COMMISSION ELECTROTECHNIQUE INTERNATIONALE

CEI IEC 61508-1

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: General requirements

Contents

Figures

Tables

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

Part 1: General requirements

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC national committees). The object of the IEC is to promote international cooperation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes international standards. Their preparation is entrusted to technical committees; any IEC national committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of the IEC on technical matters, prepared by technical committees on which all the national committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.

3) They have the form of recommendations for international use published in the form of standards, technical reports or guides and they are accepted by the national committees in that sense.

4) In order to promote international unification, IEC national committees undertake to apply IEC international standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC standard and the corresponding national or regional standard shall be clearly indicated in the latter.

5) Attention is drawn to the possibility that some of the elements of IEC 61508 may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

6) The IEC has not laid down any procedure concerning marking as an indication of approval and has no responsibility when an item of equipment is declared to comply with one of its standards.

IEC 61508-1 has been prepared by sub-committee 65A: System aspects, of IEC technical committee ~~65: Industrial process measurement and control~~65: Industrial process measurement and control~~65: Industrial process measurement and control~~.

The text of this part is based on the following documents:

FDIS	Report on voting
65A/xxx	65A/xxx

Full information on the voting for the approval of this standard can be found in the voting report indicated in the above table.

Annexes A, B and C are for information only.

IEC 61508 consists of the following parts, under the general title “Functional safety of electrical/ electronic/programmable electronic safety-related systems”:

— Part 1: General requirements;

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

— Part 3: Software requirements;

— Part 4: Definitions and abbreviations;

— Part 5: Examples of methods for the determination of safety integrity levels;

— Part 6: Guidelines on the application of parts 2 and 3;

— Part 7: Overview of techniques and measures.

Introduction

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

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

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

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

This standard:

— considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs are used to perform safety functions;

— has been conceived with a rapidly developing technology in mind – the framework is sufficiently robust and comprehensive to cater for future developments;

— enables application sector international standards, dealing with safety-related E/E/PESs, to be developed – the development of application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc) both within application sectors and across application sectors; this will have both safety and economic benefits;

— provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;

— uses safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

— adopts a risk-based approach for the determination of the safety integrity level requirements;

— sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;

— sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in:

  — a low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand,

  — a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

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

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

Part 1: General requirements

1 Scope

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

1.2 In particular, this standard:

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

NOTE 1 In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this standard may be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.4 of part 4).

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

NOTE 3 In the USA and Canada, until an international standard specific to the process industry is published in the USA and Canada, existing process safety standards can be applied to the process industry sector instead of IEC 61508.

b) is generically-based and applicable to all E/E/PE safety-related systems irrespective of the application;

c) covers possible hazards caused by failures of the safety functions to be performed by E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself (for example electric shock etc);

d) does not cover E/E/PE systems where:

— a single E/E/PE system is capable of providing the necessary risk reduction; and

— the required safety integrity of the E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).

e) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment – however, it is recognised 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;

f) considers E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;

g) uses an overall safety lifecycle model as the technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;

NOTE 4 The early phases of the overall safety lifecycle include, of necessity, consideration of other technology (as well as the E/E/PE safety-related systems) and external risk reduction facilities, in order that the safety requirements specification for the E/E/PE safety-related systems can be developed in a systematic, risk-based manner.

NOTE 5 Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it could also provide a technical framework for the consideration of any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

h) does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application) – the technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards;

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

j) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems.

1.3 This part of IEC 61508 specifies the general requirements that are applicable to all parts. Other parts of IEC 61508 concentrate on more specific topics. That is:

— parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (for hardware and software);

— part 4 gives definitions and abbreviations that are used throughout this standard;

— part 5 provides guidelines on the application of part 1 in determining safety integrity levels, by showing example methods;

— part 6 provides guidelines on the application of parts 2 and 3;

— part 7 contains an overview of techniques and measures.

1.4 Parts 1, 2, 3 and 4 of this standard are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 of part 4). As basic safety publications, they are intended for use by Technical Committees in the preparation of standards in accordance with the principles contained in ISO/IEC Guide 104 and ISO/IEC Guide 51. One of the responsibilities of a Technical Committee is, wherever applicable, to make use of basic safety publications in the preparation of its own publications. IEC 61508 is also intended for use as a stand-alone standard.

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

Figure 1 — Overall framework of this standard

2 Normative references

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

ISO/IEC Guide 51, ~~*Guidelines for the inclusion of safety aspects*~~*Safety aspects – Guidelines for their inclusion in standards*

ISO/IEC Guide 104, *Guide to the drafting of safety standards, and the role of committees with safety pilot functions and safety group functions*

3 Definitions and abbreviations

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

4 Conformance to this standard

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

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

— consequence and risk reduction;

— nature of the hazards;

— safety integrity level;

— type of implementation technology;

— size of systems;

— number of teams involved;

— physical distribution;

— novelty of design.

4.2 This standard specifies the requirements for E/E/PE safety-related systems and has been developed to meet the full range of complexity associated with such systems. However, for low complexity E/E/PE safety-related systems (see 3.4.4 of part 4), where dependable field experience exists which provides the necessary confidence that the required safety integrity can be achieved, the following options are available:

— in application sector standards implementing the requirements of parts 1 to 7 of this standard, certain requirements in this standard may be unnecessary and exemption from compliance with such requirements is acceptable;

— if this standard is used directly for those situations where no application sector international standard exists, certain of the requirements specified in this standard may be unnecessary and exemption from compliance with such requirements is acceptable providing this is justified.

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

5 Documentation

5.1 Objectives

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

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

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

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

NOTE 3 See annex A concerning possible documentation structures.

NOTE 4 See reference [[38]] in annex C.

5.2 Requirements

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

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

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

NOTE See notes to 5.1.2.

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

NOTE See notes to 5.1.2.

5.2.4 Unless justified in the functional safety planning or specified in the application sector standard, the information to be documented shall be as stated in the various clauses of this standard.

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

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

5.2.6 The documentation shall:

— be accurate and concise;

— be easy to understand by those persons having to make use of it;

— suit the purpose for which it is intended;

— be accessible and maintainable.

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

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

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

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

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

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

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

6 Management of functional safety

6.1 Objectives

6.1.1 The first objective of the requirements of this clause is to specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.

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

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

6.2 Requirements

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

a) the policy and strategy for achieving functional safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organization to ensure a culture of safe working;

b) ~~spec~~identification of the persons, departments and organizations which are responsible for carrying out and reviewing the applicable overall, E/E/PES or software safety lifecycle phases (including, where relevant, licensing authorities or safety regulatory bodies);

c) the overall, E/E/PES or software safety lifecycle phases to be applied;

d) the way in which information is to be structured and the extent of the information to be documented (see clause 5);

e) the selected measures and techniques used to meet the requirements of a specified clause or subclause (see parts 2, 3 and 6);

f) the functional safety assessment activities (see clause 8);

g) the procedures for ensuring prompt follow-up and satisfactory resolution of recommendations relating to E/E/PE safety-related systems arising from:

- hazard and risk analysis (see 7.4),
- functional safety assessment (see clause 8),
- verification activities (see 7.18),
- validation activities (see 7.8 and 7.14),
- configuration management (see 6.2.1 o), 7.16 and parts 2 and 3);

h) the procedures for ensuring that applicable parties involved in any of the overall, E/E/PES or software safety lifecycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified:

— the training of staff in diagnosing and repairing faults and in system testing,

— the training of operations staff,

— the retraining of staff at periodic intervals;

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

i) the procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations made to minimise the probability of a repeat occurrence;

j) the procedures for analysing operations and maintenance performance. In particular procedures for:

— recognising systematic faults which could jeopardise functional safety, including procedures used during routine maintenance which detect recurring faults,

— assessing whether the demand rates and failure rates during operation and maintenance are in accordance with assumptions made during the design of the system;

k) requirements for periodic functional safety audits in accordance with this subclause including:

— the frequency of the functional safety audits,

— consideration as to the level of independence required for those responsible for the audits,

— the documentation and follow-up activities;

l) the procedures for initiating modifications to the safety-related systems (see 7.16.2.2);

m) the required approval procedure and authority for modifications;

n) the procedures for maintaining accurate information on potential hazards and safety-related systems;

o) the procedures for configuration management of the E/E/PE safety-related systems during the overall, E/E/PES and software safety lifecycle phases; in particular the following should be specified:

— the stage at which formal configuration control is to be implemented,

— the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software),

— the procedures for preventing unauthorized items from entering service;

NOTE 2 For more details on configuration management see references [[45]] and [[46]] in annex C.

