context of a larger system (see Annex D of IEC 61508-2; Annex D of IEC 61508-3 and 3.8.17 of IEC 61508-4).

a) the precise identification of the compliant item including the version of its hardware and software;

NOTE If the compliant item was assessed as a part of a larger system or equipment family, the precise identification of that system or equipment family should also be documented.

b) the conditions assumed during the assessment (e.g. the conditions of use of the E/E/PE safety-related system);

c) reference to the documentation evidence on which the assessment conclusion was based;

d) the procedures, methods and tools used for assessing the systematic capability along with the justification of its effectiveness;

e) the procedures, methods and tools used for assessing the hardware safety integrity together with the justification of the approach adopted and the quality of the data (e.g. the failure rate/distribution data sources);

f) the assessment results obtained in relation to the requirements of this standard and to the specification of the safety characteristics of the compliant item in its safety manual;

g) the accepted deviations to IEC 61508 requirements, with corresponding explanation and / or reference to evidence contained in documentation.

8.2.14 Those carrying out a functional safety assessment shall be competent for the activities to be undertaken, according to the requirements of 6.2.13 to 6.2.15.

8.2.15 The minimum level of independence of those carrying out a functional safety assessment shall be as specified in Tables 4 and 5. Product and application sector international standards may specify, with respect to compliance to their standards, different levels of independence to those specified in Tables 4 and 5. The tables shall be interpreted as follows:

– X: the level of independence specified is the minimum for the specified consequence (Table 4) or safety integrity level/systematic capability (Table 5). If a lower level of independence is adopted, then the rationale for using it shall be detailed.

– X1 and X2: see 8.2.16.

– Y: the level of independence specified is considered insufficient for the specified consequence (Table 4) or safety integrity level/ systematic capability (Table 5).

8.2.16 In the context of Tables 4 and 5, only cells marked X, X1, X2 or Y shall be used as a basis for determining the level of independence. For cells marked X1 or X2, either X1 or X2 is applicable (not both), depending on a number of factors specific to the application. The rationale for choosing X1 or X2 should be detailed. Factors that will make X2 more appropriate than X1 are:

– lack of previous experience with a similar design;

– greater degree of complexity;

– greater degree of novelty of design;

– greater degree of novelty of technology.

NOTE 1 Depending upon the company organization and expertise within the company, the requirement for independent persons and departments may have to be met by using an external organization. Conversely, companies that have internal organizations skilled in risk assessment and the application of safety-related systems, that are independent of and separate (by ways of management and other resources) from those responsible for the main development, may be able to use their own resources to meet the requirements for an independent organization.

NOTE 2 See 3.8.11, 3.8.12 and 3.8.13 of IEC 61508-4 for definitions of independent person, independent department, and independent organization respectively.

NOTE 3 Those carrying out a functional safety assessment should be careful in offering advice on anything within the scope of the assessment, since this could compromise their independence. It is often appropriate to give advice on aspects that could incur a judgement of inadequate safety, such as a shortfall in evidence, but it is usually inappropriate to offer advice or give recommendations for specific remedies for these or other problems.

8.2.17 In the context of Table 4, the consequence values for the specified level of independence are:

– Consequence A: minor injury (for example temporary loss of function);

– Consequence B: serious permanent injury to one or more persons, death to one person;

– Consequence C: death to several people;

– Consequence D: very many people killed.

The consequences specified in Table 4 are those that would arise in the event of failure of all the risk reduction measures including the E/E/PE safety-related systems.

8.2.18 In the context of Table 5, the minimum levels of independence shall be based on the safety function, carried out by the E/E/PE safety-related system, that has the highest safety integrity level or for elements/subsystems, the highest systematic capability, specified in terms of the safety integrity level.

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))

Minimum level of independence	Consequence (see 8.2.17)			
	A	B	C	D
Independent person	X	X1	Y	Y
Independent department		X2	X1	Y
Independent organization			X2	X
NOTE See 8.2.15, 8.2.16 and 8.2.17 for details on interpreting this table.				

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))

Minimum level of independence	Safety integrity level/Systematic capability			
	1	2	3	4
Independent person	X	X1	Y	Y
Independent department		X2	X1	Y
Independent organization			X2	X
NOTE See 8.2.15, 8.2.16 and 8.2.18 for details on interpreting this table.				

Annex A
(informative)

Example of a documentation structure

A.1 General

This annex provides an example documentation structure and method for specifying the documents for structuring the information in order to meet the requirements in Clause 5. The documentation has to contain sufficient information necessary to effectively perform

– each phase of the overall, E/E/PE system and software safety lifecycles;

– the management of functional safety (Clause 6);

– functional safety assessments (Clause 8).

