IEC 61508-1

Edition 2.0 2010-04

INTERNATIONAL STANDARD

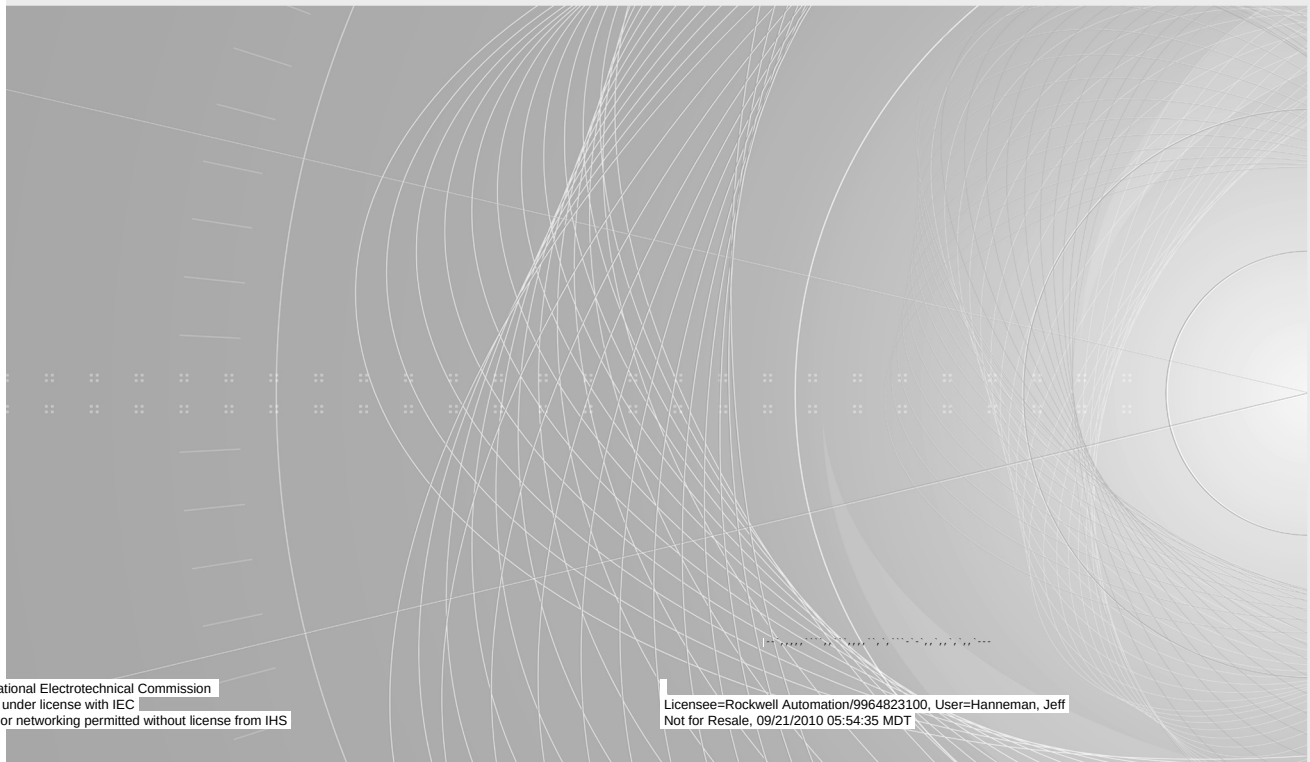
NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales



IEC 61508-1:2010

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61508-1

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 13.110; 25.040; 29.020

ISBN 978-2-88910-524-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: General requirements

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. 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 IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1998. This edition constitutes a technical revision.

This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.

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

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

FDIS	Report on voting
65A/548/FDIS	65A/572/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

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

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

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

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

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

This International Standard

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

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

– sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in

  – a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5};

  – a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}];

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

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

– sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;

– introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;

– adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe. However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

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

Part 1: General requirements

1 Scope

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

1.2 In particular, this standard

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

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

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

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

c) covers the achievement of a tolerable risk through the application of E/E/PE safety-related systems, but does not cover hazards arising from the E/E/PE equipment itself (for example electric shock);

d) applies to all types of E/E/PE safety-related systems, including protection systems and control systems;

e) does not cover E/E/PE systems where

   – a single E/E/PE system is capable on its own of meeting the tolerable risk, and

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

f) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE 3 See 3.1.1 of IEC 61508-4.

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

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

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

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

j) provides general requirements for E/E/PE safety-related systems where no product or application sector international standards exist;

k) requires malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases;

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

l) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems (see k) above);

m) does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system;

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

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

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

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

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

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

– part 7 contains an overview of techniques and measures.

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

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

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

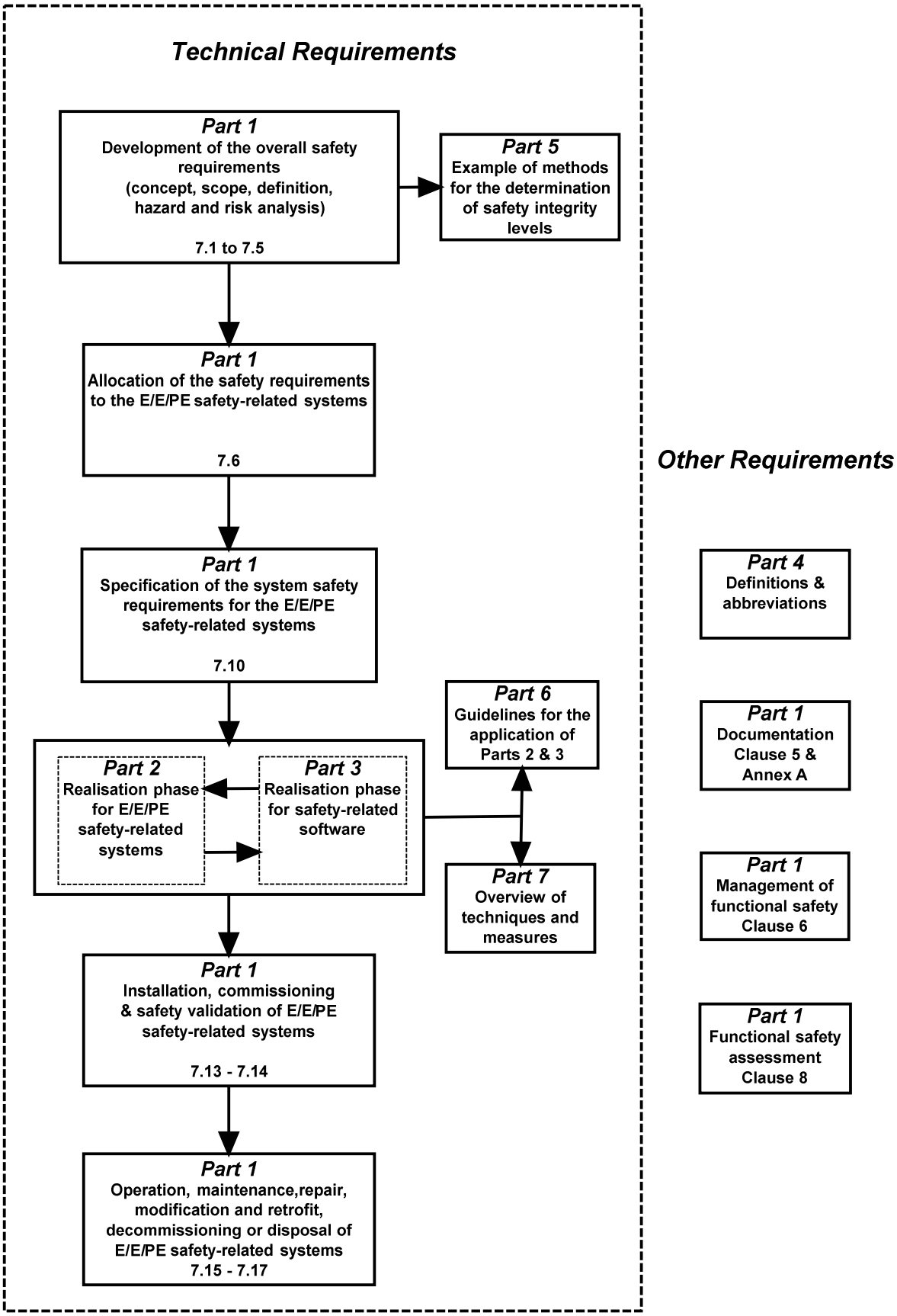


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

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

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

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

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

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

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

3 Definitions and abbreviations

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

4 Conformance to this standard

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

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

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

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

5 Documentation

5.1 Objectives

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

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

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

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

NOTE 3 See Annex A concerning possible documentation structures.

NOTE 4 See reference [7] in the Bibliography.

5.2 Requirements

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

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

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

NOTE See notes to 5.1.2.

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

NOTE See notes to 5.1.2.

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

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

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

5.2.6 The documentation shall:

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

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

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

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

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

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

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

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

6 Management of functional safety

6.1 Objectives

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

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

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

6.2 Requirements

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

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

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

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

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

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

NOTE See Clause 5 for documentation requirements.

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

a) hazard and risk analysis (see 7.4);

b) functional safety assessment (see Clause 8);

c) verification activities (see 7.18);

d) validation activities (see 7.8 and 7.14);

e) configuration management (see 6.2.10, 7.16, IEC 61508-2 and IEC 61508-3);

f) incident reporting and analysis (see 6.2.6).

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

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

a) the frequency of the functional safety audits;

b) the level of independence of those carrying out the audits;

c) the necessary documentation and follow-up activities.

6.2.8 Procedures shall be developed for:

a) initiating modifications to the E/E/PE safety-related systems (see 7.16.2.2);

b) obtaining approval and authority for modifications.

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

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

a) the point, in respect of specific phases, at which formal configuration control is to be implemented;

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

c) the procedures for preventing unauthorized items from entering service.

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

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

a) the selected measures and techniques used to meet the requirements of a specified clause or subclause (see IEC 61508-2, IEC 61508-3 and IEC 61508-6);

b) the functional safety assessment activities, and the way in which the achievement of functional safety will be demonstrated to those carrying out the functional safety assessment (see Clause 8);

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

– the selection of an appropriate organisation, person or persons, at the appropriate level of independence;

– the drawing up, and making changes to, terms of reference for functional safety assessments;

– the change of those carrying out the functional safety assessment at any point during the lifecycle of a system;

– the resolution of disputes involving those carrying out functional safety assessments.

c) the procedures for analysing operations and maintenance performance, in particular for

   – recognising systematic faults that could jeopardise functional safety, including procedures used during routine maintenance that detect recurring faults;

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

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

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

a) the responsibilities of the person;

b) the level of supervision required;

c) the potential consequences in the event of failure of the E/E/PE safety-related systems – the greater the consequences, the more rigorous shall be the specification of competence;

d) the safety integrity levels of the E/E/PE safety-related systems – the higher the safety integrity levels, the more rigorous shall be the specification of competence;

e) the novelty of the design, design procedures or application – the newer or more untried these are, the more rigorous shall be the specification of competence;

f) previous experience and its relevance to the specific duties to be performed and the technology being employed – the greater the required competence, the closer the fit shall be between the competences developed from previous experience and those required for the specific activities to be undertaken;

g) the type of competence appropriate to the circumstances (for example qualifications, experience, relevant training and subsequent practice, and leadership and decision-making abilities);

h) engineering knowledge appropriate to the application area and to the technology;

i) safety engineering knowledge appropriate to the technology;

j) knowledge of the legal and safety regulatory framework;

k) relevance of qualifications to specific activities to be performed.

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

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

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

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

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

7 Overall safety lifecycle requirements

7.1 General

7.1.1 Introduction

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

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

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

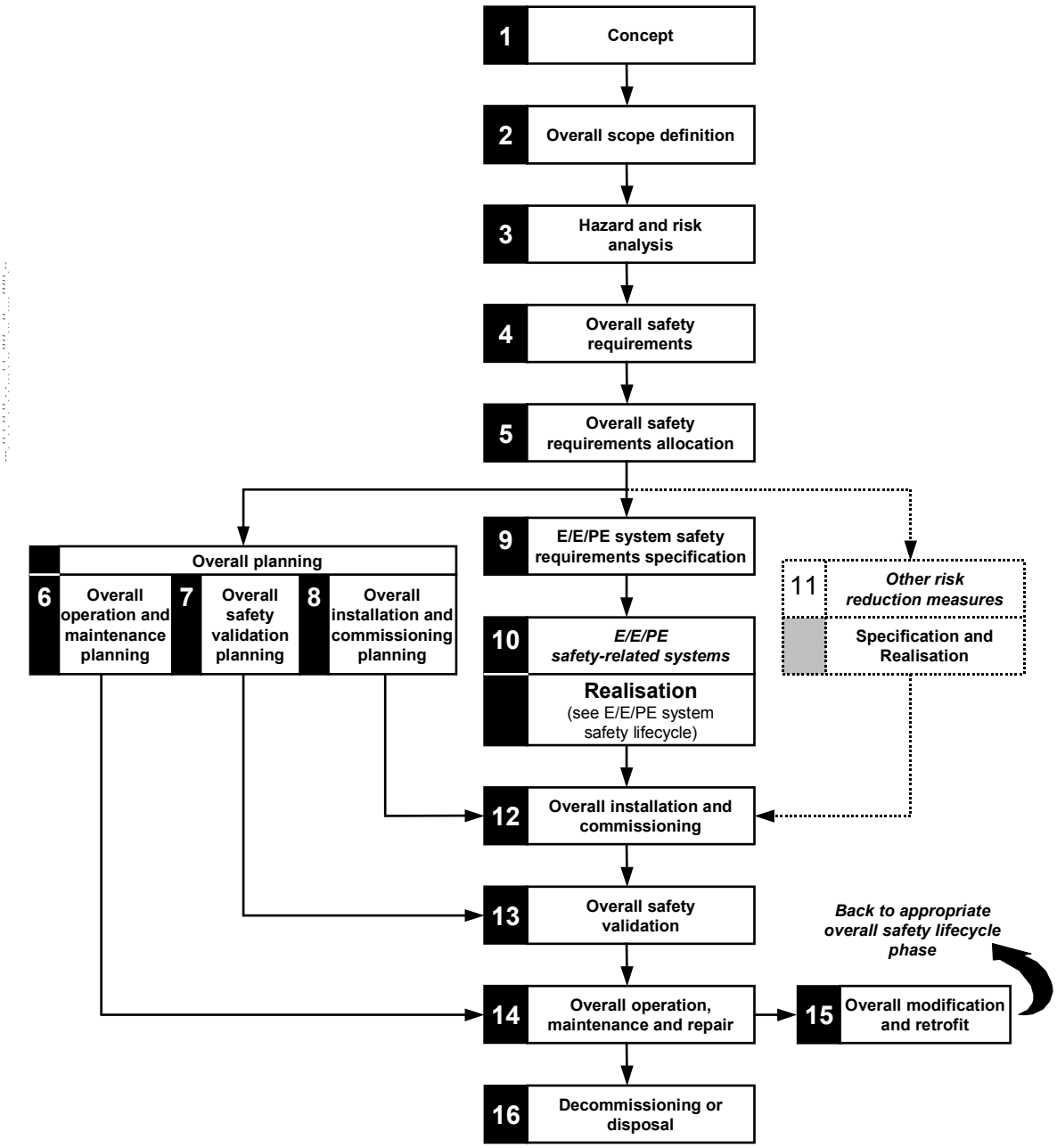
– E/E/PE safety-related systems;

– other risk reduction measures.

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

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

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



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

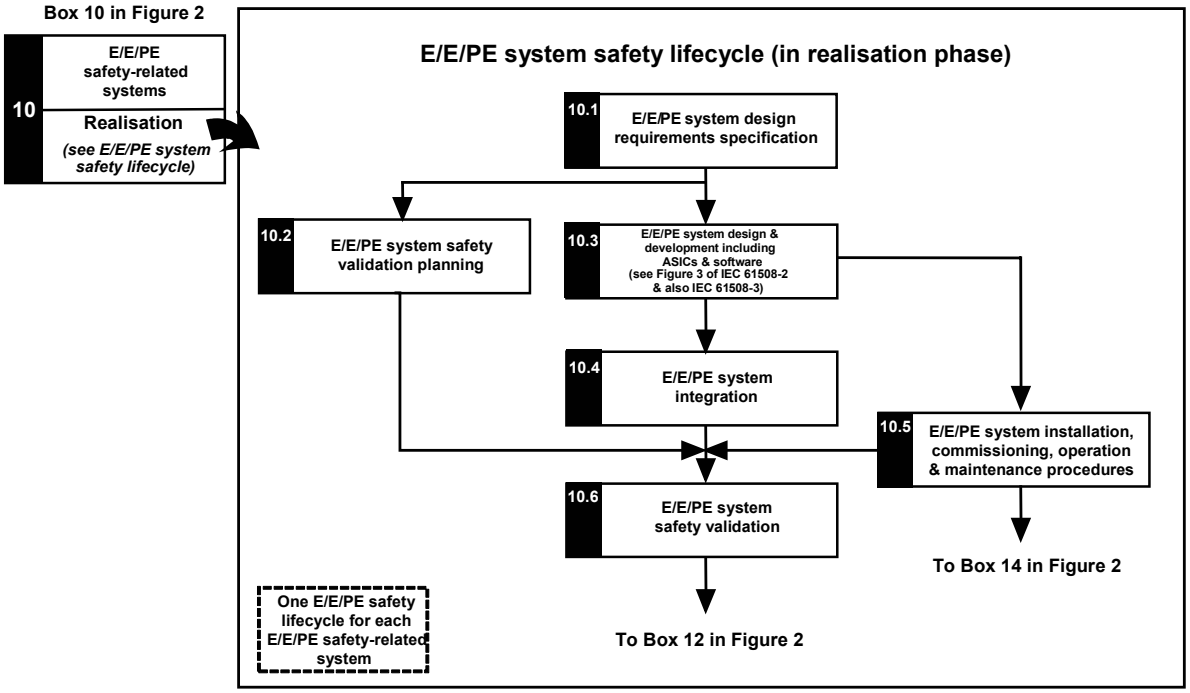
NOTE 2 The phase represented by Box 11 is outside the scope of this standard.

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

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

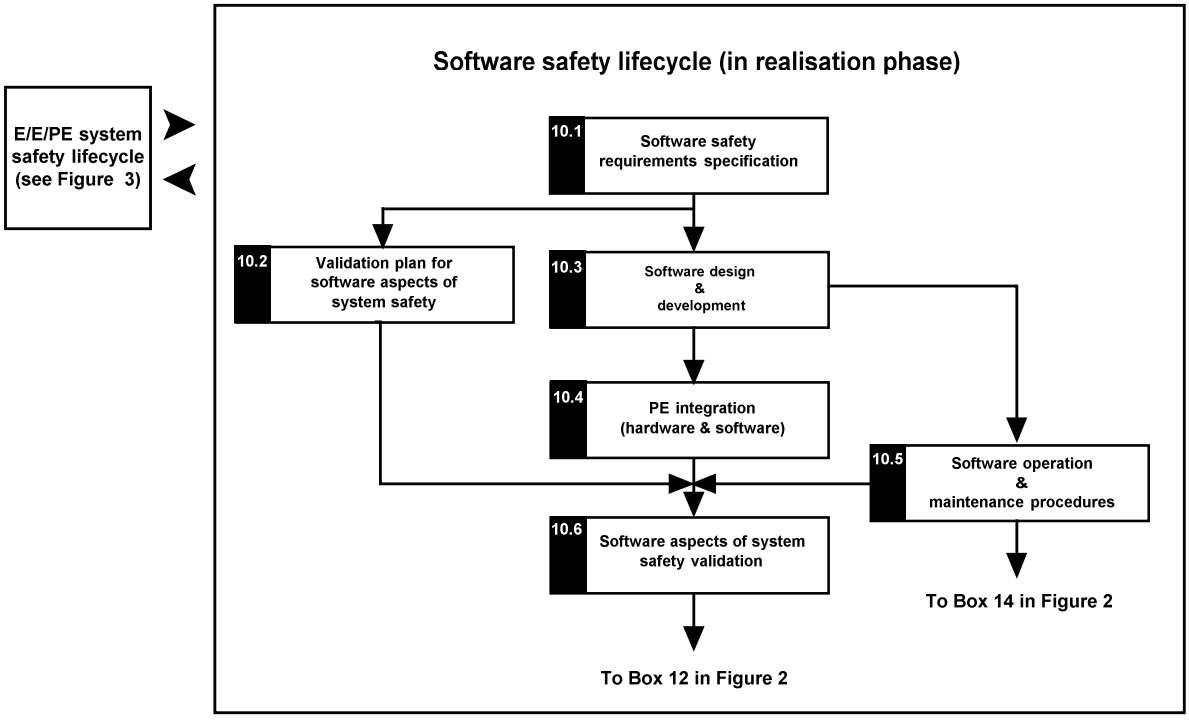
NOTE 5 The technical requirements necessary for overall operation, maintenance, repair, modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.