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

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

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

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

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

7 Overall safety lifecycle requirements

7.1 General

7.1.1 Introduction

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

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

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

— E/E/PE safety-related systems;

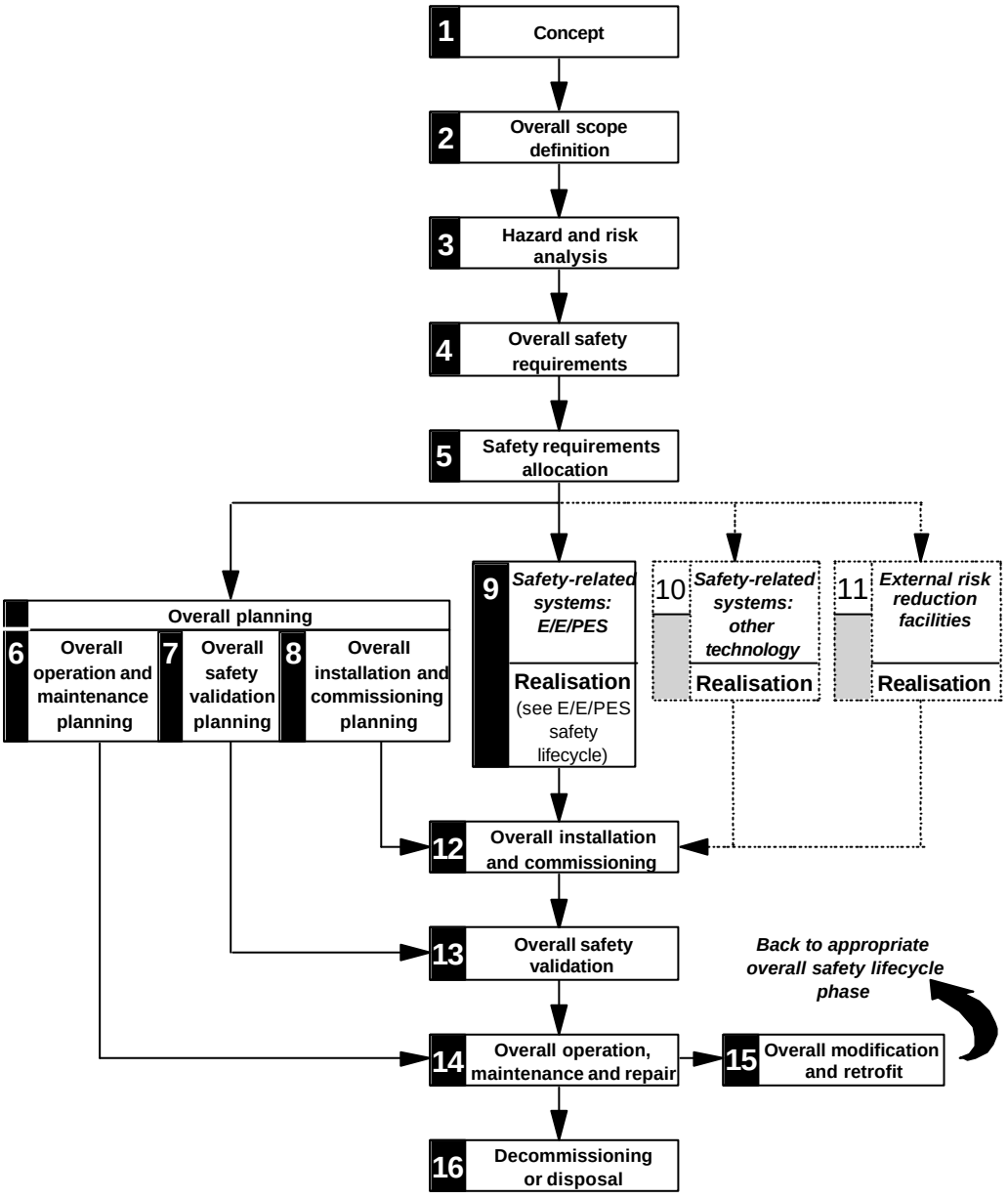
— other technology safety-related systems;

— external risk reduction facilities.

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

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

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



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

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

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

Figure 2 — Overall safety lifecycle

Figure 3 — E/E/PES safety lifecycle (in realisation phase)

Figure 4 — Software safety lifecycle (in realisation phase)

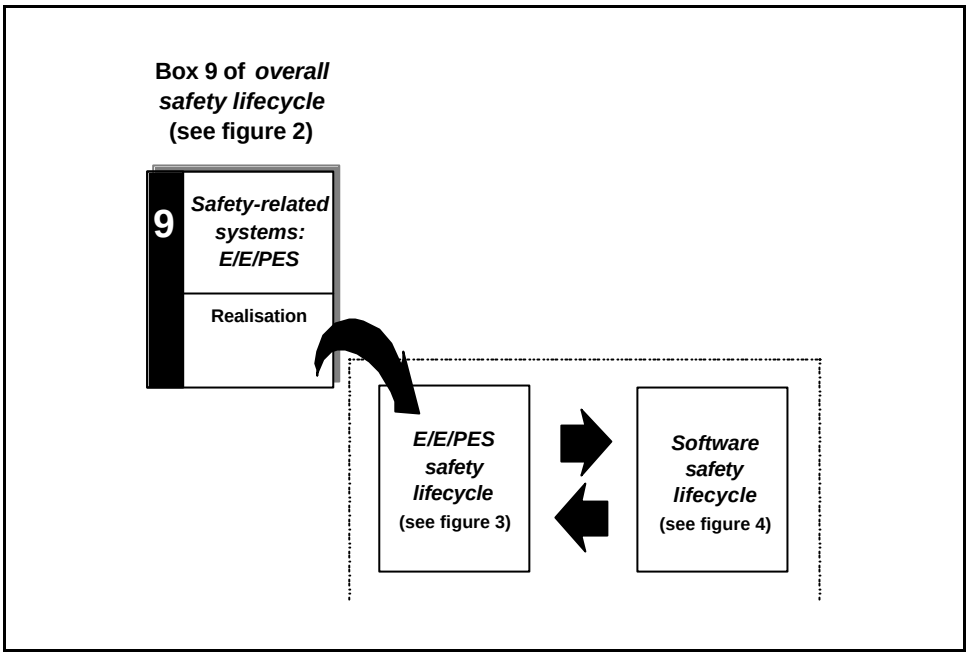


Figure 5 — Relationship of overall safety lifecycle to E/E/PES and software safety lifecycles

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/PES and software safety lifecycle phases are contained in parts 2 and 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-	Inputs	Outputs
Figure 2 box number	Title			ments subclause		
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 acquired in 7.2.2.1 to 7.2.2.6.
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 acquired in 7.2.2.1 to 7.2.2.6.	Information acquired in 7.3.2.1 to 7.3.2.5.
3	**Hazard and risk analysis**	7.4.1: To determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse; To determine the event sequences leading to the hazardous events determined; To determine the EUC risks associated with the hazardous events determined.	The scope will be dependent upon the phase reached in the overall, E/E/PES 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 comprise the EUC, the EUC control system and human factors.	7.4.2	Information acquired in 7.3.2.1 to 7.3.2.5.	Description of, and information relating to, the hazard and risk analysis.
4	**Overall safety requirements**	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, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.	EUC, the EUC control system and human factors.	7.5.2	Description of, and information relating to, the hazard and risk analysis.	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.
5	**Safety requirements 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, other technology safety-related systems and external risk reduction facilities; To allocate a safety integrity level to each safety function.	EUC, the EUC control system and human factors.	7.6.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	Information and results of the safety requirements allocation.