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. The necessary documentation may be specified in product and application specific international standards.

The amount of information in each document may vary from a few lines to many pages, and the complete set of information may be divided and presented in many physical documents or one physical document. The physical documentation structure will again depend upon the size and complexity of the E/E/PE safety-related systems, and will take into account company procedures and the working practices of the specific product or application sector.

The example documentation structure indicated in this annex has been provided to illustrate one particular way in which the information could be structured and the way the documents could be titled. See reference [7] in the Bibliography for more details.

A document is a structured amount of information intended for human perception, that may be interchanged as a unit between users and/or systems (see reference [16] in the Bibliography). The term applies therefore not only to documents in the traditional sense, but also to concepts such as data files and database information.

In this standard, the term document is understood normally to mean information rather than physical documents, unless this is explicitly declared or understood in the context of the clause or subclause in which it is stated. Documents may be available in different forms for human presentation (for example on paper, film or any data medium to be presented on screens or displays).

The example documentation structure in this annex specifies documents in two parts:

– **document kind**;

– **activity or object**.

The document kind is defined in Bibliography reference [16] and characterizes the content of the document, for example function description or circuit diagram. The activity or object describes the scope of the content, for example pump control system.

The basic document kinds specified in this annex are

– **specification** – specifies a required function, performance or activity (for example requirements specification);

– **description** – specifies a planned or actual function, design, performance or activity (for example function description);

– **instruction** – specifies in detail the instructions as to when and how to perform certain jobs (for example operator instruction);
– **plan** – specifies the plan as to when, how and by whom specific activities shall be performed (for example maintenance plan);
– **diagram** – specifies the function by means of a diagram (symbols and lines representing signals between the symbols);
– **list** – provides information in a list form (for example code list, signal list);
– **log** – provides information on events in a chronological log form;
– **report** – describes the results of activities such as investigations, assessments, tests etc. (for example test report);
– **request** – provides a description of requested actions that have to be approved and further specified (for example maintenance request).

The basic document kind may have a prefix, such as **requirements** specification or **test** specification, which further characterizes the content.

A.2 Safety lifecycle document structure

Tables A.1, A.2 and A.3 provide an example documentation structure for structuring the information in order to meet the requirements specified in Clause 5. The tables indicate the safety lifecycle phase that is mainly associated with the documents (usually the phase in which they are developed). The names given to the documents in the tables are in accordance with the scheme outlined in A.1.

In addition to the documents listed in Tables A.1, A.2 and A.3, there may be supplementary documents giving detailed additional information or information structured for a specific purpose, for example parts lists, signal lists, cable lists, wiring tables, loop diagrams, list of variables.

NOTE Examples of such variables are values for regulators, alarm values for variables, priorities in the execution of tasks in the computer. Some of the values of the variables could be given before the delivery of the system, others could be given during commissioning or maintenance.

Table A.1 – Example of a documentation structure for information related to the overall safety lifecycle

Overall safety lifecycle phase	Information
Concept	Description (overall concept)
Overall scope definition	Description (overall scope definition)
Hazard and risk analysis	Description (hazard and risk analysis)
Overall safety requirements	Specification (overall safety requirements, comprising: overall safety functions requirements and overall safety integrity requirements)
Overall safety requirements allocation	Description (overall safety requirements allocation)
Overall operation and maintenance planning	Plan (overall operation and maintenance)
Overall safety validation planning	Plan (overall safety validation)
Overall installation and commissioning planning	Plan (overall installation); Plan (overall commissioning)
E/E/PE system safety requirements	Specification (E/E/PE system safety requirements, comprising: E/E/PE system safety functions requirements and E/E/PE system safety integrity requirements)
E/E/PE safety related system realisation	See Table A.2 and Table A.3
Overall installation and commissioning	Report (overall installation); Report (overall commissioning)
Overall safety validation	Report (overall safety validation)
Overall operation and maintenance	Log (overall operation and maintenance)
Overall modification and retrofit	Request (overall modification); Report (overall modification and retrofit impact analysis); Log (overall modification and retrofit)
Decommissioning or disposal	Report (overall decommissioning or disposal impact analysis); Plan (overall decommissioning or disposal); Log (overall decommissioning or disposal)
Concerning all phases	Plan (safety); Plan (verification); Report (verification); Plan (functional safety assessment); Report (functional safety assessment)