Figure 2 – Overall safety lifecycle



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

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



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

Figure 4 – Software safety lifecycle (in realisation phase)

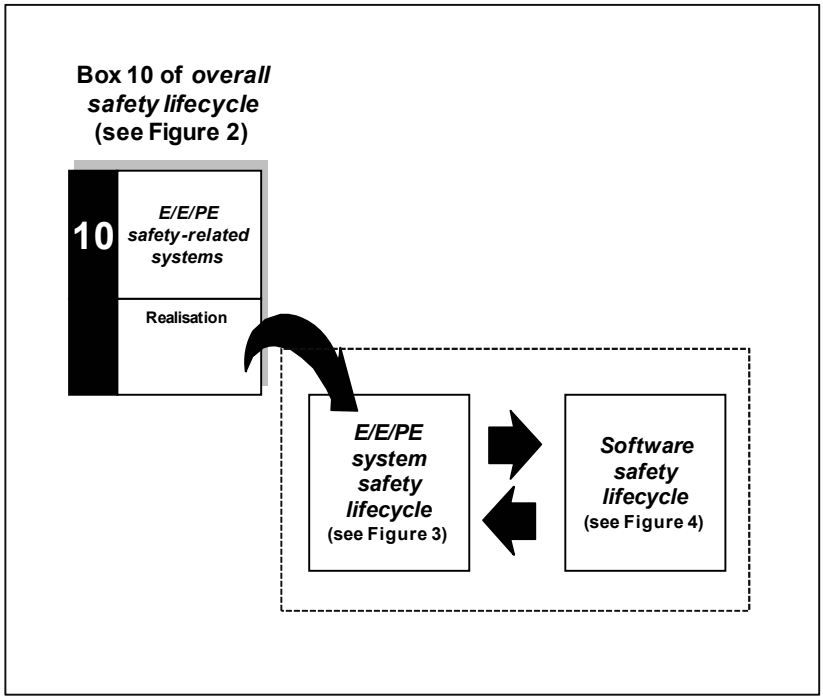


Figure 5 – Relationship of overall safety lifecycle to the E/E/PE system and software safety lifecycles

7.1.2 Objectives and requirements – general

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

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

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

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

Table 1 – Overall safety lifecycle – overview

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

Table 1 *(continued)*

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

Table 1 *(continued)*

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

Table 1 *(continued)*

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

7.1.3 Objectives

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

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

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

7.1.4 Requirements

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

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

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

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

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

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

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

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

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

7.2 Concept

NOTE This phase is Box 1 of Figure 2.

7.2.1 Objective

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

7.2.2 Requirements

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

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

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

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

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

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

7.3 Overall scope definition

NOTE This phase is Box 2 of Figure 2.

7.3.1 Objectives

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

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

7.3.2 Requirements

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

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

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

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

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

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

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

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

7.4 Hazard and risk analysis

NOTE This phase is Box 3 of Figure 2.

7.4.1 Objectives

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

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

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

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

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

7.4.2 Requirements

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

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

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

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

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

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

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

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

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

NOTE 4 Malevolent or unauthorised action covers security threats.

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

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

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

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

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

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

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

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

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

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

7.4.2.10 The hazard and risk analysis shall consider the following:

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

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

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

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

7.5 Overall safety requirements

NOTE This phase is Box 4 of Figure 2.

7.5.1 Objective

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

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

7.5.2 Requirements

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

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

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

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

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

NOTE Guidance is given in IEC 62443 series.

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

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

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

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

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

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

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

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

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

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

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

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

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

a) the rate of dangerous failure claimed for the EUC control system shall be supported by data acquired through one of the following:
   - actual operating experience of the EUC control system in a similar application;
   - a reliability analysis carried out to a recognised procedure;
   - an industry database of reliability of generic equipment;

b) the rate of dangerous failure that can be claimed for the EUC control system shall be no lower than 10^{-5} dangerous failures per hour;

NOTE 1 See 7.5.2.5.

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

d) the EUC control system shall be independent from the E/E/PE safety-related systems and other risk reduction measures.

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

NOTE 3 See 7.6.2.7 for meaning of independent.

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

NOTE See 7.5.2.5 and also 7.6.2.10.

7.6 Overall safety requirements allocation

NOTE This phase is Box 5 of Figure 2.

7.6.1 Objectives

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

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

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

7.6.2 Requirements

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

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

– other risk reduction measures.

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

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

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

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

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

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

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

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

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

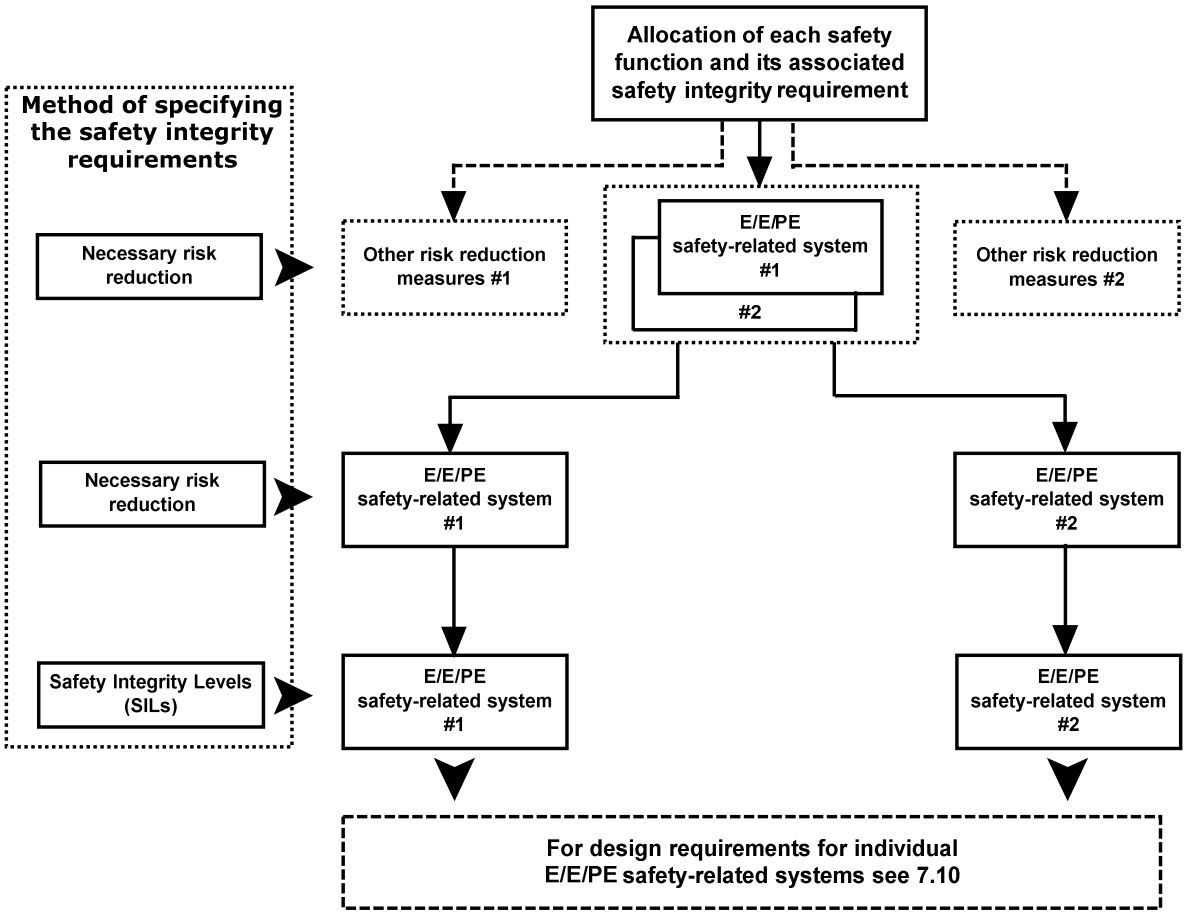
– the average probability of a dangerous failure on demand of the safety function, for a low demand mode of operation, or

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

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

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

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



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

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

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

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

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

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

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

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

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

– not share common operational, maintenance or test procedures.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

– a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of the safety function of 10^{-5};
– a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}]).

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

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

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

7.7 Overall operation and maintenance planning

NOTE 1 This phase is Box 6 of Figure 2.

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

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

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

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

7.7.1 Objective

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

7.7.2 Requirements

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

a) the routine actions that need to be carried out to maintain the required functional safety of the E/E/PE safety-related systems;
b) the actions and constraints that are necessary (for example during start-up, normal operation, routine testing, foreseeable disturbances, faults and shutdown) to prevent an

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE If unrevealed faults are not detected, they may

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

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

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

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

7.8 Overall safety validation planning

NOTE 1 This phase is Box 7 of Figure 2.

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

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

7.8.1 Objective

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

7.8.2 Requirements

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

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

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

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

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

7.9 Overall installation and commissioning planning

NOTE 1 This phase is Box 8 of Figure 2.

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

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

7.9.1 Objectives

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

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

7.9.2 Requirements

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

a) the installation schedule;

b) those responsible for different parts of the installation;

c) the procedures for the installation;

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

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

f) procedures for the resolution of failures and incompatibilities.

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

a) the commissioning schedule;

b) those responsible for different parts of the commissioning;

c) the procedures for the commissioning;

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

e) the relationships to the validation.

7.9.2.3 The overall installation and commissioning planning shall be documented.

7.10 E/E/PE system safety requirements specification

NOTE This phase is Box 9 of Figure 2.

7.10.1 Objective

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

7.10.2 Requirements

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

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

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

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

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

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

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

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

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

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

f) all relevant modes of operation of the EUC, including:
   – preparation for use including setting and adjustment,
   – start-up, teach, automatic, manual, semi-automatic, steady state of operation,
   – steady state of non-operation, re-setting, shut-down, maintenance,
   – reasonably foreseeable abnormal conditions;

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

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

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

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

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

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

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

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

c) the required duty cycle and lifetime;

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

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

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

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

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

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

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

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

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

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

7.11.1 Objective

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

7.11.2 Requirements

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

7.12 Other risk reduction measures – specification and realisation

NOTE This phase is Box 11 of Figure 2.

7.12.1 Objective

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

7.12.2 Requirements

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

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

7.13 Overall installation and commissioning

NOTE 1 This phase is Box 12 of Figure 2.

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

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

7.13.1 Objectives

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

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

7.13.2 Requirements

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

7.13.2.2 The information documented during installation shall include

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

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

7.13.2.4 The information documented during commissioning shall include

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

7.14 Overall safety validation

NOTE 1 This phase is Box 13 of Figure 2.

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

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

7.14.1 Objective

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

7.14.2 Requirements

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

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

7.14.2.3 The information documented during validation shall include

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

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

7.15 Overall operation, maintenance and repair

NOTE 1 This phase is Box 14 of Figure 2.

NOTE 2 The organizational measures dealt with in this subclause provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of functional safety of the E/E/PE safety-related systems. The technical requirements necessary for maintaining functional safety will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.

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

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

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

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

7.15.1 Objective

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

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

7.15.2 Requirements

7.15.2.1 The following shall be implemented:

– the plan for operating and maintaining the E/E/PE safety-related systems (see 7.7);

– the operation, maintenance and repair procedures for the E/E/PE safety-related systems.

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

– the implementation of procedures;

– the following of maintenance schedules;

– the maintaining of documentation;

– the carrying out, periodically, of functional safety audits (see 6.2.7);

– the documenting of modifications that have been made to the E/E/PE safety-related systems.

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

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

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

– the results of functional safety audits and tests;

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

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

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

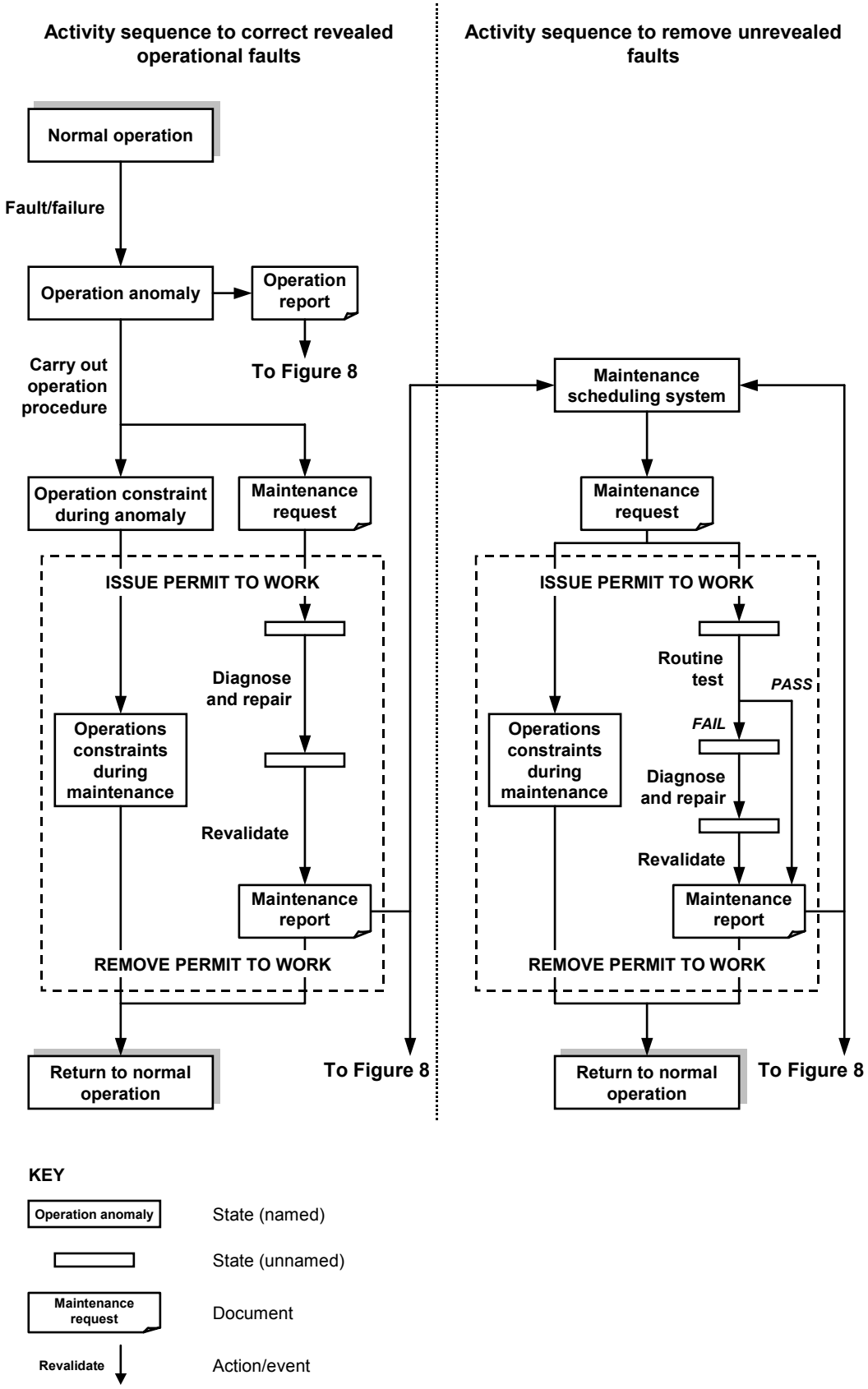


Figure 7 – Example of operations and maintenance activities model

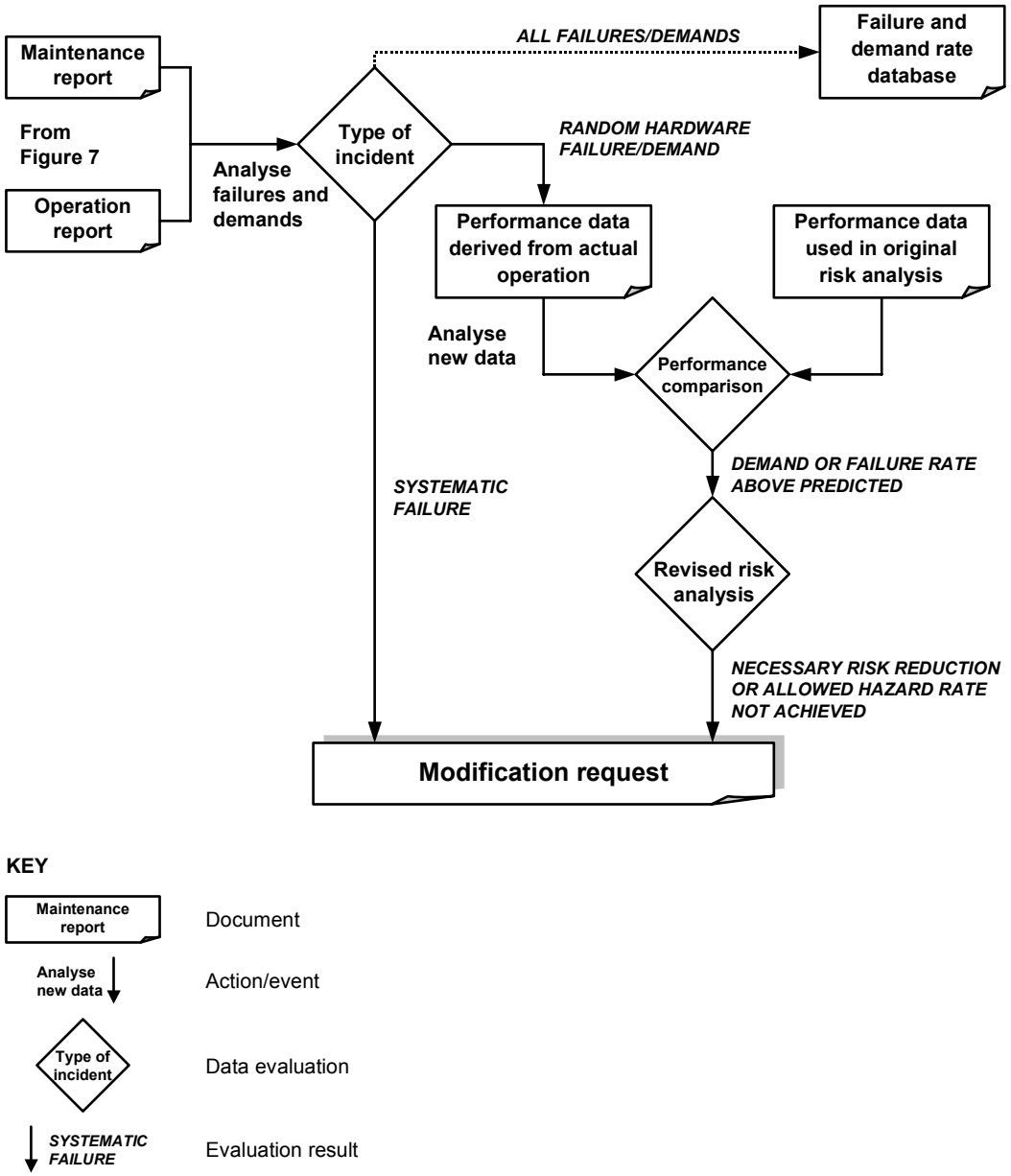


Figure 8 – Example of operation and maintenance management model

7.16 Overall modification and retrofit

NOTE 1 This phase is Box 15 of Figure 2.

NOTE 2 The organizational measures dealt with in this subclause provide for the effective implementation of the technical requirements, and are solely aimed at the achievement and maintenance of functional safety of the E/E/PE safety-related systems. The technical requirements necessary for maintaining functional safety will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.

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

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

7.16.1 Objective

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

7.16.2 Requirements

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

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

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

– the determined hazards that may be affected;

– the proposed change (both hardware and software);

– the reasons for the change.

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

a) functional safety below that specified;

b) systematic fault experience;

c) new or amended safety legislation;

d) modifications to the EUC or its use;

e) modification to the overall safety requirements;

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

g) routine functional safety audits.

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

7.16.2.4 The results described in 7.16.2.3 shall be documented.

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

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

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

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

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

– the modification or retrofit request;

– the impact analysis;

– reverification and revalidation of data and results;

– all documents affected by the modification and retrofit activity.

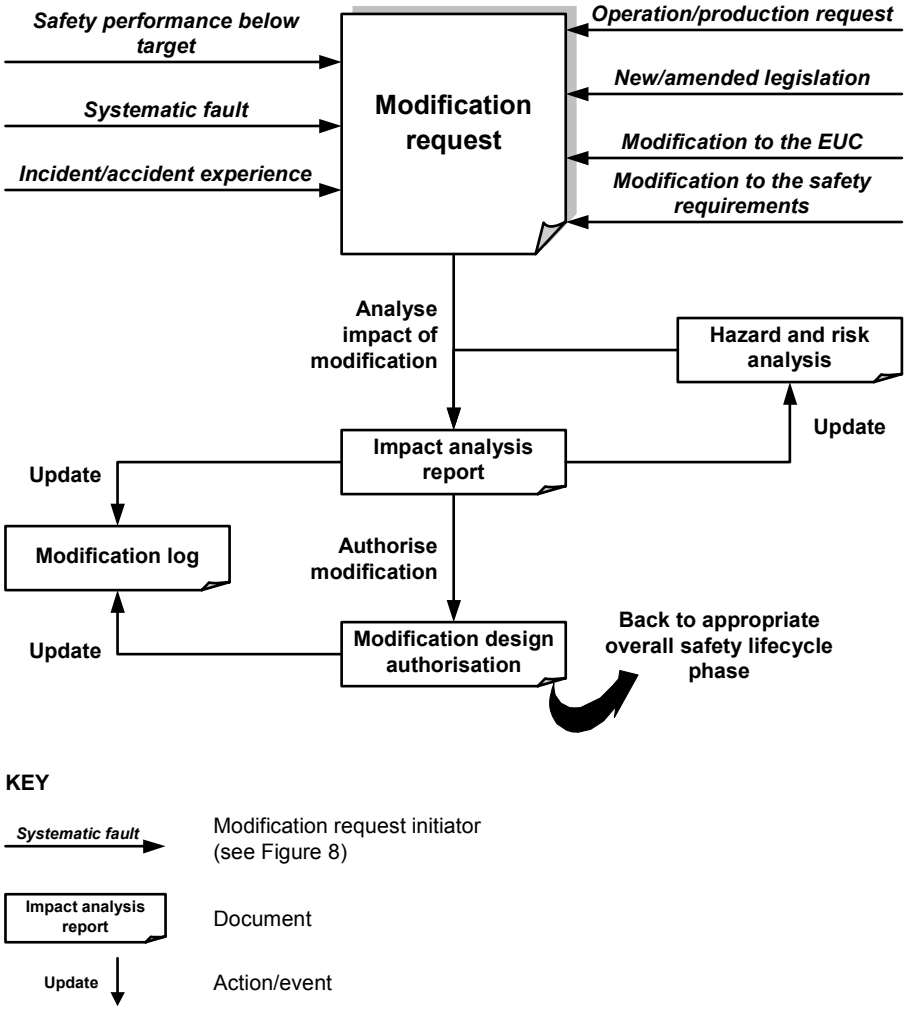


Figure 9 – Example of modification procedure model

7.17 Decommissioning or disposal

NOTE 1 This phase is Box 16 of Figure 2.