Table 1 *(continued)*

Safety lifecycle phase		Objectives	Scope	Require-	Inputs	Outputs
Figure 2 box number	Title			ments subclause		
6	**Overall operation and maintenance 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	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	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 to facilitate 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	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan to facilitate the validation of the E/E/PE safety-related systems.
8	**Overall installation and commission - ing 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 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 the required functional safety is achieved.	EUC and the EUC control system; E/E/PE safety-related systems.	7.9.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	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.
9	**E/E/PE safety-related systems: realisation**	7.10.1 and parts 2 and 3: To create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).	E/E/PE safety-related systems.	7.10.2 and parts 2 and 3	Specification for the E/E/PES safety requirements.	Confirmation that each E/E/PE safety-related system meets the E/E/PES safety requirements specification.
10	**Other technology safety-related systems: realisation**	7.11.1: To create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other technology safety-related systems.	7.11.2	Other technology safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each other technology safety-related systems meets the safety requirements for that system.

Safety lifecycle phase		Objectives	Scope	Require-	Inputs	Outputs
Figure 2 box number	Title			ments subclause		
11	**External risk reduction facilities: realisation**	7.12.1: To create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities (outside the scope of this standard).	External risk reduction facilities.	7.12.2	External risk reduction facilities safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each external risk reduction facility meets the safety requirements for that facility.

Table 1 *(concluded)*

Safety lifecycle phase		Objectives	Scope	Require-	Inputs	Outputs
Figure 2 box number	Title			ments subclause		
12	**Overall installation and commissio n- ing**	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 commissioning 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; Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements; Safety requirements allocation.	Confirmation that all the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems.
14	**Overall operation, maintenanc e and repair**	7.15.1: To operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.	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.

Safety lifecycle phase		Objectives	Scope	Require-	Inputs	Outputs
Figure 2 box number	Title			ments subclause		
15	**Overall modification and retrofit**	7.16.1: 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 operation, repair and maintenance of the E/E/PE safety-related systems.
16	**Decommiss-ioning or disposal**	7.17.1: 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 decommissioning 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 decommissioning or disposal activities; Chronological documentation of the decommissioning 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 and annex A for documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific 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 during the functional safety planning, and all the objectives and requirements in each clause or subclause in this standard shall be met.

NOTE The E/E/PES safety lifecycle and the software safety lifecycle (which form the realisation phase of the overall safety lifecycle) that shall be used in claiming conformance are specified in parts 2 and 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.

7.1.4.6 Unless justified in the functional safety planning or specified in the application sector standard, the outputs from each phase of the overall safety lifecycle shall be those specified in table 1.

7.1.4.7 The outputs from each phase of 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 shall be determined.

7.2.2.3 Information about the determined hazards shall be obtained (toxicity, explosive conditions, corrosiveness, reactivity, flammability etc).

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

7.2.2.5 Hazards due to interaction with other EUCs (installed or to be installed) in the proximity of the EUC shall be considered.

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 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 [[6]] and [[8]] in annex C.

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

7.3.2.3 The subsystems which are associated with the hazards shall be specified.

7.3.2.4 The type of accident-initiating events that need to be considered (for example component failures, procedural faults, human error, dependent failure mechanisms which can cause accident sequences to occur) shall be specified.

7.3.2.5 The information and results acquired in 7.3.2.1 to 7.3.2.4 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 and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse.

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, likely hazards, 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 annexes D and E of part 5.

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/PES or software safety lifecycle phases which 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 [[6]] and [[8]] in annex C.

NOTE 2 It may be necessary for more than one hazard and risk analysis to be carried out.

NOTE 3 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 analysed, 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 of the hazards.

NOTE Although not within the scope of this standard, it is of primary importance that determined 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 and hazardous events of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC.

NOTE For reasonably foreseeable misuse see 3.1.10 of part 4.

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

NOTE 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.

NOTE The likelihood of a specific event may be expressed quantitatively or qualitatively (see part 5).

7.4.2.6 The potential 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 part 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 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 necessary risk reduction 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;

— references to key information (see clause 5 and annex A) which relates to the safety-related systems at each E/E/PES safety lifecycle phase (for example verification and validation activities).

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

7.4.2.12 The information and results which 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 and results from the hazard and risk analysis phase, is the principal means for establishing progress on the resolution of 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 safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.

NOTE In application areas where valid assumptions can be made about the risks, likely hazards, hazardous 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 annexes D and E of part 5.

7.5.2 Requirements

7.5.2.1 The safety functions necessary to ensure the required functional safety for each determined hazard shall be specified. This shall constitute the specification for the overall safety functions requirements.

NOTE The 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 safety functions will not be known until later. During the allocation of safety requirements (see 7.6), the description of the safety functions may need to be modified to reflect the specific method of implementation.

7.5.2.2 The necessary risk reduction shall be determined for each determined hazardous event. The necessary risk reduction may be determined in a quantitative and/or qualitative manner.

NOTE The necessary risk reduction is required in order to determine the safety integrity requirements for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities. Annex C of part 5 outlines one way in which the necessary risk reduction may be determined when a quantitative approach has been adopted. Annexes D and E of part 5 outline qualitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly rather than stated explicitly.

7.5.2.3 For situations where an application sector international standard exists, which includes appropriate methods for directly determining the necessary risk reduction, then such standards may be used to meet the requirements of this subclause.

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

a) the dangerous failure rate 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; and

b) the dangerous failure rate that can be claimed for the EUC control system shall be not lower than 10^{-5} dangerous failures per hour; and

NOTE 1 The rationale of this requirement is that if the EUC control system is not designated as a safety-related system, then the failure rate that can be claimed for the EUC control system shall not be lower than the higher target failure measure for safety integrity level 1 (which is 10^{-5} dangerous failures per hour - see table 3).

c) all reasonably foreseeable dangerous failure modes of the EUC control system shall be determined and taken into account in developing the specification for the overall safety requirements; and

d) the EUC control system shall be separate and independent from the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

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 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.

7.5.2.5 If the requirements of 7.5.2.4 a) to d) inclusive cannot be met then the EUC control system shall be designated as a safety-related system. The safety integrity level allocated to the EUC control system shall be based on the failure rate that is claimed for the EUC control system in accordance with the target failure measures specified in tables 2 and 3. In such cases, the requirements in this standard, relevant to the allocated safety integrity level, shall apply to the EUC control system.

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

NOTE 2 See also 7.6.2.10.

7.5.2.6 The safety integrity requirements, in terms of the necessary risk reduction, shall be specified for each safety function. This shall constitute the specification for the overall safety integrity requirements.

NOTE The specification of the safety integrity requirements is an interim stage towards the determination of the 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 annexes D and E of part 5) progress directly from the risk parameters to the safety integrity levels. In such cases the necessary risk reduction is implicitly rather than explicitly stated because it is incorporated in the method itself.

7.5.2.7 The specification for the safety functions (see 7.5.2.1) and the specification for the safety integrity requirements (see 7.5.2.6) shall together constitute the specification for the overall safety requirements.

7.6 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 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, other technology safety-related systems and external risk reduction facilities.

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

7.6.1.2 The second objective of the requirements of this subclause is to allocate a safety integrity level to each safety function.

NOTE The safety integrity requirements, as specified in 7.5, are specified in terms of risk reduction.

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 necessary risk reduction may be achieved by:

— external risk reduction facilities;

— E/E/PE safety-related systems;

— other technology safety-related systems.