Table A.2 – Example of a documentation structure for information related to the E/E/PE system safety lifecycle

E/E/PE system safety lifecycle phase	Information
E/E/PE system validation planning	Plan (E/E/PE system safety validation)
E/E/PE system design and development	
E/E/PE system architecture	Description (E/E/PE system architecture design, comprising: hardware architecture and software architecture); Specification (programmable electronic integration tests); Specification (integration tests of programmable electronic and non programmable electronic hardware)
Hardware architecture	Description (hardware architecture design); Specification (hardware architecture integration tests)
Hardware module design	Specification (hardware module design); Specifications (hardware module tests)
Component construction and/or procurement	Hardware modules; Report (hardware modules tests)
Programmable electronic integration	Report (programmable electronic hardware and software integration tests) (see Table A.3)
E/E/PE system integration	Report (programmable electronic and other hardware integration tests)
E/E/PE system operation and maintenance procedures	Instruction (user); Instruction (operation and maintenance)
E/E/PE system safety validation	Report (E/E/PE system safety validation)
E/E/PE system modification	Instruction (E/E/PE system modification procedures); Request (E/E/PE system modification); Report (E/E/PE system modification impact analysis); Log (E/E/PE system modification)
Concerning all phases	Plan (E/E/PE system safety); Plan (E/E/PE system verification); Report (E/E/PE system verification); Plan (E/E/PE system functional safety assessment); Report (E/E/PE system functional safety assessment)
Concerning all relevant phases	Safety manual for compliant items

Table A.3 – Example of a documentation structure for information related to the software safety lifecycle

Software safety lifecycle phase	Information
Software safety requirements	Specification (software safety requirements, comprising: software safety functions requirements and software safety integrity requirements)
Software validation planning	Plan (software safety validation)
Software design and development	
Software architecture	Description (software architecture design) (see Table A.2 for hardware architecture design description); Specification (software architecture integration tests); Specification (programmable electronic hardware and software integration tests); Instruction (development tools and coding manual)
Software system design	Description (software system design); Specification (software system integration tests)
Software module design	Specification (software module design); Specification (software module tests)
Coding	List (source code); Report (software module tests); Report (code review)
Software module testing	Report (software module tests)
Software integration	Report (software module integration tests); Report (software system integration tests); Report (software architecture integration tests)
Programmable electronic integration	Report (programmable electronic hardware and software integration tests)
Software operation and maintenance procedures	Instruction (user); Instruction (operation and maintenance)
Software safety validation	Report (software safety validation)
Software modification	Instruction (software modification procedures); Request (software modification); Report (software modification impact analysis); Log (software modification)
Concerning all phases	Plan (software safety); Plan (software verification); Report (software verification); Plan (software functional safety assessment); Report (software functional safety assessment)
Concerning all relevant phases	Safety manual for compliant items

A.3 Physical document structure

The physical structure of the documentation is the way that the different documents are combined into documents, document sets, binders and groups of binders. The same document may occur in different sets.

For a large and complex system, the many physical documents are likely to be split into several binders. For a small, low complexity system with a limited number of physical documents, they may be combined into one binder with different tabs for the different sets of documents. Figure A.1 shows examples of combining documents into binders according to user groups.

The physical structure provides a means of selecting the documentation needed for the specific activities by the person or group of persons performing the activities. Consequently, some of the physical documents may occur in several binder sets or other media (for example computer disks).

NOTE The information required by the documents in Table A.1 may be contained within the different sets of documents shown in Figure A.1. For example, the engineering set may contain the hazard and risk analysis description and the overall safety requirements specification.