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

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

7.17.1 Objective

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

7.17.2 Requirements

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

7.17.2.2 The results described in 7.17.2.1 shall be documented.

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

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

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

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

– dismantling the E/E/PE safety-related systems.

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

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

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

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

– the plan used for the decommissioning or disposal activities;

– the impact analysis.

7.18 Verification

7.18.1 Objective

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

7.18.2 Requirements

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

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

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

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

The factors could include, for example

– size of project;

– degree of complexity;

– degree of novelty of design;

– degree of novelty of technology.

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

8 Functional safety assessment

8.1 Objective

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

8.2 Requirements

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

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

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

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

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

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

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

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

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

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

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

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

– the work done since the previous functional safety assessment;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

– X1 and X2: see 8.2.16.

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

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

– lack of previous experience with a similar design;

– greater degree of complexity;

– greater degree of novelty of design;

– greater degree of novelty of technology.

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

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

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

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

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

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

– Consequence C: death to several people;

– Consequence D: very many people killed.

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

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

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 2))

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

Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 9 and 10, including all phases of E/E/PE system and software safety lifecycles (see Figures 2, 3 and 4))

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

Annex A
(informative)

Example of a documentation structure

A.1 General

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

– each phase of the overall, E/E/PE system and software safety lifecycles;
– the management of functional safety (Clause 6);
– functional safety assessments (Clause 8).

What constitutes sufficient information will be dependent upon a number of factors, including the complexity and size of the E/E/PE safety-related systems and the requirements relating to the specific application. The necessary documentation may be specified in product and application specific international standards.

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

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

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

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

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

– **document kind**;
– **activity or object**.

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

The basic document kinds specified in this annex are

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

– **instruction** – specifies in detail the instructions as to when and how to perform certain jobs (for example operator instruction);

– **plan** – specifies the plan as to when, how and by whom specific activities shall be performed (for example maintenance plan);

– **diagram** – specifies the function by means of a diagram (symbols and lines representing signals between the symbols);

– **list** – provides information in a list form (for example code list, signal list);

– **log** – provides information on events in a chronological log form;

– **report** – describes the results of activities such as investigations, assessments, tests etc. (for example test report);

– **request** – provides a description of requested actions that have to be approved and further specified (for example maintenance request).

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

A.2 Safety lifecycle document structure

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

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

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

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

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

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

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

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

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

A.3 Physical document structure

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

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

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

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

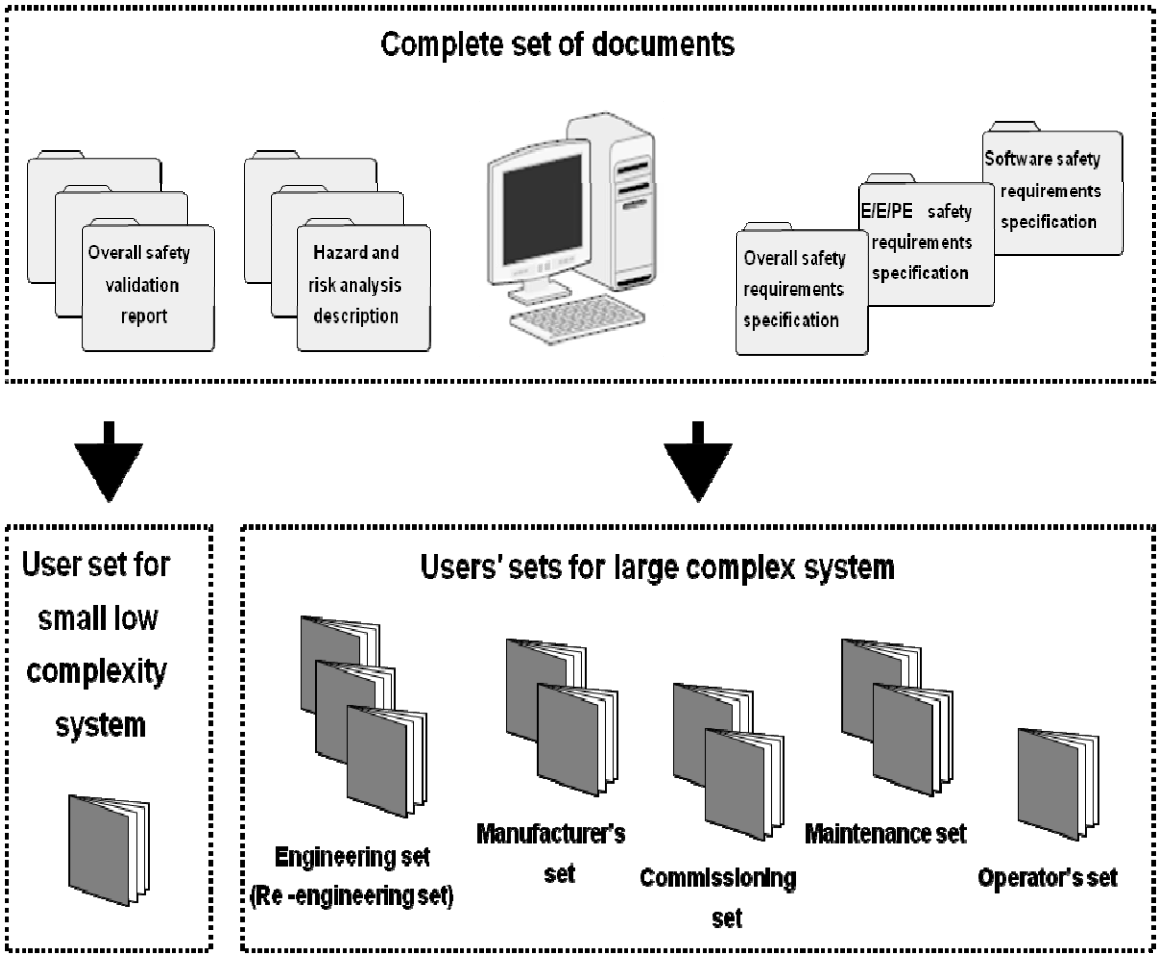


Figure A.1 – Structuring information into document sets for user groups

A.4 List of documents

The list of documents will typically include the following information:

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

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

Bibliography

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ –

Partie 1: Exigences générales

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61508-1 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition publiée en 1998 dont elle constitue une révision technique.

La présente édition a fait l'objet d'une révision approfondie et intègre de nombreux commentaires reçus lors des différentes phases de révision.

Elle a le statut d'une publication fondamentale de sécurité conformément au Guide CEI 104.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/548/FDIS	65A/572/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61508, présentées sous le titre général *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

Les systèmes comprenant des composants électriques et/ou électroniques sont utilisés depuis de nombreuses années pour exécuter des fonctions relatives à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (dénommés de manière générique systèmes électroniques programmables) sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non relatives à la sécurité, mais aussi de plus en plus souvent relatives à la sécurité. Si l'on veut exploiter efficacement et en toute sécurité la technologie des systèmes informatiques, il est indispensable de fournir à tous les responsables suffisamment d'éléments relatifs à la sécurité pour les guider dans leurs prises de décisions.

La présente Norme internationale présente une approche générique de toutes les activités liées au cycle de vie de sécurité de systèmes électriques et/ou électroniques et/ou électroniques programmables (E/E/PE) qui sont utilisés pour réaliser des fonctions de sécurité. Cette approche unifiée a été adoptée afin de développer une politique technique rationnelle et cohérente concernant tous les systèmes électriques relatifs à la sécurité. Un objectif principal de cette approche est de faciliter le développement de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508.

NOTE 1 Des exemples de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508 sont donnés dans la Bibliographie (voir références [1], [2] et [3]).

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes fondés sur diverses technologies (par exemple mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). En conséquence, toute stratégie de sécurité doit non seulement prendre en compte tous les éléments d'un système individuel (par exemple, les capteurs, les appareils de commande et les actionneurs), mais également prendre en considération tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. Par conséquent, la présente Norme internationale, bien que traitant des systèmes E/E/PE relatifs à la sécurité, peut aussi fournir un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

Il est admis qu'il existe une grande variété d'applications utilisant des systèmes E/E/PE relatifs à la sécurité dans un grand nombre de secteurs, et couvrant un large éventail de complexité et de potentiel de dangers et de risques. Pour chaque application particulière, les mesures de sécurité requises dépendent de nombreux facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rend désormais possible la prescription de ces mesures dans les futures normes internationales de produit et d'application sectorielle, ainsi que dans les révisions des normes déjà existantes.

La présente Norme internationale

– concerne toutes les phases appropriées du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel (par exemple, depuis la conceptualisation initiale, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service) lorsque les systèmes E/E/PE permettent d'exécuter des fonctions de sécurité,
– a été élaborée dans le souci de la prise en compte de l'évolution rapide des technologies; le cadre fourni par la présente Norme internationale est suffisamment solide et étendu pour pourvoir aux évolutions futures,
– permet l'élaboration de normes internationales de produit et d'application sectorielle concernant les systèmes E/E/PE relatifs à la sécurité; il convient que l'élaboration de normes internationales de produit et d'application sectorielle dans le cadre de la présente norme, permette d'atteindre un haut niveau de cohérence (par exemple, pour ce qui est des principes sous-jacents, de la terminologie, etc.) à la fois au sein de chaque secteur d'application, et d'un secteur à l'autre. La conséquence en sera une amélioration en termes de sécurité et de gains économiques,
– fournit une méthode de définition d'une spécification des exigences de sécurité nécessaire pour obtenir la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité,

– adopte une approche basée sur les risques qui permet de déterminer les exigences en matière d'intégrité de sécurité,

– introduit les niveaux d'intégrité de sécurité pour la spécification du niveau cible d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes E/E/PE relatifs à la sécurité,

NOTE 2 La norme ne spécifie aucune exigence de niveau d'intégrité de sécurité pour aucune fonction de sécurité, ni comment le niveau d'intégrité de sécurité est déterminé. Elle fournit en revanche un cadre conceptuel basé sur les risques, ainsi que des exemples de méthodes.

– fixe des objectifs chiffrés de défaillance pour les fonctions de sécurité exécutées par les systèmes E/E/PE relatifs à la sécurité, qui sont en rapport avec les niveaux d'intégrité de sécurité,

– fixe une limite inférieure pour les objectifs chiffrés de défaillance pour une fonction de sécurité exécutée par un système E/E/PE relatif à la sécurité unique. Pour des systèmes E/E/PE relatifs à la sécurité fonctionnant

  – en mode de fonctionnement à faible sollicitation, la limite inférieure est fixée pour une probabilité moyenne de défaillance dangereuse de 10^{-5} en cas de sollicitation,

  – en mode de fonctionnement continu ou à sollicitation élevée, la limite inférieure est fixée à une fréquence moyenne de défaillance dangereuse de 10^{-9} [h^{-1}],

NOTE 3 Un système E/E/PE relatif à la sécurité unique n'implique pas nécessairement une architecture à un seul canal.

NOTE 4 Dans le cas de systèmes non complexes, il peut être possible de concevoir des systèmes relatifs à la sécurité ayant des valeurs plus basses pour l'intégrité de sécurité cible. Il est toutefois considéré que ces limites représentent ce qui peut être réalisé à l'heure actuelle pour des systèmes relativement complexes (par exemple, des systèmes électroniques programmables relatifs à la sécurité).

– établit des exigences fondées sur l'expérience et le jugement acquis dans le domaine des applications industrielles afin d'éviter des anomalies systématiques ou pour les maintenir sous contrôle. Même si, en général, la probabilité d'occurrence des défaillances systématiques ne peut être quantifiée, la norme permet cependant pour une fonction de sécurité spécifique, de déclarer que l'objectif chiffré de défaillance associé à cette fonction de sécurité peut être réputé atteint si toutes les exigences de la norme sont remplies,

– introduit une capabilité systématique s'appliquant à un élément du fait qu'il permet d'assurer que l'intégrité de sécurité systématique satisfait aux exigences du niveau d'intégrité de sécurité spécifié,

– adopte une large gamme de principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, mais n'utilise pas de manière explicite le concept de sécurité intrinsèque. Les principes de « sécurité intrinsèque » peuvent toutefois être applicables, l'adoption de ces concepts étant par ailleurs acceptable sous réserve de la satisfaction aux exigences des articles concernés de la norme.

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ –

Partie 1: Exigences générales

1 Domaine d'application

1.1 La présente Norme internationale traite des aspects à prendre en considération lors de l'utilisation de systèmes électriques/électroniques/électroniques programmables (E/E/PE) pour exécuter des fonctions de sécurité. L'un des objectifs majeurs de la présente norme est de permettre l'élaboration par les comités d'études qui en sont responsables de normes internationales de produit et d'application sectorielle. Cela permet de prendre pleinement en compte l'ensemble des facteurs pertinents associés au produit ou à l'application, et donc de répondre aux besoins spécifiques des utilisateurs du produit et du secteur d'application concernés. Un second objectif de la présente norme est de permettre le développement de systèmes E/E/PE relatifs à la sécurité en l'absence de normes internationales de produit ou d'application sectorielle.

1.2 En particulier, la présente norme

a) s'applique aux systèmes relatifs à la sécurité lorsqu'un ou plusieurs de ces systèmes comporte(nt) des dispositifs électriques/électroniques/électroniques programmables,

NOTE 1 En ce qui concerne les systèmes E/E/PE relatifs à la sécurité de faible complexité, certaines exigences décrites dans la présente norme peuvent ne pas être nécessaires et une exemption de conformité à de telles exigences est possible (voir 4.2, et la définition d'un système E/E/PE relatif à la sécurité de faible complexité en 3.4.3 de la CEI 61508-4).

NOTE 2 Bien qu'une personne physique puisse faire partie d'un système relatif à la sécurité (voir 3.4.1 de la CEI 61508-4), les exigences concernant le facteur humain dans la conception de systèmes E/E/PE relatifs à la sécurité ne sont pas détaillées dans la présente norme.

b) est génériquement basée sur et applicable à tous les systèmes E/E/PE relatifs à la sécurité, indépendamment de l'application,

c) couvre l'occurrence d'un risque tolérable engendré par l'application de systèmes E/E/PE relatifs à la sécurité, mais ne couvre pas les dangers qui découlent de l'équipement E/E/PE lui-même (par exemple, choc électrique),

d) s'applique à tous les types de systèmes E/E/PE relatifs à la sécurité, y compris les systèmes de protection et de commande,

e) ne couvre pas les systèmes E/E/PE lorsque

   – un système E/E/PE unique est capable par lui-même de pallier le risque tolérable, et

   – l'intégrité de sécurité requise des fonctions de sécurité du système E/E/PE unique est moindre que celle spécifiée pour le niveau 1 d'intégrité de sécurité (niveau d'intégrité de sécurité le plus faible décrit dans la présente norme),

f) traite principalement des systèmes E/E/PE relatifs à la sécurité dont la défaillance pourrait avoir un impact sur la sécurité des personnes et/ou sur l'environnement; cependant, les défaillances peuvent avoir des conséquences économiques sévères, et dans de pareils cas, la présente norme peut être utilisée pour prescrire tout système E/E/PE utilisé pour protéger l'équipement ou le produit,

NOTE 3 Voir 3.1.1 de la CEI 61508-4.

g) considère les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque de façon à ce que la spécification des exigences de sécurité pour les systèmes E/E/PE relatifs à la sécurité puisse être déterminée en étant basée systématiquement sur le risque,

h) utilise, en tant que cadre technique, un modèle de cycle de vie de sécurité global pour traiter, de façon systématique, des activités nécessaires pour assurer la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité,

NOTE 4 Bien que le cycle de vie de sécurité global concerne avant tout les systèmes E/E/PE relatifs à la sécurité, il peut aussi fournir un cadre technique pour l'étude de tout système relatif à la sécurité, indépendamment de la technologie employée par ce système (par exemple, mécanique, hydraulique ou pneumatique).

i) ne spécifie pas les niveaux d'intégrité de sécurité requis pour les applications sectorielles (ces niveaux doivent être basés sur des informations détaillées et une bonne connaissance de l'application sectorielle). Les comités d'études responsables des secteurs d'application spécifiques doivent spécifier, si nécessaire, les niveaux d'intégrité de sécurité dans les normes sectorielles,

j) spécifie des exigences générales pour les systèmes E/E/PE relatifs à la sécurité en l'absence de normes internationales de produit ou d'application sectorielle,

k) nécessite de prendre en considération au cours de l'analyse des dangers et des risques, les actions malveillantes et non autorisées. L'étendue de l'analyse comprend toutes les phases pertinentes du cycle de vie de sécurité,

NOTE 5 D'autres normes CEI/ISO traitent de ce sujet en profondeur; voir ISO/CEI/TR 19791 et la série CEI 62443.

l) ne traite pas des mesures préventives qu'il peut être nécessaire de prendre afin d'éviter que des personnes non autorisées altèrent, et/ou exercent, d'une manière quelconque, une activité dommageable pour la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité (voir k) ci-dessus),

m) ne spécifie pas les exigences relatives au développement, à la mise en oeuvre, à la maintenance et/ou à l'application de politiques ou de services de sécurité nécessaires pour satisfaire à une politique de sécurité donnée, susceptible d'être requise par le système E/E/PE relatif à la sécurité,

n) ne s'applique pas aux appareils médicaux conformes à la série CEI 60601.

1.3 La présente partie de la série de normes CEI 61508 définit les exigences générales qui sont applicables à toutes les parties. Les autres parties de la série CEI 61508 traitent de sujets plus spécifiques:

– les parties 2 et 3 fournissent des exigences supplémentaires et spécifiques pour les systèmes E/E/PE relatifs à la sécurité (pour le matériel et le logiciel),

– la partie 4 donne les définitions et les abréviations qui sont utilisées tout au long de la présente norme,

– la partie 5 fournit des lignes directrices concernant l'application de la partie 1 pour la détermination des niveaux d'intégrité de sécurité, en présentant des exemples de méthodes,

– la partie 6 fournit des lignes directrices concernant l'application des parties 2 et 3,

– la partie 7 contient une présentation des techniques et des mesures.

1.4 Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont des publications fondamentales de sécurité, bien que ce statut ne soit pas applicable dans le contexte des systèmes E/E/PE de faible complexité relatifs à la sécurité (voir 3.4.3 de la CEI 61508-4). En tant que publications fondamentales de sécurité, ces normes sont destinées à être utilisées par les comités d'études pour la préparation des normes conformément aux principes contenus dans le Guide CEI 104 et le Guide ISO/CEI 51. Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont également destinées à être utilisées comme publications autonomes. La fonction de sécurité horizontale de la présente norme internationale ne s'applique pas aux appareils médicaux conformes à la série CEI 60601.

NOTE Une des responsabilités incombant à un comité d'études consiste, dans toute la mesure du possible, à utiliser les publications fondamentales de sécurité pour la préparation de ses publications. Dans ce contexte, les exigences, les méthodes ou les conditions d'essai de cette publication fondamentale de sécurité ne s'appliquent que si elles sont indiquées spécifiquement ou incluses dans les publications préparées par ces comités d'études.

1.5 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-1 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

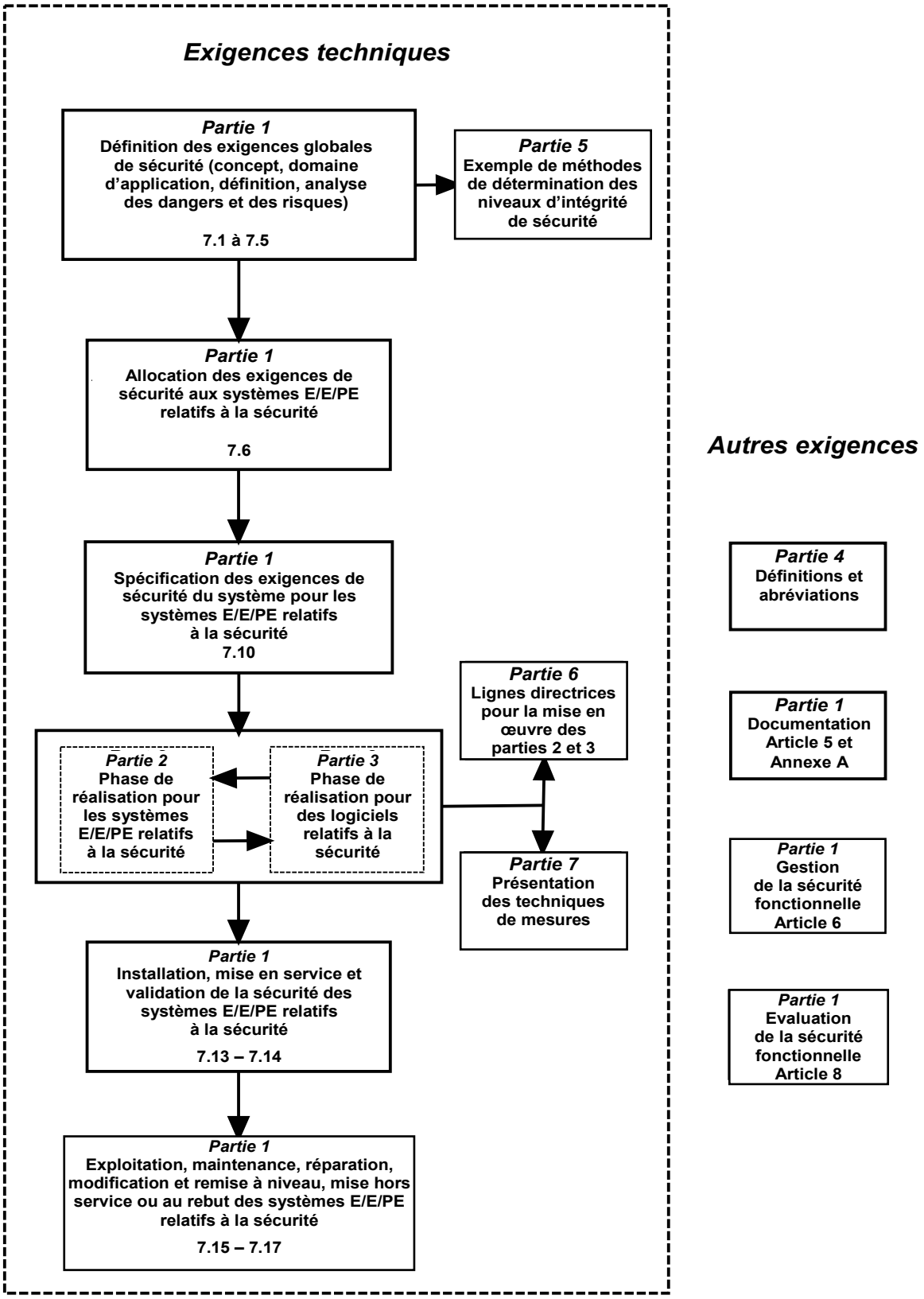


Figure 1 – Structure générale de la série CEI 61508

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences concernant les systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

CEI 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

Guide CEI 104:1997, *Elaboration des publications de sécurité et utilisation des publications fondamentales de sécurité et publications groupées de sécurité*

Guide ISO/CEI 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

3 Définitions et abréviations

Pour les besoins du présent document, les définitions et les abréviations données dans la CEI 61508-4 s'appliquent.