NOTE This subclause is applicable only if one of the safety-related systems is an E/E/PES.

7.6.2.2 In allocating safety functions to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, 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 stages, from specification through to maintenance and operation. 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 safety function, with its associated safety integrity requirement developed according to 7.5, shall be allocated to the designated E/E/PE safety-related systems taking into account the risk reductions achieved by the other technology safety-related systems and external risk reduction facilities, so the necessary risk reduction for that safety function is achieved. This allocation is iterative, and if it is found that the necessary risk reduction cannot be met, then the architecture shall be modified and the allocation repeated.

NOTE 1 Each safety function, with its associated safety integrity requirement specified in terms of the necessary risk reduction (from 7.5), will be allocated to one or more E/E/PE safety-related systems, to other technology safety-related systems, and to external risk reduction facilities. The decision to allocate a specific safety function across one or more safety-related systems will depend on a number of factors, but particularly on the risk reduction to be achieved by the safety function. The larger the risk reduction required, the more likely the function will be spread over more than one safety-related system.

NOTE 2 Figure 6 indicates the approach adopted in this subclause to safety requirements allocation.

7.6.2.4 The allocation indicated in 7.6.2.3 shall be done in such a way that all safety functions are allocated and the safety integrity requirements are met for each safety function (subject to the overriding requirements specified in 7.6.2.10).

7.6.2.5 The safety integrity requirements for each safety function shall be qualified to indicate whether each target safety integrity parameter is either:

— the average probability of failure to perform its design function on demand (for a low demand mode of operation); or

— the probability of a dangerous failure per hour (for a high demand or 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 Safety requirements allocation may be carried out in a qualitative and/or quantitative manner.

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

— be functionally diverse (ie use totally different approaches to achieve the same results); and

— be based on diverse technologies (ie use different types of equipment to achieve the same results); and

NOTE 1 It has to be 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; and

— not share common operational, maintenance or test procedures; and

— be physically separated such that foreseeable failures do not affect redundant safety-related systems and external risk reduction facilities.

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

Figure 6 — Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities

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, the other technology safety-related systems and the external risk reduction facilities shall not be treated as independent, for the purposes of the safety integrity allocation, unless an analysis has been carried out which shows that they are sufficiently independent (from a safety integrity viewpoint).

NOTE 1 For further information on dependent failures analysis see references [[49]] and [[50]] in annex C.

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

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 tables 2 and 3 and be qualified to indicate whether the target safety integrity parameter is either:

— the average probability of failure to perform its design function on demand (for a low demand mode of operation); or

— the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

NOTE 1 Prior to this step the safety integrity requirements were specified in terms of the risk reduction (see 7.5).

NOTE 2 Tables 2 and 3 contain the target failure measures for the safety integrity levels. 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 necessary to meet the target failure measures. This is particularly true in the case of systematic safety integrity (see 3.5.4 of part 4).

Table 2 — Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in low demand mode of operation

Safety integrity level	**Low demand mode of operation** (Average probability of failure to perform its design function on demand)
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 $< 10^{-1}$
NOTE See notes 3 to 9 below for details on interpreting this table.	

Table 3 — Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in high demand or continuous mode of operation

Safety integrity level	**High demand or continuous mode of operation** (Probability of a dangerous failure per hour)
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 See notes 3 to 9 below for details on interpreting this table.	

NOTE 3 See 3.5.12 of part 4 for definition of the terms low demand mode and high demand or continuous mode of operation.

NOTE 4 The parameter in table 3 for high demand or continuous mode of operation, probability of a dangerous failure per hour, is sometimes referred to as the frequency of dangerous failures, or dangerous failure rate, in units of dangerous failures per hour.

NOTE 5 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 probability of failure per hour, then use table 3 to derive the required safety integrity level.

NOTE 6 This standard sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed. These are specified as the lower limits for safety integrity level 4 (ie an average probability of failure of 10^{-5} to perform its design function on demand, or a probability of a dangerous failure of 10^{-9} per hour). It may be possible to achieve designs of safety-related systems with lower values for the target failure measures for non-complex systems, but it is considered that the figures in the table represent the limit of what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

NOTE 7 The target failure measures that can be claimed when two or more E/E/PE safety-related systems are used may be better than those indicated in tables 2 and 3 providing that adequate levels of independence are achieved.

NOTE 8 It is important to note that the failure measures for safety integrity levels 1, 2, 3 and 4 are target failure measures. It is accepted that only with respect to the hardware safety integrity (see 3.5.5 of part 4) will it be possible to quantify and apply reliability prediction techniques in assessing whether the target failure measures have been met. Qualitative techniques and judgements have to be made with respect to the precautions necessary to meet the target failure measures with respect to the systematic safety integrity (see 3.5.4 of part 4).

NOTE 9 The safety integrity requirements for each safety function shall be qualified to indicate whether each target safety integrity parameter is either:

— the average probability of failure to perform its design function on demand (for a low demand mode of operation); or

— the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

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 7.4.2.4 of part 2 and 7.4.2.8 of part 3.

7.6.2.11 An architecture that is comprised of only a single E/E/PE safety-related system of safety integrity level 4 shall be permitted only if the criteria in either a) or both b) and c) below are met:

a) there has been an explicit demonstration, by a combination of appropriate analytical methods and testing, of the target safety integrity failure measure;

b) there has been extensive operating experience of the components used as part of the E/E/PE safety-related system – such experience shall have been gained in a similar environment and, as a minimum, have been used in a system of comparable complexity level;

c) there is sufficient hardware failure data, obtained from components used as part of the E/E/PE safety-related system, to allow sufficient confidence in the hardware safety integrity target failure measure that is to be claimed – the data should be relevant to the proposed environment, application and complexity level.

7.6.2.12 No single E/E/PE safety-related system shall be allocated a target safety integrity failure measure 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 failure of 10^{-5} to perform its design function on demand;

— a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour.

7.6.2.13 The information and results of the safety requirements allocation acquired in subclauses 7.6.2.1 to 7.6.2.12, together with any assumptions and justifications made, 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 developed in part 2.

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.

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

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 which shall specify the following:

a) the routine actions which 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 hazardous events;

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

— constraints on the EUC operation during a fault or failure of the E/E/PE safety-related systems;

— constraints on the EUC operation during maintenance of the E/E/PE safety-related systems;

— when constraints on the EUC operation may be removed;

— the procedures for returning to normal operation;

— the procedures for confirming that normal operation has been achieved;

— the circumstances under which the E/E/PE safety-related system functions may be by-passed for start-up, for special operation or for testing;

— 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 which needs to be maintained showing results of functional safety audits and tests;

d) the documentation which needs to be maintained on hazardous incidents 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 hazards 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 which can be revealed only by testing during routine maintenance. In such cases, if testing is not carried out at sufficient frequency, the required safety integrity of the E/E/PE safety-related system will not be achieved. Where testing is carried out on-line, it may be necessary to disable the E/E/PE safety-related system on a temporary basis. This should be considered only if the probability of a demand occurring during this time is remote. Where this cannot be ensured, it may be necessary to install additional sensors and actuators to maintain the required functional safety during testing.

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 part 3). Implementing these procedures is covered by 7.15, and 7.8 of part 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 7.16, and 7.6 of part 3. Implementing those procedures is covered by 7.16, and 7.8 of part 2.

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

7.7.2.2 The routine maintenance activities which are carried out to detect unrevealed faults should be determined by a systematic analysis.

NOTE If unrevealed faults are not detected, it may:

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

— in the case of non-safety-related systems, lead to demands on the E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities.

7.7.2.3 The plan for maintaining the E/E/PE safety-related systems shall be agreed upon with those responsible for the future operation and maintenance of the E/E/PE safety-related systems, the other technology safety-related systems, the external risk reduction facilities, and the non-safety-related systems that have the potential to place demands on the safety-related systems.

7.8 Overall safety validation planning

NOTE This phase is box 7 of figure 2.