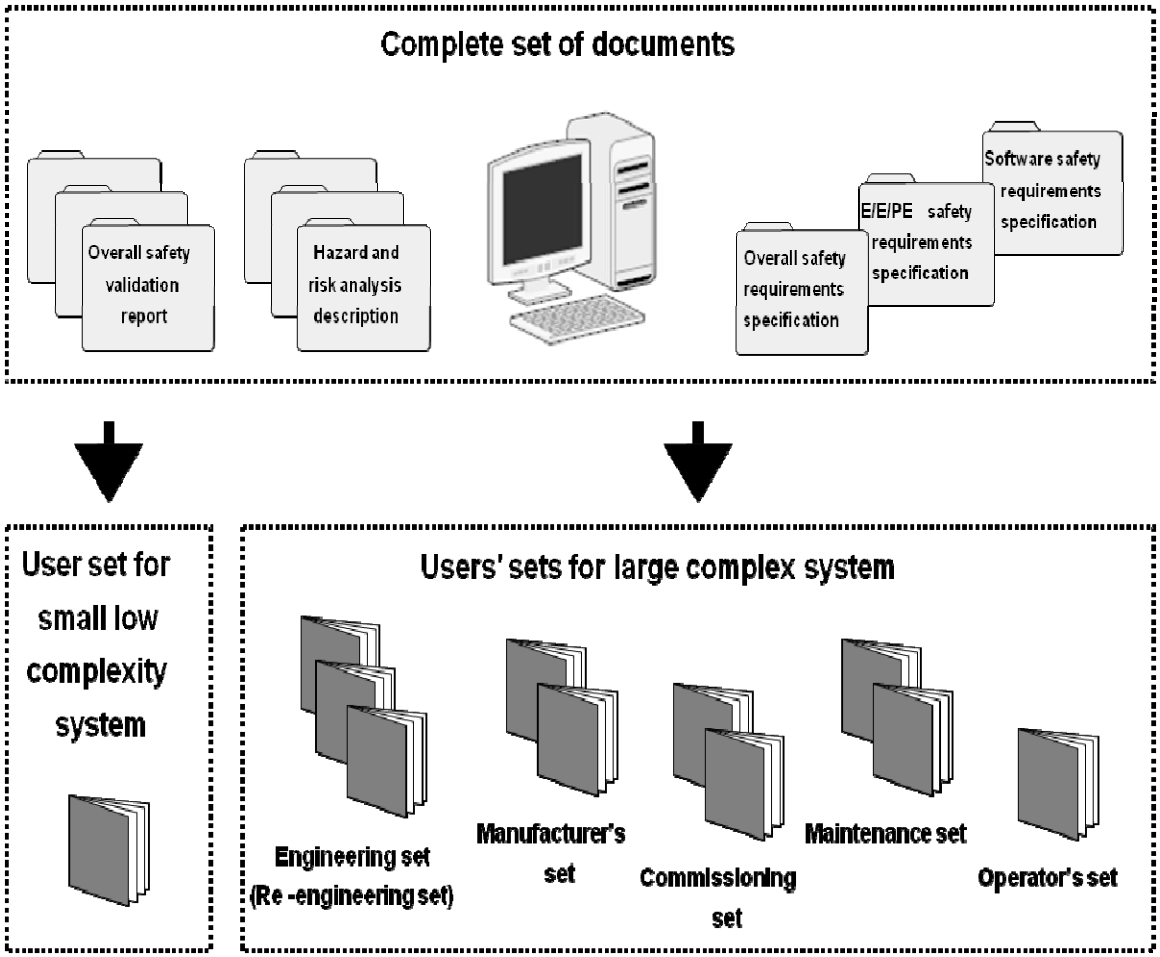


Figure A.1 – Structuring information into document sets for user groups

A.4 List of documents

The list of documents will typically include the following information:

– drawing or document number;
– revision index;
– document designation code;
– title;
– date of revision;
– data carrier.

This list may appear in different forms, for example in a database capable of being sorted according to drawing, document number or document designation code. The document designation code may contain the reference designation for the function, location or product described in the document, making it a powerful tool in searching for information.

Bibliography

[1] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[2] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[3] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

[4] IEC/TR 61508-0:2005, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*

[5] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

[7] IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

[8] *Managing Competence for Safety-Related Systems*, IET/BCS/HSE, 2007; (Part 1: Key guidance; Part 2 Supplementary material). HSE. 2007

[9] *Competence criteria for safety-related system practitioners*. IET. 2006

[10] IEC 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

[11] IEC 60300-3-9:1995, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

[12] IEC 61882:2001, *Hazard and operability studies (HAZOP studies) – Application guide*

[13] NUREG/CR-4780, Volume 1, January 1988, *Procedures for treating common cause failures in safety and reliability studies – Procedural framework and examples*

[14] NUREG/CR-4780, Volume 2, January 1989, *Procedures for treating common cause failures in safety and reliability studies – Analytical background and techniques*

[15] 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*

[16] ISO 8613-1:1994, *Information technology – Open Document Architecture (ODA) and Interchange Format: Introduction and general principles*

[17] IEC 61355 (all parts), *Classification and designation of documents for plants, systems and equipment*

[18] IEC 60601 (all parts), *Medical electrical equipment*

[19] 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*

[20] IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

[21] IEC 62443(all parts), *Industrial communication networks – Network and system security*

[22] ISO/IEC/TR 19791, *Information technology – Security techniques – Security assessment of operational systems*

_____

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™