4 Conformité à la présente norme

4.1 Pour pouvoir déclarer la conformité à la présente norme, il doit être démontré que toutes les exigences pertinentes ont été satisfaites pour les critères requis spécifiés (par exemple, le niveau d'intégrité de sécurité), et que, par conséquent, pour chaque article ou paragraphe, que tous les objectifs ont été atteints.

4.2 La présente norme spécifie les exigences pour les systèmes E/E/PE relatifs à la sécurité et elle a été développée pour couvrir tous les niveaux de complexité associés à ces systèmes. Cependant, pour les systèmes E/E/PE relatifs à la sécurité de faible complexité (voir 3.4.3 de la CEI 61508-4) pour lesquels une solide expérience en exploitation apporte la confiance nécessaire pour assurer que l'intégrité de sécurité requise peut être réalisée, les options suivantes sont envisageables:

– dans les normes internationales de produit et d'application sectorielle mettant en œuvre les exigences de la CEI 61508-1 à la CEI 61508-7, certaines exigences peuvent ne pas être nécessaires et il est acceptable de ne pas satisfaire à de telles exigences,
– si la présente norme est directement utilisée dans les cas où il n'existe pas de norme internationale de produit ou d'application sectorielle, certaines exigences spécifiées dans la présente norme peuvent ne pas être nécessaires et l'exemption de conformité avec de telles exigences est acceptable à condition d'être dûment justifiée.

4.3 Les normes internationales de produit ou d'application sectorielle pour les systèmes E/E/PE relatifs à la sécurité développées dans le cadre de la présente norme doivent prendre en compte les exigences du Guide ISO/CEI 51 et du Guide 104 de la CEI.

5 Documentation

5.1 Objectifs

5.1.1 Le premier objectif des exigences du présent article est de spécifier l'information qu'il est nécessaire de documenter afin que toutes les phases du cycle de vie de sécurité global du système E/E/PE et du logiciel puissent être exécutées efficacement.

5.1.2 Le second objectif des exigences du présent article est de spécifier l'information qu'il est nécessaire de documenter afin que les activités de gestion de la sécurité fonctionnelle (voir Article 6), de vérification (voir 7.18) et d'évaluation de la sécurité fonctionnelle (voir Article 8) puissent être exécutées efficacement.

NOTE 1 Les exigences documentaires de la présente norme se rapportent essentiellement à l'information en tant que telle plutôt qu'aux documents physiques. L'information peut ne faire partie d'aucun document physique, sauf si cela est explicitement demandé dans le paragraphe s'y rapportant.

NOTE 2 La documentation peut être disponible sous différentes formes (par exemple, sur papier, film, ou tout support de donnée pouvant être affiché sur des écrans).

NOTE 3 Voir Annexe A pour des exemples de structures de documentation possibles.

NOTE 4 Voir référence [7] dans la Bibliographie.

5.2 Exigences

5.2.1 Pour chaque phase réalisée du cycle de vie de sécurité global du système E/E/PE et du logiciel, la documentation doit contenir l'information nécessaire et suffisante à la réalisation efficace des phases suivantes et des activités de vérification.

NOTE Ce qui constitue l'information suffisante dépend d'un certain nombre de facteurs, y compris de la complexité et la taille des systèmes E/E/PE relatifs à la sécurité et les exigences relatives à l'application spécifique.

5.2.2 La documentation doit contenir l'information nécessaire et suffisante pour la gestion de la sécurité fonctionnelle (Article 6).

NOTE Voir notes en 5.1.2.

5.2.3 La documentation doit contenir l'information nécessaire et suffisante à la mise en œuvre d'une évaluation de la sécurité fonctionnelle, ainsi que l'information et les résultats provenant de toute évaluation de la sécurité fonctionnelle.

NOTE Voir notes en 5.1.2.

5.2.4 L'information à documenter doit être telle qu'elle est mentionnée dans les divers articles de la présente norme, sauf justification contraire ou doit être comme spécifié dans la norme internationale de produit ou d'application sectorielle appropriée à l'application.

5.2.5 La disponibilité de la documentation doit être suffisante pour permettre l'accomplissement des activités dans le respect des articles de la présente norme.

NOTE Chaque partie concernée ne doit détenir que l'information nécessaire à la réalisation d'une activité déterminée, requise par la présente norme.

5.2.6 La documentation doit:

– être concise et précise,
– être aisément compréhensible par les personnes qui doivent l'utiliser,
– être adaptée à son objectif,
– être accessible et actualisable.

5.2.7 La documentation ou l'ensemble des informations doivent comporter des titres ou des noms indiquant le domaine d'application de leurs contenus, et comporter un système d'indexation permettant un accès rapide aux informations requises dans la présente norme.

5.2.8 La structure de la documentation peut tenir compte des procédures de l'entreprise et des pratiques professionnelles de secteurs de produit ou d'application spécifiques.

5.2.9 Les documents ou l'ensemble des informations doivent comporter un index de révision (numéros de version) permettant d'identifier les différentes versions du document.

5.2.10 Les documents ou l'ensemble des informations doivent être structurés de façon à permettre la recherche d'informations pertinentes. Il doit être possible d'identifier la dernière révision (version) d'un document ou d'un ensemble d'informations.

NOTE La structure physique de la documentation est fonction d'un certain nombre de facteurs, comme la dimension du système, sa complexité et les exigences en matière d'organisation.

5.2.11 Tous les documents pertinents doivent faire l'objet de révisions, d'amendements, de revues et d'approbations, dans le cadre d'un plan approprié de maîtrise des documents.

NOTE Lorsque des outils de production automatique ou semi-automatique de la documentation sont utilisés, des procédures spéciales peuvent être nécessaires pour assurer que des mesures efficaces pour la gestion des versions ou d'autres aspects de la maîtrise des documents sont en place.

6 Gestion de la sécurité fonctionnelle

6.1 Objectifs

6.1.1 Le premier objectif des exigences du présent article est de spécifier en matière de gestion de la sécurité fonctionnelle les responsabilités des personnes en charge d'un système E/E/PE relatif à la sécurité, ou d'une ou de plusieurs phases du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel.

6.1.2 Le second objectif des exigences du présent article est de spécifier les activités devant être exécutées par les personnes ayant des responsabilités en matière de gestion de la sécurité fonctionnelle.

NOTE Les mesures organisationnelles dont traite le présent article permettent la mise en œuvre efficace des exigences techniques et ont pour unique but la réalisation et le maintien de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité. Les exigences techniques nécessaires au maintien de la sécurité fonctionnelle sont spécifiées comme partie intégrante des informations communiquées par le fournisseur du système E/E/PE relatif à la sécurité et de ses éléments et composants.

6.2 Exigences

6.2.1 Une entité responsable d'un système E/E/PE relatif à la sécurité, ou d'une ou de plusieurs phases du cycle de vie de sécurité global du système E/E/PE ou du logiciel, doit désigner une ou plusieurs personnes assumant la responsabilité globale:

– du système et des différentes phases de son cycle de vie,

– de la coordination des activités relatives à la sécurité exécutées au cours de ces phases,

– des interfaces entre ces phases et les autres phases exécutées par d'autres entités,

– de l'application des exigences de 6.2.2 à 6.2.11 et 6.2.13,

– de la coordination des évaluations de la sécurité fonctionnelle (voir 6.2.12 b) et Article 8) – notamment, lorsque les personnes qui procèdent à l'évaluation de la sécurité fonctionnelle ne sont pas les mêmes selon les phases – y compris la communication, la planification et l'intégration de la documentation, les jugements et les recommandations,

– de l'assurance de la réalisation et de la démonstration de la sécurité fonctionnelle conformément aux objectifs et aux exigences de la présente norme.

NOTE La responsabilité des activités relatives à la sécurité ou des phases du cycle de vie de sécurité peut être déléguée à d'autres personnes, notamment celles ayant une compétence appropriée, et différentes personnes peuvent assumer la responsabilité de différentes activités et exigences. Toutefois, il convient que la responsabilité de la coordination, et de la sécurité fonctionnelle globale, incombe à une ou à un petit nombre de personnes ayant une autorité de management suffisante.

6.2.2 La politique et la stratégie pour obtenir la sécurité fonctionnelle doivent être spécifiées, ainsi que les moyens pour évaluer sa réalisation et les moyens de communication de cette politique et de cette stratégie au sein de l'entité.

6.2.3 Toutes les personnes, tous les services et toutes les entités qui sont responsables de l'exécution des activités relevant des phases applicables du cycle de vie de sécurité global des systèmes E/E/PE ou des logiciels (y compris les personnes responsables de la vérification et de l'évaluation de la sécurité fonctionnelle et, le cas échéant, les autorités administratives ou les organismes de réglementation de la sécurité) doivent être identifiés, leurs responsabilités devant par ailleurs leur être pleinement et clairement communiquées.

6.2.4 Des procédures doivent être développées pour définir les informations devant être communiquées, entre les parties appropriées, ainsi que le support de communication utilisé.

NOTE Voir Article 5 pour les exigences relatives à la documentation.

6.2.5 Des procédures doivent être développées pour assurer rapidement un suivi et une prise en compte satisfaisante des recommandations ayant trait aux systèmes E/E/PE relatifs à la sécurité, y compris les recommandations issues:

a) de l'analyse des dangers et des risques (voir 7.4),

b) de l'évaluation de la sécurité fonctionnelle (voir Article 8),

c) des activités de vérification (voir 7.18),

d) des activités de validation (voir 7.8 et 7.14),

e) de la gestion de la configuration (voir 6.2.10, 7.16, CEI 61508-2 et CEI 61508-3),

f) du compte-rendu et de l'analyse des incidents (voir 6.2.6).

6.2.6 Des procédures doivent être développées pour assurer l'analyse de tous les événements dangereux détectés, ainsi que la formulation de recommandations visant à réduire autant que possible toute probabilité de répétition d'une occurrence.

6.2.7 Les exigences relatives aux audits de sécurité fonctionnelle réguliers doivent être spécifiées, y compris:

a) la fréquence des audits de sécurité fonctionnelle,

b) le degré d'indépendance des personnes chargées des audits,

c) les activités de documentation et de suivi nécessaires.

6.2.8 Des procédures doivent être développées pour:

a) procéder à des modifications des systèmes E/E/PE relatifs à la sécurité (voir 7.16.2.2),

b) obtenir l'approbation et l'autorisation nécessaires pour les modifications.

6.2.9 Des procédures doivent être développées pour maintenir des informations précises sur les dangers et les événements dangereux, les fonctions de sécurité et les systèmes E/E/PE relatifs à la sécurité.

6.2.10 Des procédures doivent être développées pour la gestion de configuration des systèmes E/E/PE relatifs à la sécurité pendant les phases du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel, y compris notamment

a) compte tenu des phases spécifiques, l'étape à laquelle un contrôle formel de configuration doit être mis en œuvre,

b) les procédures devant être utilisées pour identifier de façon unique toutes les parties constitutives d'un élément (matériel ou logiciel),

c) les procédures permettant d'éviter que des éléments non autorisés n'entrent en service.

6.2.11 Une formation et des informations destinées aux services d'urgence doivent être fournies le cas échéant.

6.2.12 Les personnes ayant une responsabilité pour l'une ou plusieurs des phases du cycle de vie de sécurité global des systèmes E/E/PE ou des logiciels doivent pour ces phases et conformément aux procédures définies en 6.2.1 à 6.2.11, spécifier toutes les activités techniques et de gestion qui sont nécessaires pour assurer la réalisation, la démonstration et le maintien de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, y compris:

a) les mesures choisies et les techniques utilisées pour satisfaire aux exigences d'un article ou d'un paragraphe spécifié (voir CEI 61508-2, CEI 61508-3 et 61508-6),

b) les activités d'évaluation de la sécurité fonctionnelle, ainsi que la méthode de démonstration de la réalisation de cette dernière aux personnes effectuant l'évaluation de cette sécurité (voir Article 8),

NOTE Il convient d'utiliser des procédures appropriées d'évaluation de la sécurité fonctionnelle pour définir

– le choix d'une entité ou d'une ou de plusieurs personnes appropriées, au degré d'indépendance approprié,

– l'élaboration et la modification de lignes directrices pour les évaluations de la sécurité fonctionnelle,

– le remplacement de personnes effectuant l'évaluation de la sécurité fonctionnelle à tout moment du cycle de vie d'un système,

– le règlement des litiges impliquant les personnes effectuant les évaluations de la sécurité fonctionnelle.

c) les procédures d'analyse des performances d'exploitation et de maintenance, en particulier pour

   – identifier les défauts systématiques qui pourraient compromettre la sécurité fonctionnelle, y compris les procédures utilisées pendant la maintenance périodique qui permettent de détecter les défauts récurrents,

   – évaluer si les fréquences de sollicitation et les taux de défaillance pendant l'exploitation et la maintenance sont conformes aux hypothèses formulées lors de la conception du système.

6.2.13 Des procédures doivent être développées pour assurer que toutes les personnes ayant les responsabilités définies conformément à 6.2.1 et 6.2.3 (c'est-à-dire également toutes les personnes impliquées dans toute activité du cycle de vie global des systèmes E/E/PE ou des logiciels, y compris les activités de vérification, gestion et évaluation de la sécurité fonctionnelle), doivent avoir les compétences appropriées (c'est-à-dire formation, connaissances techniques, expérience et qualifications) adaptées aux tâches spécifiques qu'elles doivent effectuer. Ces procédures doivent inclure les exigences relatives au renouvellement, à la mise à jour et à l'évaluation continue des compétences.

6.2.14 La pertinence des compétences doit être prise en considération en fonction de l'application particulière, compte tenu de tous les facteurs pertinents incluant:

a) les responsabilités de la personne,

b) le niveau de supervision requis,

c) les conséquences possibles dans le cas d'une défaillance des systèmes E/E/PE relatifs à la sécurité; plus les conséquences sont importantes, plus la spécification des compétences doit être rigoureuse,

d) les niveaux d'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité; plus les niveaux d'intégrité de sécurité sont élevés, plus la spécification des compétences doit être rigoureuse,

e) l'innovation dans la conception, les procédures de conception ou l'application; plus la conception, les procédures de conception ou l'application sont récentes ou innovantes, plus la spécification des compétences doit être rigoureuse,

f) l'expérience accumulée et sa pertinence vis–à-vis des tâches spécifiques devant être réalisées et de la technologie employée; plus le niveau de compétence requis est élevé, plus les compétences acquises par l'expérience et celles exigées pour réaliser les tâches spécifiques doivent être proches,

g) le type de compétence approprié aux circonstances (par exemple, qualifications, expérience, formation appropriée, et pratique ultérieure, ainsi que capacités de direction et de prise de décisions),

h) les connaissances d'ingénierie appropriées au secteur d'application et à la technologie,

i) les connaissances d'ingénierie de la sécurité appropriées à la technologie,

j) la connaissance du cadre légal et réglementaire concernant la sécurité,

k) l'adéquation des qualifications aux activités spécifiques à exécuter.

NOTE La Référence [8] de la Bibliographie comporte un exemple de méthode de gestion des compétences adaptée aux systèmes E/E/PE relatifs à la sécurité.

6.2.15 La compétence de toutes les personnes ayant des responsabilités définies conformément aux 6.2.1 et 6.2.3 doit être documentée.

6.2.16 Les activités spécifiées résultant de l'application de 6.2.2 à 6.2.15 doivent être mises en œuvre et surveillées.

6.2.17 Les fournisseurs de produits ou de services à une entité ayant une responsabilité globale pour l'une ou plusieurs des phases du cycle de vie de sécurité global des systèmes E/E/PE ou des logiciels (voir 6.2.1), doivent délivrer leurs produits ou services comme spécifié par cette entité, et doivent disposer d'un système de management de la qualité approprié.

6.2.18 Les activités relatives à la gestion de la sécurité fonctionnelle doivent être appliquées aux phases appropriées du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel (voir 7.1.1.5).

7 Exigences du cycle de vie de sécurité global

7.1 Généralités

7.1.1 Introduction

7.1.1.1 Afin de traiter de façon systématique toutes les activités nécessaires pour atteindre l'intégrité de sécurité requise pour les fonctions de sécurité exécutées par les systèmes E/E/PE relatifs à la sécurité, la présente norme adopte un cycle de vie de sécurité global (voir Figure 2) comme cadre technique.

NOTE Il convient d'utiliser le cycle de vie de sécurité global pour la déclaration de conformité à la présente norme, un cycle de vie de sécurité global différent de celui décrit dans la Figure 2 pouvant toutefois être utilisé sous réserve que les objectifs et les exigences de chaque article de la présente norme soient satisfaits.

7.1.1.2 Le cycle de vie de sécurité global englobe les moyens suivants permettant d'atteindre l'objectif de risque tolérable:

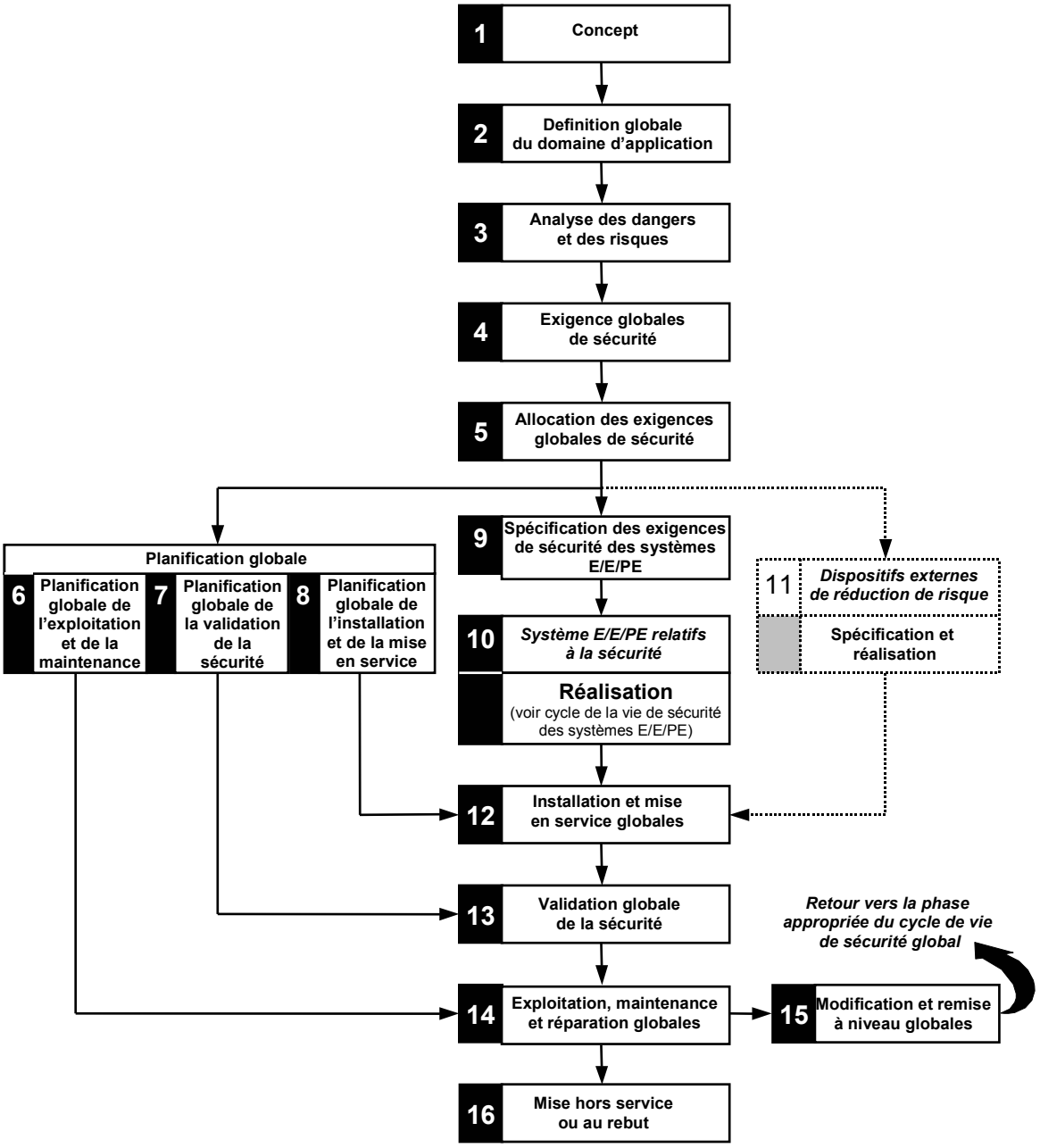
– des systèmes E/E/PE relatifs à la sécurité,

– des dispositifs externes de réduction de risque.