7.8.1 Objective

The objective of the requirements of this subclause is to develop a plan to facilitate 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 which 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 which 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/PES safety validation and software validation as required by parts 2 and 3. It is important to ensure that the interactions between all risk reduction measures are considered and 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 This phase is box 8 of figure 2.

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 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:

— the installation schedule;

— those responsible for different parts of the installation;

— the procedures for the installation;

— the sequence in which the various elements are integrated;

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

— 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:

— the commissioning schedule;

— those responsible for different parts of the commissioning;

— the procedures for the commissioning;

— the relationships to the different steps in the installation;

— the relationships to the validation.

7.9.2.3 The overall installation and commissioning planning shall be documented.

7.10 Realisation: E/E/PES

NOTE This phase is box 9 of figure 2 and boxes 9.1 to 9.6 of figures 3 and 4.

7.10.1 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/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements). See parts 2 and 3.

7.10.2 Requirements

The requirements that shall be met are contained in parts 2 and 3.

7.11 Realisation: other technology

NOTE: This phase is box 10 of figure 2.

7.11.1 Objective

The objective of the requirements of this subclause is to create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems.

7.11.2 Requirements

The specification to meet the safety functions requirements and safety integrity requirements for other technology safety-related systems is not covered in this standard.

NOTE Other technology safety-related systems are based on a technology other than electrical/electronic/programmable electronic (for example hydraulic, pneumatic etc). The other technology safety-related systems have been included in the overall safety lifecycle, together with the external risk reduction facilities, for completeness (see 7.12).

7.12 Realisation: external risk reduction facilities

NOTE This phase is box 11 of figure 2.

7.12.1 Objective

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

7.12.2 Requirements

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

NOTE The external risk reduction facilities have been included in the overall safety lifecycle, together with the other technology safety-related systems for completeness (see 7.11).

7.13 Overall installation and commissioning

NOTE This phase is box 12 of figure 2.

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.

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 This phase is box 13 of figure 2.

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**.**

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

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

7.15.1 Objective

The objective of the requirements of this subclause is to operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.

7.15.2 Requirements

7.15.2.1 The following shall be implemented:

— the plan for maintaining the E/E/PE safety-related systems;

— the operation, maintenance and repair procedures for the E/E/PE safety-related systems (see part 2);

— the operation and maintenance procedures for software (see part 3).

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 6.2.1 k));

— 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 application and shall, where relevant, be detailed in application sector standards.