7.1.1.3 Une description développée de la phase de réalisation des systèmes E/E/PE relatifs à la sécurité à partir du cycle de vie de sécurité global est donnée dans la Figure 3. Cette partie du cycle de vie de sécurité des systèmes E/E/PE constitue le cadre technique applicable à la CEI 61508-2. La partie du cycle de vie de sécurité des logiciels illustrée à la Figure 4 constitue le cadre technique applicable à la CEI 61508-3. La Figure 5 illustre la relation entre le cycle de vie de sécurité global des systèmes E/E/PE et le cycle de vie de sécurité global des logiciels adaptés à ces systèmes.

7.1.1.4 Les figures du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel (Figures 2 à 4) constituent des représentations simplifiées de la réalité et ne représentent donc pas toutes les itérations correspondant à des phases spécifiques ou entre phases. Cependant, l'itération constitue une partie essentielle et vitale d'un développement qui utilise les cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel.

7.1.1.5 Les activités relatives à la gestion de la sécurité fonctionnelle (Article 6), à la vérification (7.18) et à l'évaluation de la sécurité fonctionnelle (Article 8) ne sont pas représentées sur les cycles de vie de sécurité globaux des systèmes E/E/PE ou des logiciels. Ce choix a été fait pour réduire la complexité des figures du cycle de vie. Lorsqu'elles sont requises, ces activités doivent être appliquées aux phases appropriées des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel.



NOTE 1 Les activités relatives à la ***vérification**, à la **gestion de la sécurité fonctionnelle*** et à l'***évaluation de la sécurité fonctionnelle*** ne sont pas représentées pour des raisons de clarté, mais concernent toutefois toutes les phases du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel.

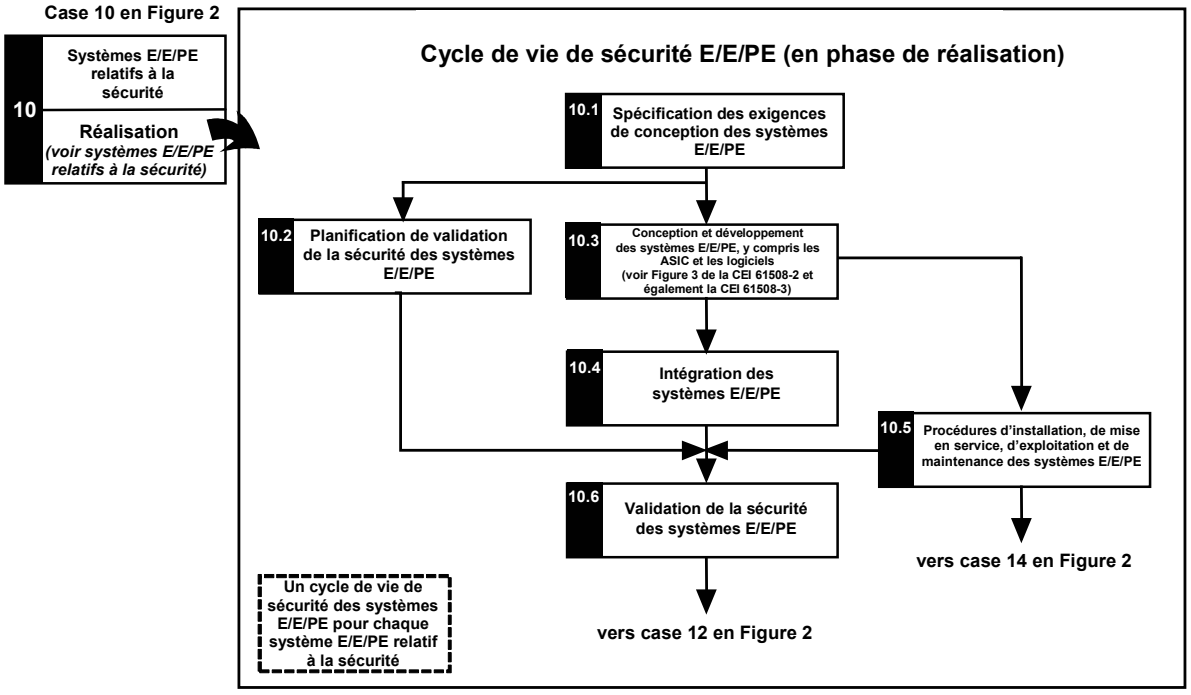
NOTE 2 La phase représentée par la case 11 ne relève pas du domaine d'application de la présente norme.

NOTE 3 La CEI 61508-2 et la CEI 61508-3 traitent de la case 10 (réalisation) mais traitent également le cas échéant, de l'électronique programmable (matériel et logiciel) des cases 13, 14 et 15.

NOTE 4 Voir le Tableau 1 pour une description des objectifs et du domaine d'application des phases représentées par chaque case.

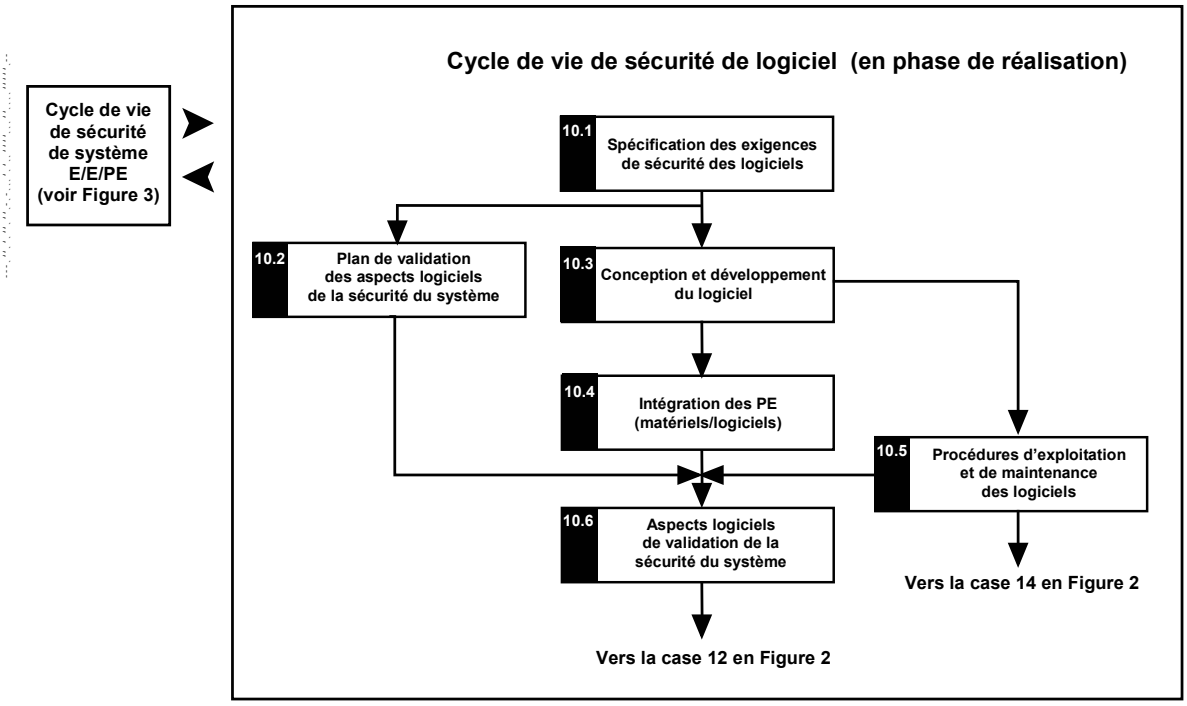
NOTE 5 Les exigences techniques nécessaires aux activités globales d'exploitation, maintenance, réparation, modification, remise à niveau et mise hors service ou mise au rebut sont spécifiées comme partie intégrante des informations communiquées par le fournisseur du système E/E/PE relatif à la sécurité et de ses éléments et composants.

Figure 2 – Cycle de vie de sécurité global



NOTE Cette figure montre uniquement les phases du cycle de vie de sécurité du système E/E/PE intégrées à la phase de réalisation du cycle de vie de sécurité global. Le cycle de vie de sécurité complet du système E/E/PE comporte également des occurrences, spécifiques au système E/E/PE relatif à la sécurité, des phases ultérieures du cycle de vie de sécurité global (cases 12 à 16 de la Figure 2).

Figure 3 – Cycle de vie de sécurité du système E/E/PE (en phase de réalisation)



NOTE Cette figure montre uniquement les phases du cycle de vie de sécurité du logiciel intégrées à la phase de réalisation du cycle de vie de sécurité global. Le cycle de vie de sécurité complet du logiciel comporte également des occurrences, spécifiques au logiciel adapté au système E/E/PE relatif à la sécurité, des phases ultérieures du cycle de vie de sécurité global (cases 12 à 16 de la Figure 2).

Figure 4 – Cycle de vie de sécurité du logiciel (en phase de réalisation)

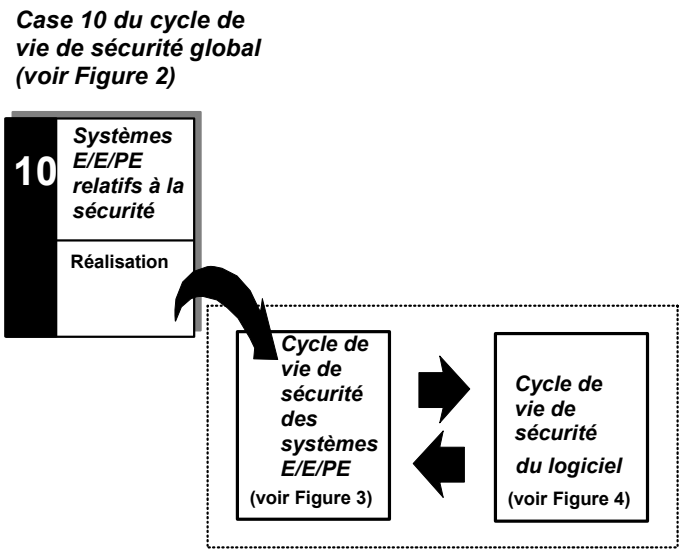


Figure 5 – Relation entre le cycle de vie de sécurité global du système E/E/PE et les cycles de vie de sécurité du logiciel

7.1.2 Objectifs et exigences – généralités

7.1.2.1 Les objectifs et les exigences relatifs aux phases du cycle de vie de sécurité global sont décrits de 7.2 à 7.17. Les objectifs et les exigences relatifs aux phases du cycle de vie de sécurité du système E/E/PE et du logiciel sont décrits respectivement dans la CEI 61508-2 et la CEI 61508-3.

NOTE Les paragraphes 7.2 à 7.17 se rapportent aux cases (phases) spécifiques de la Figure 2. La case spécifique est référencée dans des notes de ces paragraphes.

7.1.2.2 Pour toutes les phases du cycle de vie de sécurité global, le Tableau 1 indique:

– les objectifs à atteindre,
– le domaine d'application de la phase,
– la référence du paragraphe contenant les exigences,
– les données d'entrée requises de la phase,
– les données de sortie requises pour satisfaire aux exigences.

Tableau 1 – Cycle de vie de sécurité global – vue d'ensemble

Phase du cycle de vie de sécurité		Objectifs	Domaine d'application	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	**Titre**					
1	**Concept**	7.2.1: Développer un niveau de compréhension de l'EUC et son environnement (physique, légal, etc.) suffisant pour permettre aux autres activités du cycle de vie de sécurité d'être exécutées de façon satisfaisante.	L'EUC et son environnement (physique, légal, etc.).	7.2.2	Toute l'information appropriée nécessaire pour satisfaire aux exigences du paragraphe.	information concernant l'EUC, son environnement et les dangers associés.
2	**Définition globale du domaine d'application**	7.3.1: Déterminer les frontières de l'EUC et du système de commande de ce dernier, Spécifier le domaine d'application de l'analyse des dangers et des risques (par exemple, les processus dangereux, les dangers liés à l'environnement, etc.).	L'EUC et son environnement.	7.3.2	information concernant l'EUC, son environnement et les dangers associés.	Définition du domaine d'application de l'analyse des dangers et des risques.
3	**Analyse des dangers et des risques**	7.4.1: Déterminer les dangers, ainsi que les situations et événements dangereux relatifs à l'EUC et au système de commande de ce dernier (dans tous les modes de fonctionnement), pour toutes les situations raisonnablement prévisibles, y compris les conditions de défaut et de mauvais usage raisonnablement prévisibles (voir 3.1.14 de la CEI 61508-4), Déterminer les séquences d'événements menant aux événements dangereux, Déterminer les risques EUC associés aux événements dangereux.	Le domaine d'application dépend de la phase atteinte dans les cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel (dans la mesure où il peut se révéler nécessaire d'effectuer plus d'une analyse des dangers et des risques). Pour l'analyse préliminaire des dangers et des risques, le domaine d'application est déduit du résultat de la définition globale du domaine d'application.	7.4.2	Définition du domaine d'application de l'analyse des dangers et des risques.	Description et information relatives à l'analyse des dangers et des risques.
4	**Exigences globales de sécurité**	7.5.1: Développer la spécification des exigences globales de sécurité, en termes d'exigences relatives aux fonctions de sécurité et à l'intégrité de sécurité, pour les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque, afin d'obtenir la sécurité fonctionnelle requise.	Déduit du résultat de la définition globale du domaine d'application	7.5.2	Description et information relatives à l'analyse des dangers et des risques.	Spécification des exigences globales de sécurité en termes d'exigences relatives aux fonctions de sécurité et à l'intégrité de sécurité.

Tableau 1 *(suite)*

Phase du cycle de vie de sécurité		Objectifs	Domaine d'application	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	**Titre**					
5	**Allocation des exigences globales de sécurité**	7.6.1: Allouer les fonctions de sécurité, qui sont indiquées dans la spécification des exigences globales de sécurité (à la fois les exigences relatives aux fonctions de sécurité et les exigences relatives à l'intégrité de sécurité), aux systèmes E/E/PE relatifs à la sécurité désignés et aux dispositifs externes de réduction de risque, Allouer un niveau d'intégrité de sécurité à chaque fonction de sécurité devant être exécutée par un système E/E/PE relatif à la sécurité.	Déduit du résultat de la définition globale du domaine d'application	7.6.2	Spécification des exigences globales de sécurité en termes d'exigences relatives aux fonctions de sécurité et à l'intégrité de sécurité.	Information concernant l'allocation des fonctions globales de sécurité, leurs objectifs chiffrés de défaillance et les niveaux d'intégrité de sécurité associés Hypothèses formulées concernant les dispositifs externes de réduction de risque qui doivent être maîtrisés tout au long de la durée de vie de l'EUC (voir 7.6.2.13).
6	**Planification globale de l'exploitation et de la maintenance**	7.7.1: Développer un plan d'exploitation et de maintenance des systèmes E/E/PE relatifs à la sécurité, pour assurer que la sécurité fonctionnelle requise est maintenue pendant l'exploitation et la maintenance.	L'EUC, le système de commande de ce dernier et les facteurs humains, systèmes E/E/PE relatifs à la sécurité.	7.7.2	Information concernant l'allocation des fonctions globales de sécurité, leurs objectifs chiffrés de défaillance et les niveaux d'intégrité de sécurité associés Hypothèses formulées concernant les dispositifs externes de réduction de risque qui doivent être maîtrisés tout au long de la durée de vie de l'EUC (voir 7.6.2.13).	Un plan d'exploitation et de maintenance des systèmes E/E/PE relatifs à la sécurité.

Tableau 1 *(suite)*

Phase du cycle de vie de sécurité		Objectifs	Domaine d'application	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	**Titre**					
7	**Planification globale de la validation de la sécurité**	7.8.1: Développer un plan pour la validation globale de la sécurité des systèmes E/E/PE relatifs à la sécurité.	L'EUC, le système de commande de ce dernier et les facteurs humains, systèmes E/E/PE relatifs à la sécurité.	7.8.2	Information et résultats relatifs à l'allocation des exigences globales de sécurité.	Un plan pour la validation globale de la sécurité des systèmes E/E/PE relatifs à la sécurité.
8	**Planification globale de l'installation et de la mise en service**	7.9.1: Développer un plan pour que l'installation des systèmes E/E/PE relatifs à la sécurité soit maîtrisée, afin d'assurer que la sécurité fonctionnelle requise est obtenue, Développer un plan pour que la mise en service des systèmes E/E/PE relatifs à la sécurité soit maîtrisée, afin d'assurer que la sécurité fonctionnelle requise est obtenue.	L'EUC et le système de commande de ce dernier, systèmes E/E/PE relatifs à la sécurité.	7.9.2	Information et résultats relatifs à l'allocation des exigences globales de sécurité.	Un plan pour l'installation des systèmes E/E/PE relatifs à la sécurité, Un plan pour la mise en service des systèmes E/E/PE relatifs à la sécurité.
9	**Spécification des exigences de sécurité des systèmes E/E/PE**	7.10.1: Définir les exigences de sécurité des systèmes E/E/PE, en termes d'exigences relatives à la fonction de sécurité de ces systèmes et d'exigences d'intégrité de sécurité de ces mêmes systèmes, afin d'obtenir la sécurité fonctionnelle requise.	systèmes E/E/PE relatifs à la sécurité	7.10.2	Information et résultats relatifs à l'allocation des exigences globales de sécurité.	Spécification des exigences de sécurité relatives aux systèmes E/E/PE.
10	**Systèmes E/E/PE relatifs à la sécurité: réalisation**	7.11.1 et les parties 2 et 3: Créer des systèmes E/E/PE relatifs à la sécurité conformes à la spécification des exigences de sécurité des systèmes E/E/PE (comprenant la spécification des exigences relatives aux fonctions de sécurité de ces mêmes systèmes, ainsi que la spécification des exigences relatives à l'intégrité de sécurité de ces systèmes).	systèmes E/E/PE relatifs à la sécurité.	7.11.2, CEI 61508-2 et CEI 61508-3	Spécification des exigences de sécurité relatives aux systèmes E/E/PE.	Réalisation de chaque système E/E/PE relatif à la sécurité selon la spécification des exigences de sécurité des systèmes E/E/PE.

Tableau 1 *(suite)*

Phase du cycle de vie de sécurité		Objectifs	Domaine d'application	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	**Titre**					
11	**Dispositifs externes de réduction de risque: spécification et réalisation**	7.12.1: Créer des dispositifs externes de réduction de risque qui satisfont aux exigences relatives aux fonctions de sécurité et aux exigences relatives à l'intégrité de sécurité spécifiées pour de tels systèmes (hors du domaine d'application de la présente norme).	Dispositifs externes de réduction de risque.	7.12.2	Spécification des exigences de sécurité relatives aux dispositifs externes de réduction de risque (hors du domaine d'application de la présente norme et de ce fait non spécifié plus en détail dans cette dernière).	Réalisation de chaque dispositif externe de réduction de risque selon les exigences de sécurité applicables à cette mesure.
12	**Installation et mise en service globales**	7.13.1: Installer les systèmes E/E/PE relatifs à la sécurité, Mettre en service les systèmes E/E/PE relatifs à la sécurité.	L'EUC et le système de commande de ce dernier, systèmes E/E/PE relatifs à la sécurité.	7.13.2	Un plan pour l'installation des systèmes E/E/PE relatifs à la sécurité, Un plan pour la mise en service des systèmes E/E/PE relatifs à la sécurité.	Installation complète des systèmes E/E/PE relatifs à la sécurité, Mise en service complète des systèmes E/E/PE relatifs à la sécurité.
13	**Validation globale de la sécurité**	7.14.1: Valider le fait que les systèmes E/E/PE relatifs à la sécurité satisfont à la spécification relative aux exigences globales de sécurité en termes des exigences globales relatives aux fonctions de sécurité et aux exigences globales relatives à l'intégrité de sécurité, compte tenu de l'allocation des exigences de sécurité, pour les systèmes E/E/PE relatifs à la sécurité, effectuée selon 7.6.	L'EUC et le système de commande de ce dernier, systèmes E/E/PE relatifs à la sécurité.	7.14.2	Plan de validation globale de la sécurité des systèmes E/E/PE relatifs à la sécurité, information et résultats de l'allocation des exigences globales de sécurité.	Confirmation que tous les systèmes E/E/PE relatifs à la sécurité satisfont à la spécification relative aux exigences globales de sécurité, compte tenu de l'allocation des exigences de sécurité des systèmes E/E/PE relatifs à la sécurité.

Tableau 1 *(suite)*

Phase du cycle de vie de sécurité		Objectifs	Domaine d'application	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	**Titre**					
14	**Exploitation, maintenance et réparation globales**	7.15.1: Assurer que la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité est maintenue au niveau spécifié, Assurer que les exigences techniques, nécessaires à l'exploitation, la maintenance et la réparation globales des systèmes E/E/PE relatifs à la sécurité sont spécifiées et fournies aux personnes responsables de l'exploitation et de la maintenance futures de ces systèmes.	L'EUC et le système de commande de ce dernier, systèmes E/E/PE relatifs à la sécurité.	7.15.2	Plan d'exploitation et de maintenance globales des systèmes E/E/PE relatifs à la sécurité.	Réalisation permanente de la sécurité fonctionnelle requise pour les systèmes E/E/PE relatifs à la sécurité, Documentation chronologique de l'exploitation, la réparation et la maintenance des systèmes E/E/PE relatifs à la sécurité.
15	**Modification et remise à niveau globales**	7.16.1: Définir les procédures nécessaires pour assurer que la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité est appropriée, à la fois pendant et après la phase de modification et de remise à niveau.	L'EUC et le système de commande de ce dernier, systèmes E/E/PE relatifs à la sécurité.	7.16.2	Demande de modification ou de remise à niveau dans le cadre des procédures de gestion de la sécurité fonctionnelle.	Réalisation de la sécurité fonctionnelle requise pour les systèmes E/E/PE relatifs à la sécurité, à la fois pendant et après la phase de modification et de remise à niveau, Documentation chronologique de la modification et de la remise à niveau des systèmes E/E/PE relatifs à la sécurité.

Tableau 1 *(suite)*

Phase du cycle de vie de sécurité		Objectifs	Domaine d'application	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	**Titre**					
16	**Mise hors service ou au rebut**	7.17.1: Définir les procédures nécessaires pour assurer que la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité est appropriée aux circonstances pendant et après les activités de mise hors service ou au rebut de l'EUC.	L'EUC et le système de commande de ce dernier, systèmes E/E/PE relatifs à la sécurité.	7.17.2	Demande de mise hors service ou au rebut dans le cadre des procédures de gestion de la sécurité fonctionnelle.	Réalisation de la sécurité fonctionnelle requise pour les systèmes E/E/PE relatifs à la sécurité, à la fois pendant et après les activités de mise hors service ou au rebut, Documentation chronologique des activités de mise hors service ou au rebut.

7.1.3 Objectifs

7.1.3.1 Le premier objectif des exigences de ce paragraphe est de structurer, de façon systématique, les phases du cycle de vie de sécurité global qui doivent être prises en considération pour obtenir la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité.

7.1.3.2 Le second objectif des exigences de ce paragraphe est de documenter les informations essentielles, pertinentes pour la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, tout au long du cycle de vie de sécurité global.

NOTE Voir Article 5 pour les exigences en matière de documentation et l'Annexe A pour un exemple de structure de la documentation. Cette structure peut tenir compte des procédures de l'entreprise et des pratiques professionnelles de secteurs de produits ou d'application spécifiques.

7.1.4 Exigences

7.1.4.1 Le cycle de vie de sécurité global qui doit être utilisé comme base de déclaration de conformité à la présente norme est celui spécifié à la Figure 2. Si un autre cycle de vie de sécurité global est utilisé, il doit être spécifié dans le cadre de la gestion des activités liées à la sécurité fonctionnelle (voir Article 6) et tous les objectifs et exigences de chaque article ou paragraphe de la présente norme doivent être satisfaits.

NOTE Les éléments constitutifs du cycle de vie de sécurité du système E/E/PE et du cycle de vie de sécurité du logiciel qui forment la phase de réalisation du cycle de vie de sécurité global sont spécifiés dans la CEI 61508-2 et la CEI 61508-3 respectivement.

7.1.4.2 Les exigences relatives à la gestion de la sécurité fonctionnelle (voir Article 6) doivent être appliquées simultanément aux phases du cycle de vie de sécurité global.

7.1.4.3 Chaque phase du cycle de vie de sécurité global doit être appliquée et les exigences doivent être satisfaites, sauf justification contraire.

7.1.4.4 Chaque phase du cycle de vie de sécurité global doit être divisée en activités élémentaires avec, pour chaque phase, la spécification du domaine d'application, des entrées et des sorties.

7.1.4.5 Le domaine d'application et les entrées de chaque phase du cycle de vie de sécurité global doivent être tels que spécifiés dans le Tableau 1 sauf justification contraire dans le cadre de la gestion des activités liées à la sécurité fonctionnelle (voir Article 6) ou spécification dans la norme internationale de produit ou d'application sectorielle.

7.1.4.6 Les sorties de chaque phase du cycle de vie de sécurité global doivent être celles spécifiées dans le Tableau 1 sauf justification contraire dans le cadre de la gestion de la sécurité fonctionnelle (voir Article 6) ou spécification dans la norme internationale de produit ou d'application sectorielle.

7.1.4.7 Les sorties de chaque phase du cycle de vie de sécurité global doivent satisfaire aux objectifs et aux exigences spécifiés pour chaque phase (voir 7.2 à 7.17).

7.1.4.8 Les exigences de vérification qui doivent être respectées pour chaque phase du cycle de vie de sécurité global sont spécifiées en 7.18.

7.2 Concept

NOTE Cette phase correspond à la case 1 de la Figure 2.

7.2.1 Objectif

L'objectif des exigences définies dans ce paragraphe est de développer un niveau de compréhension de l'EUC et son environnement (physique, légal, etc.) suffisant pour permettre aux autres activités du cycle de vie de sécurité d'être exécutées de façon satisfaisante.

7.2.2 Exigences

7.2.2.1 Une connaissance approfondie de l'EUC, de ses fonctions de commande requises et de son environnement physique doit être acquise.

7.2.2.2 Les sources possibles de dangers, situations dangereuses et événements préjudiciables doivent être déterminées.

7.2.2.3 Les informations sur les dangers déterminés doivent être obtenues (par exemple, durée, intensité, toxicité, limite d'exposition, force mécanique, conditions explosives, réactivité, inflammabilité etc.).

7.2.2.4 Les informations sur les législations actuelles applicables en matière de sécurité (nationales et internationales) doivent être obtenues.

7.2.2.5 Les dangers, situations dangereuses et événements préjudiciables dus à l'interaction de l'EUC avec d'autres équipements ou systèmes (installés ou à installer) doivent être pris en considération avec les autres EUC (installés ou à installer).

7.2.2.6 Les informations et les résultats obtenus de 7.2.2.1 à 7.2.2.5 doivent être documentés.

7.3 Définition globale du domaine d'application

NOTE Cette phase correspond à la case 2 de la Figure 2.

7.3.1 Objectifs

7.3.1.1 Le premier objectif des exigences de ce paragraphe est de déterminer les frontières de l'EUC et de son système de commande.

7.3.1.2 Le second objectif des exigences de ce paragraphe est de spécifier le domaine d'application de l'analyse des dangers et des risques (par exemple, les processus dangereux, les dangers liés à l'environnement, etc.).

7.3.2 Exigences

7.3.2.1 Les frontières de l'EUC et de son système de commande doivent être définies de manière à inclure tous les équipements et systèmes (y compris les personnes le cas échéant) associés aux dangers et événements dangereux pertinents.

NOTE Plusieurs itérations entre la définition globale du domaine d'application et l'analyse des dangers et des risques peuvent se révéler nécessaires.

7.3.2.2 L'équipement physique, comprenant l'EUC et son système de commande, devant faire partie intégrante du domaine d'application de l'analyse des dangers et des risques doit être spécifié.

NOTE Se reporter aux références [9] et [10] dans la Bibliographie.

7.3.2.3 Les événements extérieurs devant être pris en compte dans l'analyse des dangers et des risques doivent être spécifiés.

7.3.2.4 Les équipements et les systèmes associés aux dangers et aux événements dangereux doivent être spécifiés.

7.3.2.5 Le type d'événements initiateurs qu'il est nécessaire de prendre en considération (par exemple, les défaillances de composants, les anomalies de procédure, l'erreur humaine, les mécanismes d'interdépendance entre défaillances qui peuvent être à l'origine d'événements dangereux) doit être spécifié.

7.3.2.6 Les informations et les résultats obtenus de 7.3.2.1 à 7.3.2.5 doivent être documentés.

7.4 Analyse des dangers et des risques

NOTE Cette phase correspond à la case 3 de la Figure 2.

7.4.1 Objectifs

7.4.1.1 Le premier objectif des exigences de ce paragraphe est de déterminer les dangers, situations dangereuses et événements dangereux relatifs à l'EUC et à son système de commande (dans tous les modes de fonctionnement) pour toutes les situations raisonnablement prévisibles, y compris les conditions de défaut et de mauvais usage raisonnablement prévisible (voir 3.1.4 de la CEI 61508-4).

7.4.1.2 Le second objectif des exigences de ce paragraphe est de déterminer les séquences d'événements menant aux événements dangereux déterminés en 7.4.1.1.

7.4.1.3 Le troisième objectif des exigences de ce paragraphe est de déterminer les risques EUC associés aux événements dangereux déterminés en 7.4.1.1.

NOTE 1 Ce paragraphe est nécessaire pour que les exigences de sécurité pour les systèmes E/E/PE relatifs à la sécurité soient fondées sur une approche systématique basée sur le risque. Cela ne peut être effectué qu'en prenant en considération l'EUC et son système de commande.

NOTE 2 Dans le cas d'applications où des hypothèses valides peuvent être formulées sur les risques associés aux événements dangereux et leurs conséquences, l'analyse requise dans ce paragraphe (et 7.5) peut être effectuée par les rédacteurs des versions d'application sectorielle de la présente norme, et elle peut être incluse dans des exigences simplifiées sous forme graphique. Des exemples de telles méthodes sont donnés dans les Annexes E et G de la CEI 61508-5.

7.4.2 Exigences

7.4.2.1 Une analyse des dangers et des risques doit être effectuée et elle doit prendre en compte l'information provenant de la phase de définition globale du domaine d'application (voir 7.3). Si des décisions, prises lors d'étapes ultérieures des phases du cycle de vie de sécurité global du système E/E/PE ou du logiciel, peuvent changer les bases sur lesquelles les premières décisions avaient été prises, alors une nouvelle analyse des dangers et des risques doit être effectuée.

NOTE 1 Pour des recommandations, voir les références [9] et [10] de la Bibliographie.

NOTE 2 A titre d'exemple illustrant le besoin de poursuivre l'analyse des dangers et des risques pendant tout le cycle de vie de sécurité global, considérons l'analyse d'un EUC qui comporte une soupape de sécurité. Une analyse des dangers et des risques peut déterminer deux séquences d'événements qui se rapportent respectivement à un défaut « soupape fermée » et à un défaut « soupape ouverte », menant à des événements dangereux. Cependant, lorsque la conception détaillée du système de commande de l'EUC commandant la soupape est analysée, un nouveau mode de défaillance - « soupape oscillante » - introduisant une nouvelle séquence d'événements menant à un événement dangereux peut être découvert.

7.4.2.2 L'attention doit porter sur l'élimination ou la réduction des dangers.

NOTE Bien que ne relevant pas du domaine d'application de la présente norme, il est extrêmement important que les dangers identifiés de l'EUC soient éliminés à la source, par exemple, par l'application de principes de sécurité intrinsèque et l'application de bonnes pratiques techniques.

7.4.2.3 Les dangers, situations dangereuses et événements dangereux relatifs à l'EUC et à son système de commande doivent être déterminés dans toutes les circonstances raisonnablement prévisibles (y compris les conditions de défaut, le mauvais usage raisonnablement prévisible et toute action malveillante ou non autorisée). Cela doit comprendre tout problème pertinent relevant du facteur humain et doit impliquer une attention toute particulière aux modes de fonctionnement anormaux ou peu fréquents de l'EUC. Si l'analyse des dangers identifie une action malveillante ou non autorisée, constituant par ailleurs une menace pour la sécurité, comme raisonnablement prévisible, il convient alors d'effectuer une analyse des menaces pour la sécurité.

NOTE 1 Pour un mauvais usage raisonnablement prévisible, voir 3.1.14 de la CEI 61508-4.

NOTE 2 Pour des recommandations concernant l'identification des dangers, y compris des recommandations pour la représentation et l'analyse des problèmes liés au facteur humain, se reporter à la référence [11] dans la bibliographie.

NOTE 3 Pour des recommandations concernant l'analyse des risques pour la sécurité, voir la série CEI 62443.

NOTE 4 Les actions malveillantes ou non autorisées couvrent les menaces pour la sécurité.

NOTE 5 Il convient également que l'analyse des dangers et des risques détermine si l'activation d'une fonction de sécurité suite à une sollicitation ou une action frauduleuse, génère un nouveau danger. Dans ce type de situation, il peut se révéler nécessaire de développer une nouvelle fonction de sécurité afin de prendre en considération ce danger.

7.4.2.4 Les séquences d'événements conduisant aux événements dangereux déterminés en 7.4.2.3 doivent être déterminées.

NOTE 1 Il convient d'étudier les séquences d'événements en tenant compte des décisions prises concernant la politique de sécurité et la gestion des risques.

NOTE 2 Il est en général profitable d'étudier si l'une des séquences d'événements peut être éliminée par des modifications dans la conception du procédé ou de l'équipement utilisé.

7.4.2.5 La probabilité d'occurrence des événements dangereux en ce qui concerne les conditions spécifiées en 7.4.2.3 doit être évaluée.

7.4.2.6 Les conséquences associées aux événements dangereux déterminés en 7.4.2.3 doivent être déterminées.

7.4.2.7 Le risque EUC doit être évalué ou estimé pour chaque événement dangereux déterminé.

7.4.2.8 Les exigences définies de 7.4.2.1 à 7.4.2.7 peuvent être satisfaites par l'application de techniques d'analyse des dangers et des risques qualitatives ou quantitatives (voir la CEI 61508-5).

7.4.2.9 Le caractère approprié des techniques et le degré nécessaire d'application de ces techniques dépendent d'un certain nombre de facteurs, tels que:

– les dangers spécifiques et leurs conséquences,
– la complexité de l'EUC et de son système de commande,
– le secteur d'application et ses bonnes pratiques reconnues,
– les exigences légales et celles régissant la sécurité,
– le risque EUC,
– la disponibilité de données précises sur lesquelles doit être basée l'analyse des dangers et des risques.

7.4.2.10 L'analyse des dangers et des risques doit considérer les points suivants:

– chaque événement dangereux déterminé et les composants qui y contribuent,
– les conséquences et la probabilité des séquences d'événements auxquelles chaque événement dangereux est associé,
– le risque tolérable pour chaque événement dangereux,
– les mesures prises pour réduire ou supprimer les dangers et les risques,
– les hypothèses formulées au cours de l'analyse des risques, y compris les fréquences de sollicitation et les taux de défaillance de l'équipement estimés; toute prise en compte des contraintes d'exploitation ou de l'intervention humaine doit être détaillée.

7.4.2.11 L'information et les résultats qui constituent l'analyse des dangers et des risques doivent être documentés.

7.4.2.12 L'information et les résultats qui constituent l'analyse des dangers et des risques doivent être maintenus à jour pour l'EUC et son système de commande tout au long du cycle de vie de sécurité global, depuis la phase d'analyse des dangers et des risques jusqu'à la phase de mise hors service ou au rebut.

NOTE La conservation de l'information, issue des résultats de la phase d'analyse des dangers et des risques, constitue le moyen essentiel de suivi des progrès observés relatifs aux problèmes actuels liés à l'analyse des dangers et des risques.

7.5 Exigences globales de sécurité

NOTE Cette phase correspond à la case 4 de la Figure 2.

7.5.1 Objectif

L'objectif des exigences de ce paragraphe est de développer la spécification relative aux exigences globales de sécurité, en termes d'exigences globales relatives aux fonctions de sécurité et d'exigences globales relatives à l'intégrité de sécurité, pour les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque, afin d'obtenir la sécurité fonctionnelle requise.

NOTE Dans les cas d'applications où des hypothèses valides peuvent être formulées sur les risques, les dangers potentiels, les événements préjudiciables et leurs conséquences, l'analyse requise dans ce paragraphe (et 7.4)

peut être effectuée par les rédacteurs des versions d'application sectorielle de la présente norme, et elle peut être incluse dans des exigences simplifiées sous forme graphique. Des exemples de telles méthodes sont donnés dans les Annexes E et F de la CEI 61508-5.

7.5.2 Exigences

7.5.2.1 Un regroupement de toutes les fonctions globales de sécurité nécessaires doit être développé sur la base des événements dangereux issus de l'analyse des dangers et des risques. Cela doit constituer la spécification des exigences globales de fonctions de sécurité.

NOTE 1 Il est nécessaire de créer une fonction globale de sécurité pour chaque événement dangereux.

NOTE 2 A ce stade, les fonctions globales de sécurité à exécuter ne sont pas spécifiées en des termes purement techniques dans la mesure où la méthode et la technologie de mise en œuvre des fonctions globales de sécurité ne sont connues que plus tard. Au cours de l'allocation des exigences globales de sécurité (voir 7.6), la description des fonctions de sécurité peut nécessiter une modification pour refléter la méthode de mise en œuvre spécifique.

EXEMPLE Prévenir toute augmentation de la température dans le récipient X au-dessus de 250 °C et prévenir tout dépassement de la vitesse de l'entraînement Y au-delà de 3 000 r/min constituent des exemples de fonctions globales de sécurité.

7.5.2.2 Si des menaces pour la sécurité ont été identifiées, il convient d'effectuer une analyse de vulnérabilité afin de spécifier les exigences de sécurité.

NOTE Des recommandations sont fournies dans la série CEI 62443.

7.5.2.3 Pour chaque fonction globale de sécurité, une exigence relative à l'intégrité de sécurité cible doit être déterminée, permettant ainsi de parvenir à l'objectif de risque tolérable. Chaque exigence peut être déterminée de manière quantitative et/ou qualitative. Cela doit constituer la spécification des exigences globales d'intégrité de sécurité.

NOTE 1 La spécification des exigences globales d'intégrité de sécurité constitue une étape intermédiaire vers la détermination des objectifs chiffrés de défaillance et des niveaux d'intégrité de sécurité associés pour les fonctions de sécurité devant être mises en œuvre par les systèmes E/E/PE relatifs à la sécurité. Certaines méthodes qualitatives utilisées pour déterminer les niveaux d'intégrité de sécurité (voir Annexes E et F de la CEI 61508-5) passent directement des paramètres de risque aux niveaux d'intégrité de sécurité. Dans de tels cas, les exigences relatives à l'intégrité de sécurité sont indiquées de manière implicite plutôt qu'explicite, dans la mesure où elles sont incluses dans la méthode elle-même.

NOTE 2 Il est possible de réduire le risque EUC en limitant les conséquences de l'événement dangereux (solution préférée) ou en réduisant la fréquence d'événements dangereux de l'EUC et de son système de commande (voir 7.5.2.4 ci-dessous).

NOTE 3 La réduction requise de la fréquence de l'événement dangereux peut être obtenue par l'adoption de mesures supplémentaires comprenant l'utilisation d'un ou de systèmes E/E/PE relatifs à la sécurité et/ou de dispositifs externes de réduction de risque, y compris d'autres systèmes techniques relatifs à la sécurité ou d'autres mesures dirigées telles que l'évacuation, l'occupation ou le temps d'exposition.

NOTE 4 Afin de satisfaire aux critères relatifs au risque tolérable, il peut être nécessaire lors de la détermination de l'intégrité de sécurité cible pour chaque fonction de sécurité de tenir compte du fait que les individus peuvent être exposés à des risques générés par d'autres sources.

NOTE 5 Dans les situations où une norme internationale de secteur d'application existe et comprend des méthodes appropriées pour déterminer directement les exigences relatives à l'intégrité de sécurité, des normes de cette nature peuvent alors être utilisées pour satisfaire aux exigences de ce paragraphe.

7.5.2.4 Les exigences globales relatives à l'intégrité de sécurité doivent être spécifiées en termes

– de réduction du risque requise pour parvenir à l'objectif de risque tolérable, ou

– de fréquence d'événements dangereux tolérable de manière à satisfaire à l'objectif de risque tolérable.

7.5.2.5 Si en évaluant le risque EUC, la fréquence moyenne de défaillances dangereuses d'une fonction unique du système de commande de l'EUC est déclarée comme étant inférieure à 10^{-5} défaillances dangereuses par heure, alors le système de commande de l'EUC doit être considéré comme un système de commande relatif à la sécurité soumis aux exigences de la présente norme.

NOTE Par exemple, si un taux de défaillances dangereuses compris entre 10^{-6} et 10^{-5} par heure est déclaré pour le système de commande de l'EUC, alors le système de commande de ce dernier est considéré comme un système E/E/PE relatif à la sécurité et les exigences appropriées au niveau d'intégrité de sécurité 1 devraient être satisfaites.

7.5.2.6 Lorsque les défaillances du système de commande de l'EUC entraînent une sollicitation d'un ou de plusieurs systèmes E/E/PE relatifs à la sécurité et/ou de dispositifs externes de réduction de risque, et lorsqu'il n'est pas prévu de désigner le système de commande de l'EUC comme étant un système relatif à la sécurité, les exigences suivantes doivent s'appliquer:

a) le taux de défaillance dangereuse déclaré pour le système de commande de l'EUC doit être conforté par les données acquises par l'un des moyens suivants:
   – une expérience en exploitation réelle du système de commande de l'EUC dans une application similaire,
   – une analyse de fiabilité effectuée conformément à une procédure reconnue,
   – une base de données industrielle sur la fiabilité d'équipements génériques,
b) le taux de défaillance dangereuse qui peut être déclaré pour le système de commande de l'EUC ne doit pas être inférieur à 10^{-5} défaillances dangereuses par heure,

NOTE 1 Voir 7.5.2.5.

c) tous les modes de défaillance dangereuse raisonnablement prévisibles du système de commande de l'EUC doivent être pris en compte lors de la définition de la spécification des exigences globales de sécurité,
d) le système de commande de l'EUC doit être indépendant des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque.

NOTE 2 En partant du principe que les systèmes relatifs à la sécurité ont été conçus pour garantir une intégrité de sécurité appropriée, et en tenant compte de la fréquence normale de sollicitation du système de commande de l'EUC, il n'est pas nécessaire de désigner le système de commande de l'EUC comme étant un système relatif à la sécurité (et, par conséquent, ses fonctions ne sont pas désignées comme étant des fonctions de sécurité dans le contexte de la présente norme). Dans certaines applications, notamment là où une très haute intégrité de sécurité est requise, il peut être pertinent de réduire la fréquence de sollicitation en concevant le système de commande de l'EUC de telle sorte qu'il ait un taux de défaillance plus faible que la normale. Dans de tels cas, si le taux de défaillance déclaré est inférieur à la limite la plus haute des objectifs d'intégrité de sécurité pour le niveau 1 d'intégrité de sécurité (voir Tableau 3), alors le système de commande devient un système relatif à la sécurité et les exigences de la présente norme s'appliquent.

NOTE 3 Voir 7.6.2.7 pour la signification du terme "indépendant".