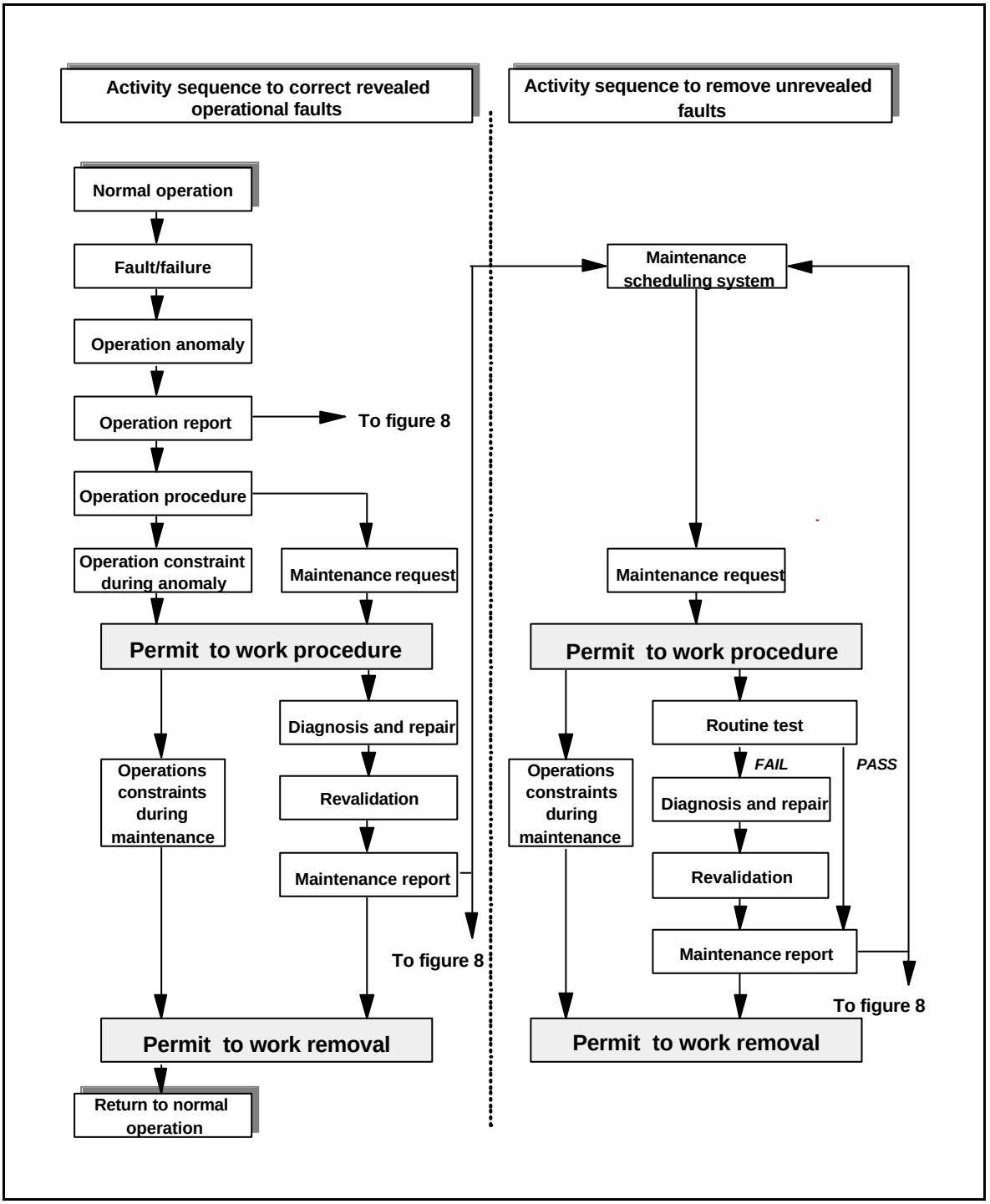


Figure 7 — Example operations and maintenance activities model

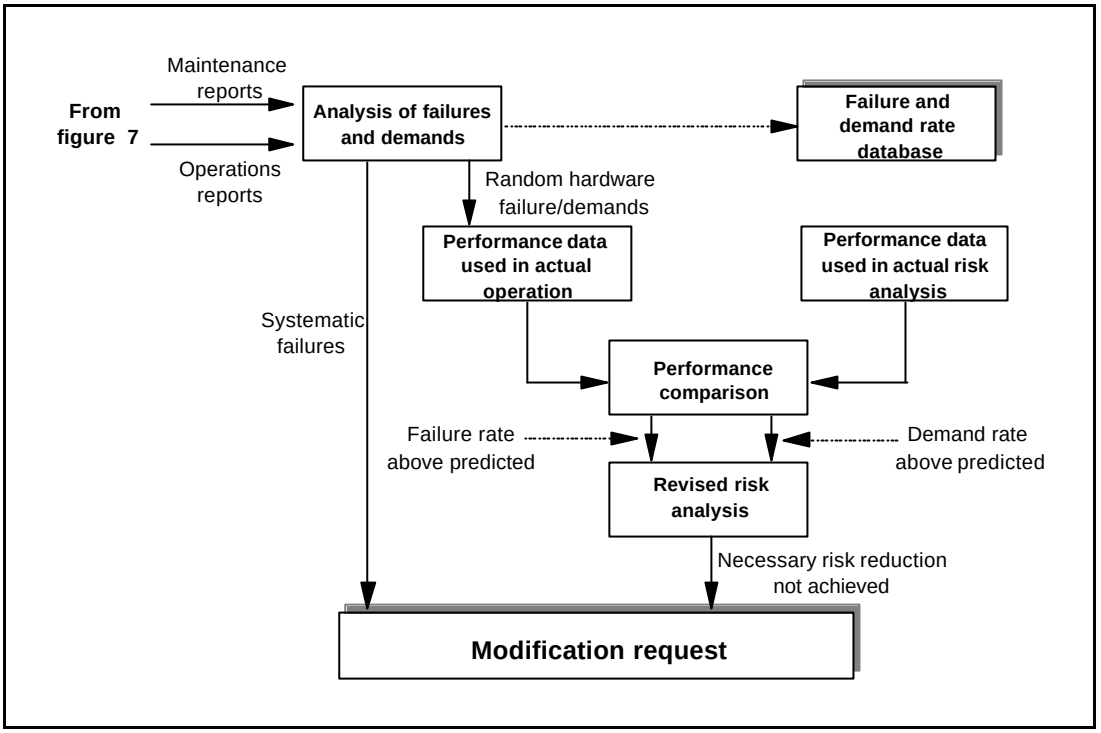


Figure 8 — Example operation and maintenance management model

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

7.16.1 Objective

The objective of the requirements of this subclause is 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 6.2.1).

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 clause 6). The request shall detail the following:

— the determined hazards which 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:

— functional safety below that specified;

— systematic fault experience;

— new or amended safety legislation;

— modifications to the EUC or its use;

— modification to the overall safety requirements;

— analysis of operations and maintenance performance, indicating that the performance is below target;

— routine functional safety audits.

7.16.2.3 An impact analysis shall be carried out which 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/PES 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 which 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/PES 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 E/E/PE safety-related systems.

NOTE 2 It must 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 which 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.

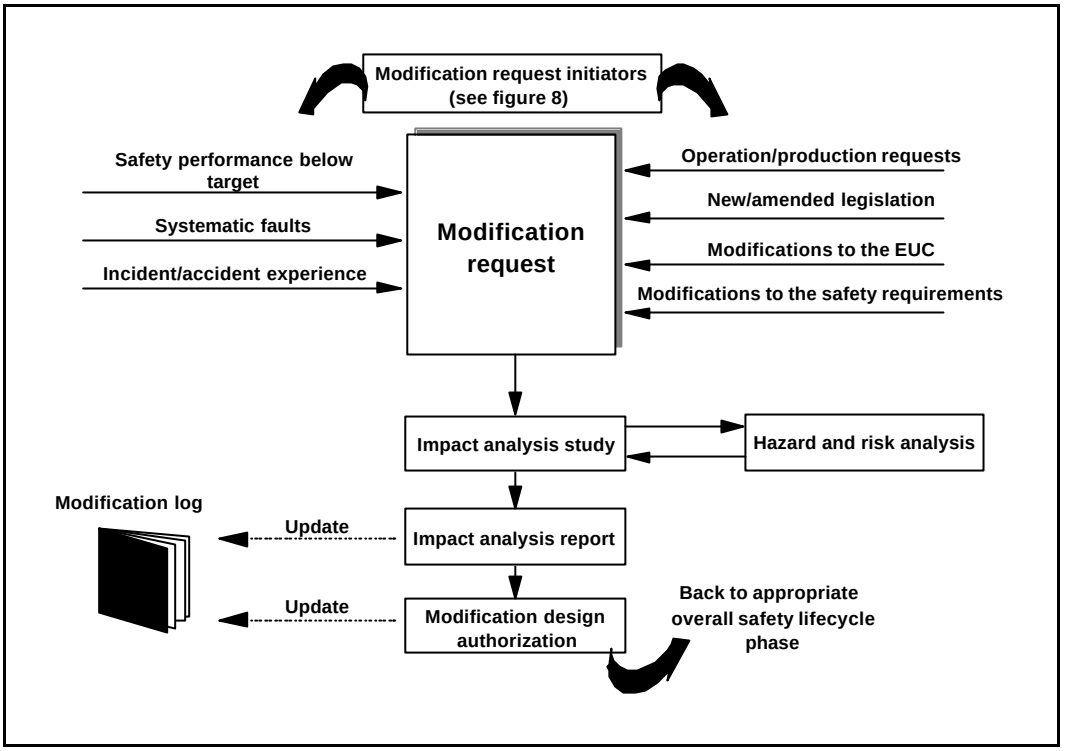


Figure 9 — Example modification procedure model

7.17 Decommissioning or disposal

NOTE This phase is box 16 of figure 2.

7.17.1 Objective

The objective of the requirements of this subclause is 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 which 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/PES 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 which 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/PES or software safety lifecycles. All subsequent phases shall then be carried out in accordance with the procedures specified in this standard for the specified safety integrity levels for 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 a different safety integrity level for 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 which 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/PES 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/PES 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 application sector 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 investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems.

8.2 Requirements

8.2.1 One or more persons shall be appointed to carry out a functional safety assessment in order to arrive at a judgement of the functional safety achieved by the E/E/PE safety-related systems.

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

8.2.3 The functional safety assessment shall be applied to all phases throughout the overall, E/E/PES and software safety lifecycles. Those carrying out the functional safety assessment shall consider the activities carried out and the outputs obtained during each phase of the overall, E/E/PES and software safety lifecycles and judge the extent to which the objectives and requirements in this standard have been met.

8.2.4 The functional safety assessment shall be carried out throughout the overall, E/E/PES and software lifecycles and may be carried out after each safety lifecycle phase 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.

8.2.5 If tools are used as part of design or assessment for any overall, E/E/PES or software safety lifecycle activity they should themselves be subject to the functional safety assessment.

NOTE 1 Example tools are CAD/CAM systems, compilers and host target systems.

NOTE 2 The degree to which the use of such tools will need to be evaluated will depend upon their impact on the functional safety of the E/E/PE safety-related systems.

8.2.6 The functional safety assessment shall consider the following:

— the work done since the previous functional safety assessment (which will normally have covered previous safety lifecycle phases);

— the plans or strategy for implementing further functional safety assessments of the overall, E/E/PES and software safety lifecycles;

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

8.2.7 The functional safety assessment activities for the different phases of the overall, E/E/PES and software safety lifecycles shall be consistent and planned.

8.2.8 The plan for the functional safety assessment shall specify:

— those to undertake the functional safety assessment;

— the outputs from each functional safety assessment;

— the scope of the functional safety assessment;

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

— the safety bodies involved;

— the resources required;

— the level of independence of those undertaking the functional safety assessment;

— the competence of those undertaking the functional safety assessment relative to the application.

8.2.9 Prior to a functional safety assessment taking place, the plan for the functional safety assessment shall be approved by those carrying out the functional safety assessment and by those responsible for the management of functional safety for the safety lifecycle phases being assessed.

8.2.10 At the conclusion of the functional safety assessment, recommendations shall be produced for acceptance, qualified acceptance or rejection.

8.2.11 Those carrying out the functional safety assessment shall be competent for the activities to be undertaken and notice should be taken of the factors for assessing competence in annex B.

8.2.12 Unless otherwise stated in application sector international standards, the minimum level of independence of those carrying out the functional safety assessment shall be as specified in tables 4 and 5. The recommendations in the tables are as follows.

— HR: the level of independence specified is highly recommended as a minimum for the specified consequence (table 4) or safety integrity level (table 5). If a lower level of independence is adopted then the rationale for not using the HR level should be detailed.

— NR: the level of independence specified is considered insufficient and is positively not recommended for the specified consequence (table 4) or safety integrity level (table 5). If this level of independence is adopted then the rationale for using it should be detailed.

— -: the level of independence specified has no recommendation for or against being used.

NOTE 1 Prior to the application of table 4, it will be necessary to define the consequence categories taking into account current good practices in the application sector. The consequences are those that would arise in the event of failure, when required to operate, of the E/E/PE safety-related systems.