7.5.2.7 Si les exigences de 7.5.2.6 a) à d) inclus ne peuvent être satisfaites, le système de commande de l'EUC doit être désigné comme étant un système relatif à la sécurité. Le niveau d'intégrité de sécurité des fonctions du système de commande de l'EUC doit être déterminé par le taux de défaillance dangereuse déclaré pour le système de commande de l'EUC, conformément au Tableau 3 (voir Note 3 du tableau 3). Dans de tels cas, les exigences spécifiées dans la présente norme et pertinentes pour le niveau d'intégrité de sécurité alloué doivent s'appliquer au système de commande de l'EUC.

NOTE Voir 7.5.2.5 et également 7.6.2.10.

7.6 Allocation des exigences globales de sécurité

NOTE Cette phase correspond à la case 5 de la Figure 2.

7.6.1 Objectifs

7.6.1.1 Le premier objectif des exigences de ce paragraphe est d'allouer les fonctions globales de sécurité qui sont indiquées dans la spécification des exigences globales de sécurité (à la fois les exigences globales relatives aux fonctions de sécurité et les exigences globales relatives à l'intégrité de sécurité), aux systèmes E/E/PE relatifs à la sécurité désignés et aux dispositifs externes de réduction de risque.

NOTE Les dispositifs externes de réduction de risque sont considérés nécessaires dans la mesure où l'allocation aux systèmes E/E/PE relatifs à la sécurité ne peut être effectuée tant que ces dispositifs externes de réduction de risque n'ont pas été pris en compte.

7.6.1.2 Le second objectif des exigences de ce paragraphe est d'allouer un objectif chiffré de défaillance et un niveau d'intégrité de sécurité associé à chaque fonction de sécurité devant être exécutée par un système E/E/PE relatif à la sécurité.

7.6.2 Exigences

7.6.2.1 Les systèmes relatifs à la sécurité désignés qui doivent être utilisés pour obtenir la sécurité fonctionnelle requise doivent être spécifiés. L'objectif de risque tolérable peut être atteint par

– les systèmes E/E/PE relatifs à la sécurité et/ou
– les dispositifs externes de réduction de risque.

NOTE La présente norme est applicable uniquement si l'objectif de risque tolérable est atteint au moins partiellement par un système E/E/PE relatif à la sécurité.

7.6.2.2 Lors de l'allocation des fonctions de sécurité globale aux systèmes E/E/PE relatifs à la sécurité désignés et aux dispositifs externes de réduction de risque, les compétences et les ressources disponibles pendant toutes les phases du cycle de vie de sécurité global doivent être considérées.

NOTE 1 L'ampleur de toutes les implications de l'utilisation de systèmes relatifs à la sécurité employant une technologie complexe est souvent sous-estimée. Par exemple, la mise en oeuvre de technologies complexes nécessite un niveau plus élevé de compétence à chaque phase, depuis la spécification jusqu'à l'exploitation et la maintenance. L'utilisation d'autres solutions technologiques plus simples peut avoir la même efficacité tout en présentant plusieurs avantages du fait de la complexité réduite.

NOTE 2 La disponibilité des compétences et ressources pour l'exploitation et la maintenance, ainsi que pour l'environnement d'exploitation, peut revêtir une importance critique dès qu'il s'agit d'assurer la sécurité fonctionnelle requise pendant l'exploitation réelle.

7.6.2.3 Chaque fonction de sécurité globale, associée à son exigence d'intégrité de sécurité globale associée et définie selon 7.5, doit être allouée à un ou plusieurs des systèmes E/E/PE relatifs à la sécurité désignés et/ou des dispositifs externes de réduction de risque de sorte que l'objectif de risque tolérable pour la fonction de sécurité soit atteint. Cette allocation étant itérative, s'il est établi que l'objectif de risque tolérable ne peut être atteint, alors les spécifications relatives au système de commande de l'EUC, aux systèmes E/E/PE relatifs à la sécurité désignés et aux dispositifs externes de réduction de risque, doivent être modifiées et l'allocation répétée.

NOTE 1 La décision d'allouer une fonction de sécurité globale spécifique à un ou plusieurs systèmes E/E/PE relatifs à la sécurité ou aux dispositifs externes de réduction de risque dépend de nombreux facteurs et notamment de l'exigence relative à son intégrité de sécurité globale. Plus l'exigence relative à l'intégrité de sécurité est astreignante, plus il est vraisemblable que la fonction de sécurité sera partagée par plusieurs systèmes E/E/PE relatifs à la sécurité et/ou dispositifs externes de réduction de risque.

NOTE 2 La Figure 6 présente l'approche adoptée pour l'allocation des exigences de sécurité globale.

7.6.2.4 L'allocation indiquée en 7.6.2.3 doit être effectuée de manière à ce que toutes les fonctions de sécurité globale soient allouées et que les objectifs chiffrés de défaillance soient définis pour chaque fonction de sécurité (sous condition des exigences spécifiées en 7.6.2.10).

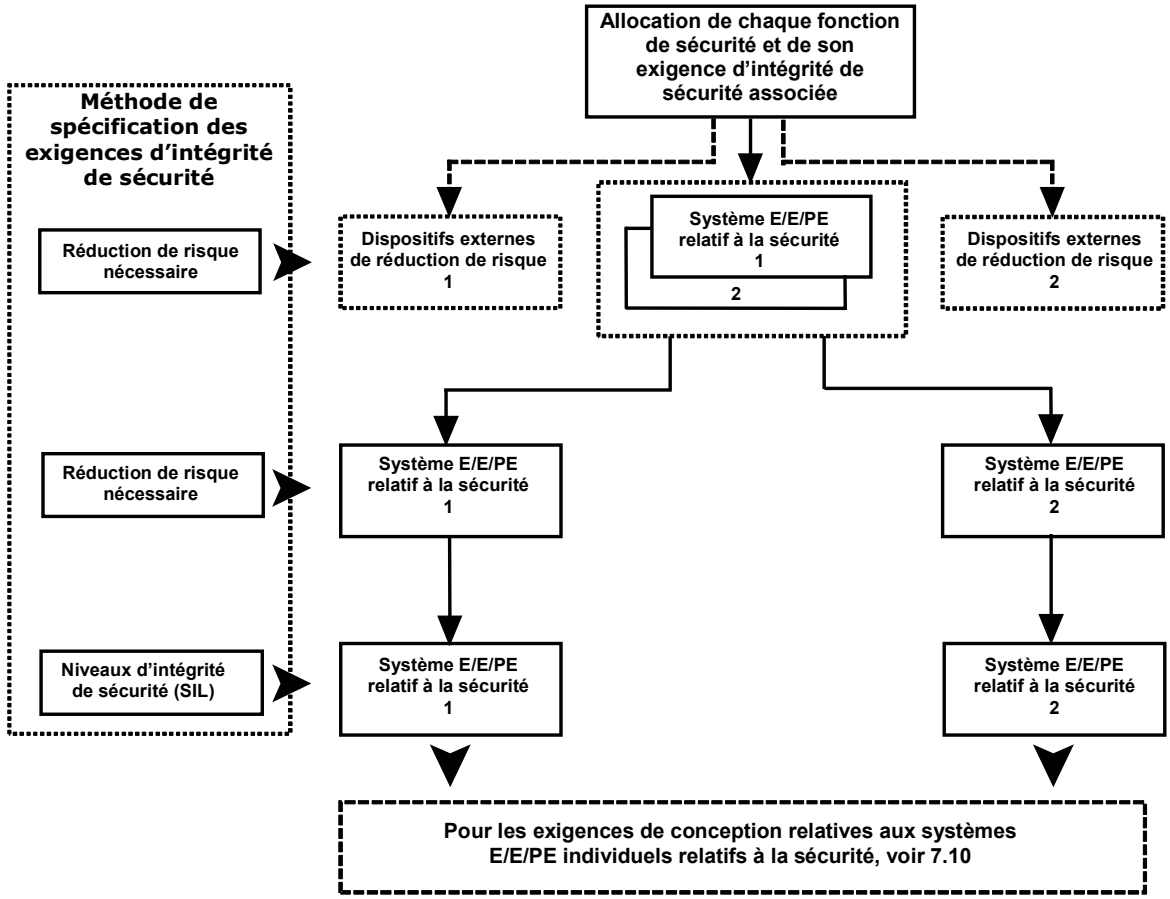
7.6.2.5 Les exigences relatives à l'intégrité de sécurité pour chaque fonction de sécurité doivent être spécifiées en termes

– de probabilité moyenne de défaillance dangereuse en cas de sollicitation de la fonction de sécurité, pour un mode de fonctionnement à faible sollicitation, ou
– de la fréquence moyenne de défaillance dangereuse de la fonction de sécurité [h^{-1}], pour un mode de fonctionnement à sollicitation élevée ou continu.

7.6.2.6 L'allocation des exigences d'intégrité de sécurité doit être réalisée en utilisant les techniques appropriées pour la combinaison des probabilités.

NOTE 1 L'allocation des exigences de sécurité peut être réalisée de manière qualitative et/ou quantitative.

NOTE 2 Lorsqu'un nombre élevé de systèmes E/E/PE relatifs à la sécurité et/ou de dispositifs externes de réduction de risque se révèle nécessaire pour atteindre l'objectif de risque tolérable, le risque réel atteint dépend des interconnexions systémiques entre les systèmes E/E/PE relatifs à la sécurité et/ou dispositifs externes de réduction de risque (voir le A.5.4 de la CEI 61508-5 pour plus de détails concernant ces interconnexions et leur méthode d'analyse).



NOTE 1 Les exigences d'intégrité de sécurité globale sont associées à chaque fonction de sécurité globale avant l'allocation (voir 7.5.2.3).

NOTE 2 L'allocation d'une fonction de sécurité globale peut être répartie sur plusieurs systèmes relatifs à la sécurité.

Figure 6 – Allocation des exigences de sécurité globale aux systèmes E/E/PE relatifs à la sécurité et dispositifs externes de réduction de risque

7.6.2.7 L'allocation doit être faite en tenant compte de la possibilité de défaillances de cause commune. Si le système de commande de l'EUC, les systèmes E/E/PE relatifs à la sécurité et les dispositifs de réduction de risque doivent être traités comme des éléments indépendants pour l'allocation, ils doivent:

– être indépendants de sorte que la probabilité de défaillances simultanées entre deux ou plusieurs de ces systèmes ou de ces dispositifs différents soit suffisamment faible par rapport à l'intégrité de sécurité requise,

– être fonctionnellement diversifiés (c'est-à-dire utiliser des approches totalement différentes pour atteindre les mêmes résultats),

– être basés sur des technologies diverses (c'est-à-dire utiliser des types différents d'équipement pour atteindre les même résultats),

NOTE 1 Il est admis qu'aussi diverses que soient les technologies employées dans le cas de systèmes à haut niveau d'intégrité de sécurité avec des conséquences particulièrement graves en cas de défaillance, des mesures spéciales seront prises à l'encontre d'événements ayant une origine commune à faible probabilité, par exemple, le crash d'un avion et les tremblements de terre.

– ne pas partager entre eux des parties, services ou systèmes annexes (par exemple, sources d'alimentation en énergie) dont la défaillance pourrait conduire à un mode de défaillance dangereux de tous les systèmes,

– ne pas partager de procédures communes d'exploitation, de maintenance ou d'essai.

NOTE 2 La présente norme traite spécifiquement de l'application des exigences de sécurité allouées aux systèmes E/E/PE relatifs à la sécurité, les exigences étant par ailleurs spécifiées en indiquant comment cela doit être effectué. L'application des exigences de sécurité allouées aux dispositifs externes de réduction de risque n'est par conséquent pas examinée en détail dans la présente norme.

Dans le cadre d'une analyse des défaillances de cause commune, les conditions limitant et contraignant la réalisation des systèmes E/E/PE relatifs à la sécurité telles que l'existence nécessaire d'une séparation physique, par exemple par un espace, entre les différents canaux d'un système, sous-système ou élément E/E/PE, doivent être vérifiées; cela peut par exemple conduire à interdire la présence de deux canaux/microprocesseurs sur une même carte de circuit imprimée ou sur une même puce (voir CEI 61508-2, Annexe E).

7.6.2.8 Si les exigences de 7.6.2.7 ne peuvent pas toutes être satisfaites, les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque ne doivent pas être considérés comme indépendants dans le cadre de l'allocation de la sécurité. En revanche, l'allocation doit tenir compte des défaillances de cause commune pertinentes entre le système de commande de l'EUC, les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque.

NOTE 1 Pour plus d'informations sur l'analyse des défaillances dépendantes, voir les références [12] et [13] dans la Bibliographie.

NOTE 2 La notion d'indépendance suffisante est établie en démontrant que la probabilité d'une défaillance dépendante est suffisamment faible pour les systèmes E/E/PE relatifs à la sécurité par rapport aux exigences d'intégrité de sécurité globale (voir 7.6.2.7).

NOTE 3 Comme indiqué en 7.6.2.3, l'allocation est itérative et si une analyse incluant les défaillances de cause commune indique que l'objectif de risque tolérable ne peut être atteint sur la base des hypothèses initiales, des modifications de conception sont alors nécessaires (pour des recommandations supplémentaires, voir la CEI 61508-5, A.5.4).

7.6.2.9 Lorsque l'allocation a suffisamment progressé, les exigences d'intégrité de sécurité pour chaque fonction de sécurité allouée au(x) système(s) E/E/PE relatif(s) à la sécurité doivent être spécifiées en termes de niveau d'intégrité de sécurité conformément au Tableau 2 ou au Tableau 3 et doivent indiquer si l'objectif chiffré de défaillance est, soit:

– la probabilité moyenne de défaillance dangereuse de la fonction de sécurité en cas de sollicitation, (PFD_{avg}), pour un mode de fonctionnement à faible sollicitation (Tableau 2), ou
– la fréquence moyenne de défaillance dangereuse de la fonction de sécurité [h^{-1}], (PFH), pour un mode de fonctionnement à sollicitation élevée (Tableau 3), ou
– la fréquence moyenne de défaillance dangereuse de la fonction de sécurité [h^{-1}], (PFH), pour un mode de fonctionnement continu (Tableau 3).

Tableau 2 – Niveaux d'intégrité de sécurité – objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à faible sollicitation

Niveau d'intégrité de sécurité (SIL)	Probabilité moyenne de défaillance dangereuse en cas de sollicitation de la fonction de sécurité (PFD_{avg})
4	$\geq 10^{-5}$ à $< 10^{-4}$
3	$\geq 10^{-4}$ à $< 10^{-3}$
2	$\geq 10^{-3}$ à $< 10^{-2}$
1	$\geq 10^{-2}$ à $< 10^{-1}$

Tableau 3 – Niveaux d'intégrité de sécurité – objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à sollicitation élevée ou en mode de fonctionnement continu

Niveau d'intégrité de sécurité (SIL)	Fréquence moyenne de défaillance dangereuse de la fonction de sécurité [h^{-1}] (PFH)
4	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-6}$ à $< 10^{-5}$

NOTE 1 Voir 3.5.16 de la CEI 61508-4 pour les définitions des termes: «mode de fonctionnement à faible sollicitation», «mode de fonctionnement à sollicitation élevée » et « mode de fonctionnement continu».

NOTE 2 Voir la CEI 61508-5 pour des recommandations concernant les modes de fonctionnement associant les objectifs chiffrés de défaillance à l'analyse des dangers et des risques.

NOTE 3 Les Tableaux 2 et 3 associent les objectifs chiffrés de défaillances alloués à une fonction de sécurité exécutée par un système E/E/PE relatif à la sécurité au niveau d'intégrité de sécurité. Il est admis qu'il n'est pas possible de prédire quantitativement l'intégrité de sécurité de tous les aspects des systèmes E/E/PE relatifs à la sécurité. Les techniques, mesures et jugements qualitatifs doivent être réalisés compte tenu des mesures de précaution considérées nécessaires pour assurer que les objectifs chiffrés de défaillance sont atteints. Cela est particulièrement vrai dans le cas d'une intégrité de sécurité systématique (voir 3.5.6 de la CEI 61508-4) où des techniques et des jugements qualitatifs doivent être réalisés compte tenu des mesures de précaution considérées nécessaires pour atteindre le niveau d'intégrité de sécurité systématique pour le niveau d'intégrité de sécurité spécifié (voir CEI 61508-2, 7.4.2.2 c), 7.4.3, 7.4.6, 7.4.7 et CEI 61508-3).

NOTE 4 Pour l'intégrité de sécurité du matériel, il est nécessaire d'appliquer des techniques d'estimation quantifiées de la fiabilité afin de déterminer si l'intégrité de sécurité cible, telle que déterminée par l'appréciation du risque, a été atteinte compte tenu des défaillances aléatoires du matériel (voir CEI 61508-2, 7.4.5).

NOTE 5 Lorsque le niveau d'intégrité de sécurité a été déterminé à l'aide d'une méthode qualitative (par exemple, un graphique qualitatif des risques), le Tableau 2 ou le Tableau 3 selon le cas, spécifie les objectifs chiffrés quantitatifs qui fixent les limites de l'intégrité de sécurité du matériel.

NOTE 6 L'intégrité de sécurité qui peut être déclarée lorsque deux ou plusieurs systèmes E/E/PE relatifs à la sécurité sont utilisés, peut être meilleure que celle indiquée dans le Tableau 2 sous réserve que des degrés d'indépendance appropriés soient atteints. Par exemple, cela serait pertinent si la fonction de sécurité spécifiée devait être exécutée par deux systèmes E/E/PE relatifs à la sécurité lorsque des niveaux adéquats d'indépendance entre les deux systèmes ont été atteints.

NOTE 7 Pour un système E/E/PE relatif à la sécurité fonctionnant en mode à sollicitation élevée ou en mode continu requis pendant une durée de mission définie au cours de laquelle aucune réparation ne peut être effectuée, le niveau d'intégrité de sécurité requis pour une fonction de sécurité peut être déduit comme suit: déterminer la probabilité de défaillance requise de la fonction de sécurité au cours de la durée de mission et la diviser par la durée de mission, afin d'obtenir une probabilité de défaillance par heure requise, puis déduire le niveau d'intégrité de sécurité requis à partir du Tableau 3.

7.6.2.10 Pour un système E/E/PE relatif à la sécurité mettant en œuvre des fonctions de sécurité ayant des niveaux d'intégrité de sécurité différents et à moins qu'il puisse être démontré qu'il existe une indépendance suffisante dans la mise en œuvre de ces fonctions de sécurité particulières, les parties du matériel et du logiciel relatifs à la sécurité où il n'existe pas d'indépendance suffisante dans leur mise en œuvre, doivent être traitées comme si elles faisaient partie intégrante de la fonction de sécurité ayant le plus haut niveau d'intégrité de sécurité. Par conséquent, les exigences applicables au plus haut niveau d'intégrité de sécurité correspondant doivent s'appliquer à toutes ces parties.

NOTE Voir également CEI 61508-2, 7.4.2.4 et CEI 61508-3, 7.4.2.8.

7.6.2.11 Dans les cas où le processus d'allocation entraîne une exigence relative à la mise en œuvre d'une fonction de sécurité SIL 4 par un système E/E/PE relatif à la sécurité, les éléments suivants doivent alors s'appliquer:

a) L'application doit être réexaminée afin de déterminer si tout paramètre de risque peut être modifié de manière à éviter l'application de l'exigence relative à l'utilisation d'une fonction de sécurité SIL 4. L'examen doit déterminer si:

   – des systèmes relatifs à la sécurité supplémentaires ou des dispositifs externes de réduction de risque, non basés sur les systèmes E/E/PE relatifs à la sécurité, pourraient être mis en place,

   – la gravité des conséquences pourrait être réduite,

   – la probabilité d'occurrence de la conséquence spécifiée pourrait être réduite.

b) Si, après examen plus approfondi de l'application, il est décidé d'appliquer la fonction de sécurité SIL 4, alors une appréciation du risque supplémentaire doit être effectuée au moyen d'une méthode quantitative qui tient compte des défaillances de cause commune potentielles entre le système E/E/PE relatif à la sécurité, et:

   – tous autres systèmes dont la défaillance solliciterait l'utilisation de ce dernier et

   – tous autres systèmes relatifs à la sécurité.

7.6.2.12 Aucune fonction de sécurité unique d'un système E/E/PE relatif à la sécurité ne doit se voir allouer une intégrité de sécurité cible inférieure à celle spécifiée dans les Tableaux 2 et 3. Cela veut dire que, pour les systèmes relatifs à la sécurité fonctionnant

– en mode de fonctionnement à faible sollicitation, la limite inférieure est fixée pour une probabilité moyenne de défaillance dangereuse de 10^{-5} en cas de sollicitation de la fonction de sécurité,

– en mode de fonctionnement continu ou à sollicitation élevée, la limite inférieure est fixée pour une fréquence moyenne de défaillance dangereuse de 10^{-9} [h^{-1}].

NOTE Il peut être possible de concevoir des systèmes relatifs à la sécurité ayant des valeurs plus basses pour l'intégrité de sécurité cible dans le cas de systèmes non complexes. Il est toutefois considéré que ces limites représentent ce qui peut être réalisé actuellement pour des systèmes relativement complexes (par exemple, des systèmes électroniques programmables relatifs à la sécurité).

7.6.2.13 Les informations et les résultats relatifs à l'allocation des exigences de sécurité globale obtenus de 7.6.2.1 à 7.6.2.12 ainsi que toutes les hypothèses et justifications formulées (y compris les hypothèses concernant les dispositifs externes de réduction de risque qui doivent être maîtrisés pendant toute la durée de vie de l'EUC) doivent être documentés.

NOTE Pour chaque système E/E/PE relatif à la sécurité, il convient de disposer d'informations suffisantes concernant les fonctions de sécurité et leurs niveaux d'intégrité de sécurité associés. Ces informations constituent la base des exigences de sécurité pour les systèmes E/E/PE relatifs à la sécurité développés en 7.10.