NOTE 2 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, which 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 3 See 3.8.10, 3.8.11 and 3.8.12 of part 4 for definitions of independent person, independent department and independent organization respectively.

8.2.13 In the context of tables 4 and 5, either HR^1 or HR^2 is applicable (not both), depending on a number of factors specific to the application. If HR^1 is applicable then HR^2 should be read as no requirement; if HR^2 is applicable then HR^1 should be read as NR (not recommended). If no application sector standard exists, the rationale for choosing HR^1 or HR^2 should be detailed. Factors that will tend to make HR^2 more appropriate than HR^1 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;

— lack of degree of standardization of design features.

8.2.14 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.

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 note 2)			
	A	B	C	D
Independent person	HR	HR[1]	NR	NR
Independent department	-	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	-	-	HR[2]	HR
NOTE 1 See 8.2.12 (including notes) and 8.2.13 for details on interpreting this table. NOTE 2 Typical consequences could be: 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.				

Table 5 — Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phase 9 - includes all phases of E/E/PES and software safety lifecycles (see figures 2, 3 and 4))

Minimum level of Independence	**Safety integrity level**			
	1	2	3	4
Independent person	HR	HR[1]	NR	NR
Independent department	-	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	-	-	HR[2]	HR
NOTE See 8.2.12 (including notes), 8.2.13 and 8.2.14 for details on interpreting this table.				

Annex A
(informative)

Example 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/PES 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 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 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 [[38]] in annex C 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 (ISO 8613-1). The term applies therefore not only to documents in the traditional sense, but also to concepts like 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 the future IEC 61355 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 is 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 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 and overall safety integrity)
Safety requirements allocation	Description (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)
Realisation	Realisation of E/E/PE safety-related systems (see parts 2 and 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 documentation structure for information related to the E/E/PES safety lifecycle

E/E/PES safety lifecycle phase	Information
E/E/PES safety requirements	Specification (E/E/PES safety requirements, comprising: E/E/PES safety functions and E/E/PES safety integrity)
E/E/PES validation planning	Plan (E/E/PES safety validation)
E/E/PES design and development	
E/E/PES architecture	Description (E/E/PES 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 modules design); Specifications (hardware modules test)
Component construction and/or procurement	Hardware modules; Report (hardware modules test)
Programmable electronic integration	Report (programmable electronic and software integration test) (see table A.3)
E/E/PES integration	Report (programmable electronic and other hardware integration test)
E/E/PES operation and maintenance procedures	Instruction (user); Instruction (operation and maintenance)
E/E/PES safety validation	Report (E/E/PES safety validation)
E/E/PES modification	Instruction (E/E/PES modification procedures); Request (E/E/PES modification); Report (E/E/PES modification impact analysis); Log (E/E/PES modification)
Concerning all phases	Plan (E/E/PES safety); Plan (E/E/PES verification); Report (E/E/PES verification); Plan (E/E/PES functional safety assessment); Report (E/E/PES functional safety assessment)

Table A.3 — Example 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 and software safety integrity)
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 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 test); Report (code review)
Software module testing	Report (software module test)
Softw are integration	Report (software module integration test); Report (software system integration test); Report (software architecture integration test)
Programmable electronic integration	Report (programmable electronic and software integration test)
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)

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. Figure A.1 shows examples of such sets of binders structured according to user groups. 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 (see figure A.2).

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 figures A.1 and A.2. For example, within the engineering set, documents such as the hazard and risk analysis description and/or overall safety requirements specification would be contained.

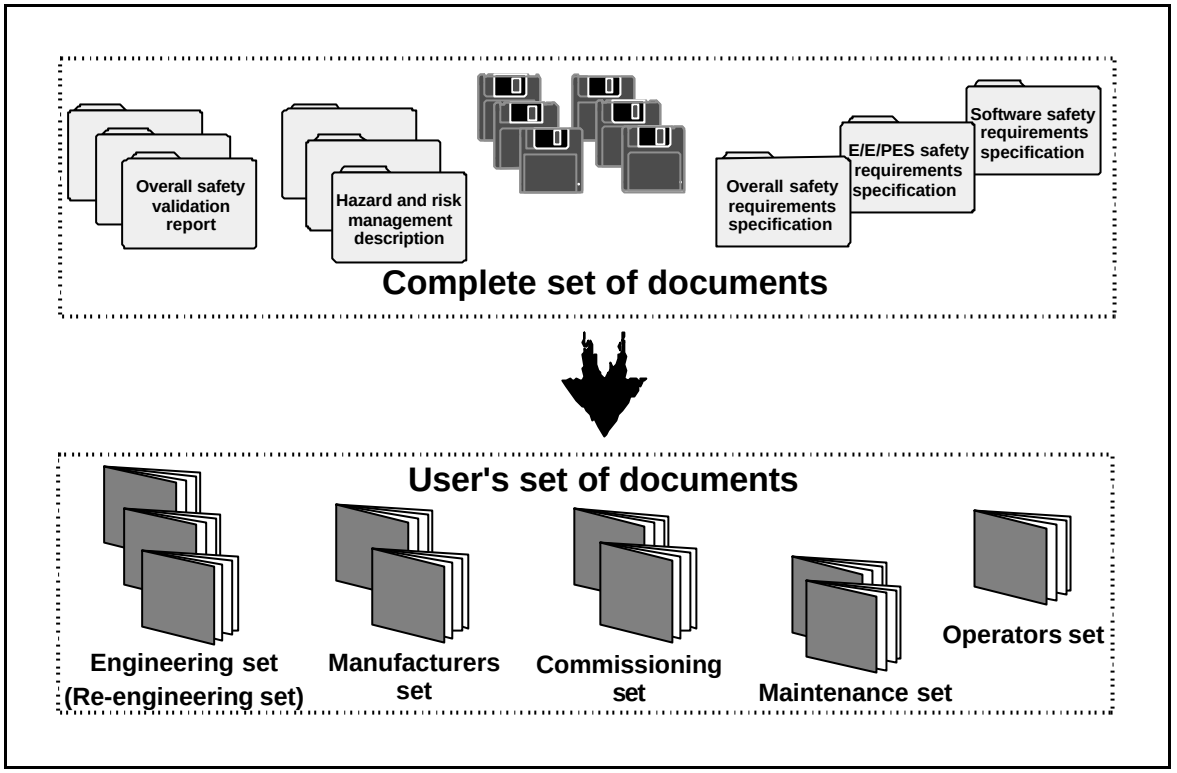


Figure A.1 — Structuring information into document sets for user groups

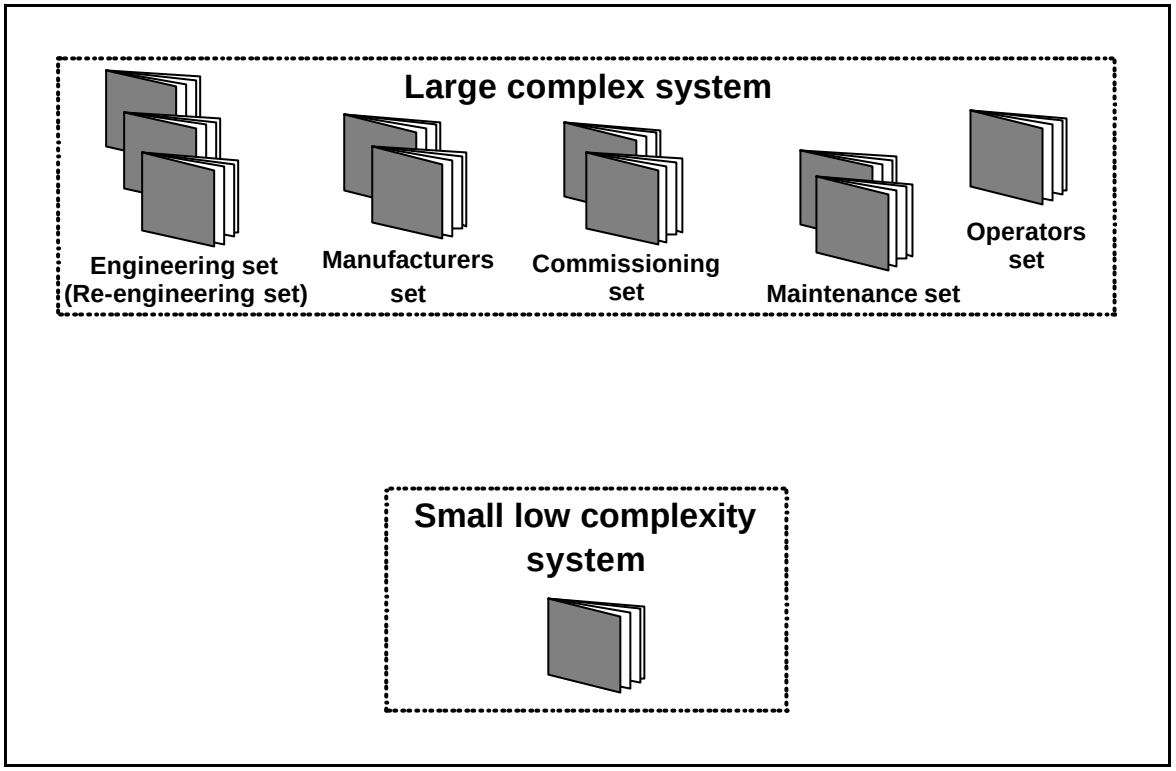


Figure A.2 — Structuring information for large complex systems and small low complexity systems

A.4 List of documents

The list of documents will typically include information such as:

— 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.

Annex B
(informative)

Competence of persons

B.1 Objective

This annex outlines considerations for ensuring that persons who have responsibilities for any overall, E/E/PES or software safety lifecycle activity are competent to discharge those responsibilities.

B.2 General considerations

All persons involved in any overall, E/E/PES or software safety lifecycle activity, including management activities, should have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform.

The training, experience and qualifications of all persons involved in any overall, E/E/PES or software safety lifecycle activity, including any management of functional safety activities, should be assessed in relation to the particular application.

The following factors should be considered when assessing the competence of persons to carry out their duties:

a) engineering knowledge appropriate to the application area;

b) engineering knowledge appropriate to the technology (for example electrical, electronic, programmable electronic, software engineering);

c) safety engineering knowledge appropriate to the technology;

d) knowledge of the legal and safety regulatory framework;

e) the consequences in the event of failure of the E/E/PE safety-related systems – the greater the consequences the more rigorous should be the specification and assessment of competence;

f) the safety integrity levels of the E/E/PE safety-related systems – the higher the safety integrity levels the more rigorous should be the specification and assessment of competence;

g) the novelty of the design, design procedures or application – the newer or more untried the designs, design procedures or application, the more rigorous the specification and assessment of competence should be;

h) previous experience and its relevance to the specific duties to be performed and the technology being employed – the greater the required competence levels, the closer the fit should be between the competencies developed from previous experience and those required for the specific duties to be undertaken;

i) relevance of qualifications to specific duties to be performed.

The training, experience and qualifications of all persons involved in any overall, E/E/PES or software safety lifecycle activity should be documented.

Annex C
(informative)

Bibliography

[1] IEC 60050, *International Electrotechnical Vocabulary (IEV)*

[2] IEC 60068, *Environmental testing*

[3] IEC 60204-1: 1992, *Electrical equipment of industrial machines – Part 1: General requirements*

[4] IEC 60255, *Electrical relays*

[5] IEC 60300: 1984, *Reliability and maintainability management*

[6] IEC 60300-3-1: 1991, *Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology*

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

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

[9] IEC 60319: 1978, *Presentation of reliability data on electronic components or parts*

[10] IEC 60362: 1971, *Guide for collection of reliability, availability and maintainability data from field performance of electronic items*

[11] IEC 60409: 1981, *Guide for the inclusion of reliability clauses into specifications for components (or parts) for electronic equipment*

[12] IEC 60414: 1973, *Safety requirements for indicating and recording electrical measuring instruments and their accessories*

[13] IEC 60513: 1994, *Fundamental aspects of safety standards for medical electrical equipment*

[14] IEC 60519, *Safety in electroheat installations*

[15] IEC 60601, *Medical electrical equipment*

[16] IEC 60605, *Equipment reliability testing*

[17] IEC 60706, *Guide on maintainability of equipment*

[18] IEC 60801, *Electromagnetic compatibility for industrial process measurement and control equipment*

NOTE IEC 60801 is now superceded by IEC 61000 (see reference [23]).

[19] IEC 60812: 1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

[20] IEC 60839, *Alarm systems*

[21] IEC 60863: 1986, *Presentation of reliability, maintainability and availability predictions*

[22] IEC 60880: 1986, *Software for computers in the safety systems of nuclear power stations*

[23] IEC 61000, *Electromagnetic compatibility (EMC)*

[24] IEC 61014: 1989, *Programmes for reliability growth*

[25] IEC 61025: 1990, *Fault tree analysis (FTA)*

[26] IEC 61069, *Industrial process measurement and control – Evaluation of system properties for the purpose of system assessment*

[27] IEC 61078: 1991, *Analysis techniques for dependability – Reliability block diagram method*

[28] IEC 61123: 1991, *Reliability testing – Compliance test plans for success ratio*

[29] IEC 61131-1: 1992, *Programmable controllers – Part 1: General information*

[30] IEC 61131-2: 1992, *Programmable controllers – Part 2: Equipment requirements and tests*

[31] IEC 61131-3: 1993, *Programmable controllers – Part 3: Programming languages*

[32] IEC 61131-4: 1995, *Programmable controllers – Part 4: Users guidelines*

[33] 65B/236/3CD, *Programmable controllers – Part 5: Manufacturing message specification* (future IEC 61131-5, in preparation)

[34] IEC 61160: 1992, *Formal design review*

[35] IEC 61164: 1995, *Reliability growth – Statistical test and estimation methods*

[36] IEC 61165: 1995, *Application of Markov techniques*

[37] 3B/181/FDIS, *Classification and designation of documentation for plants, systems and equipment* (future IEC 61355, in preparation)

[38] 65/210/FDIS, *Documentation of software for process control systems and facilities* (future IEC 61506, in preparation)

[39] 65B(Sec)191, *Guidelines for the application and implementation of languages for programmable controllers* (future IEC 61519, in preparation)

[40] 56(Sec)406, *Software maintainability and maintenance aspects of a dependability programme* (future IEC 61714, in preparation)

[41] ISO/IEC 2382-1: 1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

[42] ISO 8402: 1994, *Quality Management and quality assurance – Vocabulary*

[43] ISO 8613-1: 1994, *Information technology – Open document architecture (ODA) and interchange format – Part 1: Introduction and general principles*

[44] ISO 9001: 1994, *Quality systems – Model for quality assurance in design, development, production, installation and servicing*

[45] ISO 10007: 1995, *Quality management – Guidelines for configuration management*

[46] ISO/IEC DIS 12220-2, *Information technology software processes – Software configuration management*

[47] *Grundlegende Sicherheitbetrachtungen fur MSR – Schutzeinrichtungen* DIN V 19250, Beuth Verlag, Berlin, FRG, 1994

[48] *Guidelines for safe automation of chemical process*, published by the Center for Chemical Process safety of the American Institute of Chemical Engineering, ISBN 0-8969-0554-1, 1993

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

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

[51] *Tolerability of risk from nuclear power stations*, Health and Safety Executive (UK) publication, ISBN 011 886368 1

[52] *Development guidelines for vehicle based software*, The Motor Industry Reliability Association, Watling St, Nuneaton, Warwickshire, CV10 0TU, United Kingdom, 1994, ISBN 09524156 0 7