7.7 Planification globale de l'exploitation et de la maintenance

NOTE 1 Cette phase correspond à la case 6 de la Figure 2.

NOTE 2 Un exemple de modèle d'activités d'exploitation et de maintenance est présenté à la Figure 7 ci-après.

NOTE 3 Un exemple de modèle de gestion de l'exploitation et de la maintenance est présenté à la Figure 8 ci-après.

NOTE 4 Les exigences spécifiées au 7.2.2 sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant plus particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 5 Des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risque afin d'obtenir une sécurité fonctionnelle.

7.7.1 Objectif

L'objectif des exigences de ce paragraphe est de développer un plan d'exploitation et de maintenance des systèmes E/E/PE relatifs à la sécurité, pour assurer que la sécurité fonctionnelle requise est maintenue pendant l'exploitation et la maintenance.

7.7.2 Exigences

7.7.2.1 Un plan doit être élaboré. Il doit spécifier les aspects suivants:

a) les activités systématiques qui doivent être réalisées pour maintenir la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité,

b) les actions et contraintes qui sont nécessaires (par exemple, lors du démarrage, de l'exploitation normale, des essais systématiques, des perturbations prévisibles, des anomalies et de l'arrêt) pour éviter un état de non-sécurité, pour réduire les sollicitations du système E/E/PE relatif à la sécurité ou pour réduire les conséquences des événements préjudiciables,

NOTE 1 Les contraintes, conditions et actions suivantes se rapportent aux systèmes E/E/PE relatifs à la sécurité:

1) contraintes sur l'exploitation de l'EUC pendant une anomalie des systèmes E/E/PE relatifs à la sécurité,
2) contraintes sur l'exploitation de l'EUC pendant la maintenance des systèmes E/E/PE relatifs à la sécurité,
3) lorsque des contraintes sur l'exploitation de l'EUC peuvent être supprimées,
4) les procédures pour le retour à une exploitation normale,
5) les procédures pour confirmer que l'exploitation normale a été établie,
6) les circonstances pendant lesquelles les fonctions de sécurité mises en œuvre par le système E/E/PE relatif à la sécurité peuvent être contournées pour le démarrage, pour une exploitation spéciale ou pour des essais,
7) les procédures à suivre avant, pendant et après le contournement des systèmes E/E/PE relatifs à la sécurité, y compris les procédures d'engagement de travaux et les niveaux d'autorisation.

c) les documents qui doivent être maintenus et montrant les résultats d'audits et d'essais de sécurité fonctionnelle,

d) les documents qui doivent être maintenus et concernant tous les événements dangereux et tous les incidents susceptibles de générer un événement dangereux,

e) le domaine d'application des activités de maintenance (que l'on distingue des activités de modification),

f) les actions à entreprendre lorsque des événements dangereux surviennent,

g) le contenu de la documentation chronologique des activités d'exploitation et de maintenance (voir 7.15).

NOTE 2 La majorité des systèmes E/E/PE relatifs à la sécurité ont certains modes de défaillance qui ne peuvent être découverts que par des essais lors de la maintenance périodique. Dans de tels cas, si les essais ne sont pas effectués à une fréquence suffisante, les exigences d'intégrité de sécurité relatives au système E/E/PE relatif à la sécurité ne sont pas atteintes.

NOTE 3 Ce paragraphe s'applique à un fournisseur de logiciel(s) qui est tenu de fournir les informations et les procédures avec le produit logiciel pour permettre à l'utilisateur d'assurer la sécurité fonctionnelle requise pendant l'exploitation et la maintenance d'un système relatif à la sécurité. Cela comprend les procédures préparatoires pour toute modification de logiciel susceptible d'être effectuée en conséquence d'une exigence d'exploitation ou de maintenance (voir également 7.6 de la CEI 61508-3). La mise en œuvre de ces procédures est traitée en 7.8 de la CEI 61508-3. Les procédures préparatoires pour les futures modifications de logiciel susceptibles d'être effectuées en conséquence d'une exigence de modification pour un système relatif à la sécurité sont traitées en 7.6 de la CEI 61508-3. La mise en œuvre de ces procédures est traitée en 7.8 de la CEI 61508-2.

NOTE 4 Il convient de tenir compte des procédures d'exploitation et de maintenance développées pour satisfaire aux exigences de la CEI 61508-2 et de la CEI 61508-3.

7.7.2.2 Le plan doit assurer qu'en cas de déconnexion, pour essais, de tout sous-système d'un système E/E/PE relatif à la sécurité dont la tolérance aux anomalies du matériel est nulle, la sécurité permanente de l'EUC est maintenue par l'application de mesures et de contraintes supplémentaires. L'intégrité de sécurité garantie par ces mesures et ces contraintes supplémentaires doit être au moins égale à l'intégrité de sécurité garantie par le système E/E/PE relatif à la sécurité en fonctionnement normal. Dans le cas de tout sous-système d'un système E/E/PE relatif à la sécurité dont la tolérance aux anomalies du matériel est supérieure à zéro, au moins un canal de ce système doit alors continuer de fonctionner pendant les essais, ces derniers devant être effectués intégralement dans le cadre de la durée moyenne de

réparation (MTTR)[1] considérée dans les calculs effectués pour démontrer la conformité avec l'objectif chiffré de défaillance.

NOTE Pour la tolérance aux anomalies de matériel, voir 7.4.4.1 de la CEI 61508-2.

7.7.2.3 Les activités de maintenance périodique qui sont réalisées pour déterminer les anomalies non révélées doivent être déterminées par une analyse systématique.

NOTE En l'absence de détection des anomalies non révélées, ces dernières peuvent

a) conduire à une défaillance du fonctionnement en cas de sollicitation, dans le cas de systèmes E/E/PE relatifs à la sécurité ou de dispositifs externes de réduction de risque,

b) générer des sollicitations des systèmes E/E/PE relatifs à la sécurité ou des dispositifs externes de réduction de risque, dans le cas de systèmes non relatifs à la sécurité.

7.7.2.4 Le plan de maintenance des systèmes E/E/PE relatifs à la sécurité doit être accepté par les personnes responsables de l'exploitation et de la maintenance

– des systèmes E/E/PE relatifs à la sécurité,
– des dispositifs externes de réduction de risque et
– des systèmes non relatifs à la sécurité qui peuvent solliciter les systèmes E/E/PE relatifs à la sécurité ou les dispositifs externes de réduction de risque.

7.8 Planification globale de la validation de la sécurité

NOTE 1 Cette phase correspond à la case 7 de la Figure 2.

NOTE 2 Les exigences spécifiées dans ce paragraphe sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant plus particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 3 Pour obtenir la sécurité fonctionnelle, des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risques.

7.8.1 Objectif

L'objectif des exigences de ce paragraphe est de développer un plan de validation globale de la sécurité des systèmes E/E/PE relatifs à la sécurité.

7.8.2 Exigences

7.8.2.1 Un plan doit être développé. Il doit spécifier les aspects suivants:

a) des détails portant sur le moment où la validation doit avoir lieu,
b) des informations détaillées sur les personnes devant effectuer la validation,
c) la spécification des modes pertinents de fonctionnement de l'EUC, avec leurs relations avec le système E/E/PE relatif à la sécurité, comprenant le cas échéant
   – les préparations d'utilisation, y compris la configuration et les réglages,
   – le démarrage,
   – l'apprentissage,
   – le mode automatique,
   – le mode manuel,
   – le mode semi-automatique,
   – le régime établi,
   – la remise à zéro,

1 MTTR = *Mean Time To Repair*. --`,,,,,````,,```,,,,``,`,```-`-`,,`,,`,`,,`---

  - l'arrêt,
  - la maintenance,
  - les conditions anormales raisonnablement prévisibles,

d) la spécification des systèmes E/E/PE relatifs à la sécurité qui doivent être validés pour chaque mode de fonctionnement de l'EUC avant que ne commence la mise en service,

e) la stratégie technique de la validation (par exemple, les méthodes analytiques, les essais statistiques, etc.),

f) les mesures, techniques et procédures qui doivent être utilisées pour confirmer que l'allocation des fonctions de sécurité a été réalisée correctement; cela doit inclure la confirmation que chaque fonction de sécurité est en conformité
  - avec la spécification des exigences globales de fonctions de sécurité, et
  - avec la spécification des exigences globales d'intégrité de sécurité,

g) la référence spécifique à chaque élément contenu dans les données de sortie de 7.5 et 7.6,

h) l'environnement requis dans lequel les activités de validation doivent se dérouler (par exemple, pour des essais, cela comprendrait les outils et les équipements étalonnés),

i) les critères d'acceptation et de rejet,

j) les politiques et procédures d'évaluation des résultats de la validation, en particulier en ce qui concerne les défaillances.

NOTE Pendant la planification de la validation globale, il convient de tenir compte des travaux planifiés pour la validation de sécurité des systèmes E/E/PE et pour la validation de la sécurité du logiciel, tels que requis par les CEI 61508-2 et CEI 61508-3. Il est important d'assurer que toutes les interactions entre deux systèmes E/E/PE relatifs à la sécurité ou plus et/ou les dispositifs externes de réduction de risque sont prises en compte et que toutes les fonctions de sécurité (telles que spécifiées dans les données de sortie de 7.5) ont été réalisées.

7.8.2.2 L'information provenant de 7.8.2.1 doit être documentée et doit constituer le plan pour la validation globale de la sécurité des systèmes E/E/PE relatifs à la sécurité.

7.9 Planification globale de l'installation et de la mise en service

NOTE 1 Cette phase correspond à la case 8 de la Figure 2.

NOTE 2 Les exigences spécifiées dans ce paragraphe sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant plus particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 3 Pour obtenir la sécurité fonctionnelle, des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risques.

7.9.1 Objectifs

7.9.1.1 Le premier objectif des exigences de ce paragraphe est de développer un plan pour que l'installation des systèmes E/E/PE relatifs à la sécurité soit maîtrisée afin d'assurer que la sécurité fonctionnelle requise est obtenue.

7.9.1.2 Le second objectif des exigences de ce paragraphe est de développer un plan pour que la mise en service des systèmes E/E/PE relatifs à la sécurité soit maîtrisée afin d'assurer que la sécurité fonctionnelle requise est obtenue.

7.9.2 Exigences

7.9.2.1 Un plan pour l'installation des systèmes E/E/PE relatifs à la sécurité doit être développé, spécifiant

a) le programme d'installation,

b) les personnes responsables des différentes parties de l'installation,

c) les procédures pour l'installation,

d) la séquence d'intégration des différents éléments,

e) les critères permettant de déclarer que tout ou partie des systèmes E/E/PE relatifs à la sécurité sont prêts pour l'installation et permettant de déclarer que les activités d'installation sont terminées,

f) les procédures pour la résolution des défaillances et incompatibilités.

7.9.2.2 Un plan pour la mise en service des systèmes E/E/PE relatifs à la sécurité doit être développé, spécifiant:

a) le programme de la mise en service,

b) les personnes responsables des différentes parties de la mise en service,

c) les procédures pour la mise en service,

d) les relations avec les différentes étapes de l'installation,

e) les relations avec la validation.

7.9.2.3 La planification globale de l'installation et de la mise en service doit être documentée.

7.10 Spécification des exigences de sécurité relatives aux systèmes E/E/PE

NOTE Cette phase correspond à la case 9 de la Figure 2.

7.10.1 Objectif

L'objectif des exigences de ce paragraphe est de définir les exigences de sécurité des systèmes E/E/PE, en termes d'exigences relatives aux fonctions de sécurité de ces systèmes et d'exigences d'intégrité de sécurité de ces mêmes systèmes, afin d'obtenir la sécurité fonctionnelle requise.

7.10.2 Exigences

7.10.2.1 La spécification des exigences de sécurité des systèmes E/E/PE doit être déduite de l'allocation des exigences de sécurité, spécifiées en 7.6, ainsi que toutes les informations pertinentes liées à l'application. Ces informations doivent être mises à disposition du développeur des systèmes E/E/PE relatifs à la sécurité.

7.10.2.2 La spécification des exigences de sécurité des systèmes E/E/PE doit contenir les exigences relatives aux fonctions de sécurité et à leurs niveaux d'intégrité de sécurité associés.

NOTE L'objectif est de décrire, en termes non spécifiques aux équipements, les fonctions de sécurité et leurs performances de sécurité fonctionnelle requises. La spécification peut alors être vérifiée par rapport aux résultats des exigences globales de sécurité et aux phases d'allocation de ces exigences, et être utilisée comme base de création du système E/E/PE (voir 7.2 de la CEI 61508-2). Les concepteurs des équipements peuvent utiliser la spécification comme base de sélection des équipements et de l'architecture associée.

7.10.2.3 La spécification des exigences de sécurité des systèmes E/E/PE doit être mise à disposition du développeur du système E/E/PE relatif à la sécurité.

7.10.2.4 Elle doit par ailleurs être exprimée et structurée de manière à

a) être claire, précise, non ambiguë, vérifiable, testable, actualisable et réalisable,

b) être rédigée de manière à faciliter la compréhension des personnes susceptibles d'utiliser les informations à toute étape du cycle de vie de sécurité du système E/E/PE,

c) être exprimée en langage naturel ou formel et/ou sous forme de diagrammes logiques, séquentiels ou cause-effet qui définissent les fonctions de sécurité nécessaires, chacune de ces fonctions étant définie de manière individuelle.

7.10.2.5 La spécification des exigences de sécurité des systèmes E/E/PE doit contenir les exigences relatives aux fonctions de sécurité de ces mêmes systèmes (voir 7.10.2.6), ainsi que les exigences relatives à l'intégrité de sécurité de ces systèmes (voir 7.10.2.7).

7.10.2.6 La spécification des exigences des fonctions de sécurité des systèmes E/E/PE doit contenir:

a) une description de toutes les fonctions de sécurité nécessaires pour obtenir la sécurité fonctionnelle requise, qui doit, pour chaque fonction de sécurité:
   - fournir des exigences détaillées exhaustives et suffisantes pour la conception et le développement des systèmes E/E/PE relatifs à la sécurité,
   - comprendre la méthode qui permet aux systèmes E/E/PE relatifs à la sécurité d'atteindre ou de maintenir un état de sécurité de l'EUC,
   - spécifier si une commande continue est ou non requise, et pour quelles périodes, pour atteindre ou maintenir un état de sécurité de l'EUC, et
   - spécifier si la fonction de sécurité est applicable aux systèmes E/E/PE relatifs à la sécurité fonctionnant en modes de faible ou de sollicitation élevée ou en mode continu,
b) l'obtention du temps de réponse requis (c'est-à-dire la durée de réalisation nécessaire de la fonction de sécurité),
c) les interfaces entre les systèmes E/E/PE relatifs à la sécurité et l'opérateur qui sont nécessaires pour obtenir la sécurité fonctionnelle requise,
d) toutes les informations pertinentes pour la sécurité fonctionnelle susceptibles d'avoir une influence sur la conception des systèmes E/E/PE relatifs à la sécurité,
e) toutes les interfaces nécessaires à la sécurité fonctionnelle, entre les systèmes E/E/PE relatifs à la sécurité et tous autres systèmes (au sein ou à l'extérieur de l'EUC),
f) tous les modes de fonctionnement pertinents de l'EUC, y compris:
   - les préparations d'utilisation, y compris la configuration et les réglages,
   - le démarrage, l'apprentissage, le mode automatique, le mode manuel, le mode semi-automatique, le régime établi,
   - le régime non établi, la nouvelle configuration, l'arrêt et la maintenance,
   - les conditions anormales raisonnablement prévisibles,

NOTE Des fonctions de sécurité supplémentaires peuvent être requises pour des modes de fonctionnement particuliers (par exemple, configuration, réglage ou maintenance) afin de permettre d'effectuer ces opérations en toute sécurité.

g) tous les modes de comportement requis des systèmes E/E/PE relatifs à la sécurité doivent être spécifiés. Plus particulièrement, le comportement aux défaillances et la réponse requise dans le cas d'une défaillance (par exemple, alarmes, arrêt automatique, etc.) des systèmes E/E/PE relatifs à la sécurité.

7.10.2.7 La spécification des exigences relatives à l'intégrité de sécurité des systèmes E/E/PE doit contenir:

a) le niveau d'intégrité de sécurité pour chaque fonction de sécurité et le cas échéant, une valeur spécifiée pour l'objectif chiffré de défaillance,

NOTE 1 La valeur spécifiée de l'objectif chiffré de défaillance peut être calculé à l'aide d'une méthode quantitative (voir 7.5.2.3). Autrement, lorsque l'exigence d'intégrité de sécurité a été développée à l'aide d'une méthode qualitative et est exprimée en tant que niveau d'intégrité de sécurité, l'objectif chiffré de défaillance est alors déduit du Tableau 2 ou 3 selon le cas, selon le niveau d'intégrité de sécurité. Dans ce cas, l'objectif chiffré de défaillance spécifié correspond à la plus faible probabilité moyenne de défaillance ou plus faible taux de défaillance pour le niveau d'intégrité de sécurité, à moins qu'une valeur différente ait été utilisée pour l'étalonnage de la méthode.

NOTE 2 Dans le cas d'une fonction de sécurité fonctionnant en mode faible sollicitation, l'objectif chiffré de défaillance est exprimé en termes de probabilité moyenne de défaillance dangereuse en cas de sollicitation, telle que déterminée par le niveau d'intégrité de la fonction de sécurité (voir Tableau 2), à moins que la spécification des exigences d'intégrité de sécurité des systèmes E/E/PE ne comporte une exigence spécifiant que la fonction de sécurité doit satisfaire à un objectif chiffré de défaillance spécifique, au lieu d'un niveau d'intégrité de sécurité spécifique. Par exemple, lorsqu'un objectif chiffré de défaillance de $1{,}5 \times 10^{-2}$ (probabilité moyenne de défaillance

dangereuse en cas de sollicitation) est spécifié afin d'atteindre l'objectif de risque tolérable, la probabilité moyenne de défaillance dangereuse en cas de sollicitation de la fonction de sécurité, due à des défaillances aléatoires du matériel, doit alors être inférieure ou égale à $1,5 \times 10^{-2}$.

NOTE 3 Dans le cas d'une fonction de sécurité fonctionnant en mode sollicitation élevée ou en mode continu, l'objectif chiffré de défaillance est exprimé en termes de fréquence moyenne de défaillance dangereuse [h^{-1}], telle que déterminée par le niveau d'intégrité de sécurité de la fonction de sécurité (voir Tableau 3), à moins que la spécification des exigences d'intégrité de sécurité des systèmes E/E/PE ne comporte une exigence spécifiant que la fonction de sécurité doit satisfaire à un objectif chiffré de défaillance spécifique, au lieu d'un niveau d'intégrité de sécurité spécifique. Par exemple, lorsqu'un objectif chiffré de défaillance de $1,5 \times 10^{-6}$ (fréquence moyenne de défaillance dangereuse [h^{-1}]) est spécifié afin d'atteindre l'objectif de risque tolérable, la fréquence moyenne de défaillance dangereuse de la fonction de sécurité, due à des défaillances aléatoires du matériel, doit alors être inférieure ou égale à $1,5 \times 10^{-6}$ [h^{-1}].

b) le mode de fonctionnement (faible sollicitation, sollicitation élevée ou mode continu) de chaque fonction de sécurité,

c) le cycle de service et la durée de vie requis,

d) les exigences, contraintes, fonctions et installations qui permettent d'effectuer l'essai périodique des matériels E/E/PE,

NOTE 4 Il convient que la définition d'une spécification des exigences de sécurité des systèmes E/E/PE tienne compte de l'application effective de ces systèmes. Ceci est particulièrement important pour la maintenance, lorsqu'il convient que la durée de l'intervalle spécifié d'essai périodique ne soit pas inférieure à la durée qui peut être raisonnablement prévue pour l'application particulière. Par exemple, l'intervalle entre les opérations d'entretien et de maintenance qui peut raisonnablement être obtenu pour des articles produits en série utilisés par le public, est susceptible d'être supérieur à celui prévu avec une application davantage maîtrisée.

e) les valeurs extrêmes de toutes les conditions environnementales susceptibles d'être rencontrées au cours du cycle de vie de sécurité des systèmes E/E/PE, y compris la fabrication, le stockage, le transport, les essais, l'installation, la mise en service, l'exploitation et la maintenance,

f) les limites d'immunité électromagnétique requises pour obtenir la sécurité fonctionnelle. Il convient de calculer ces limites compte tenu à la fois de l'environnement électromagnétique et des niveaux d'intégrité de sécurité requis (voir CEI/TS 61000-1-2),

NOTE 5 La nature et les caractéristiques physiques des phénomènes électromagnétiques ne permettent pas d'établir une corrélation simple, évidente et démontrable entre le niveau d'immunité et le niveau d'intégrité de sécurité requis pour la quasi-totalité des cas de phénomènes électromagnétiques. La spécification de niveaux d'immunité effectifs uniquement selon le SIL requis n'est par conséquent ni possible ni raisonnable dans les cas mentionnés. Des approches alternatives peuvent être utilisées, qui spécifient, dans une certaine mesure, le niveau d'immunité requis selon le SIL requis et qui impliquent également des dispositions d'essai ou des critères de réalisation d'essais spéciaux. Voir la CEI/TS 61000-1-2.

NOTE 6 Se reporter également à la référence [14] dans la Bibliographie.

g) les conditions aux limites et les contraintes pour la réalisation des systèmes E/E/PE relatifs à la sécurité du fait de la possibilité de défaillances de cause commune (voir 7.6.2.7).

7.11 Systèmes E/E/PE relatifs à la sécurité – réalisation

NOTE Cette phase correspond à la case 10 de la Figure 2 et aux cases 10.1 à 10.6 des Figures 3 et 4.

7.11.1 Objectif

L'objectif des exigences de ce paragraphe est de créer des systèmes E/E/PE relatifs à la sécurité conformes à la spécification des exigences de sécurité des systèmes E/E/PE (comprenant la spécification des exigences relatives aux fonctions de sécurité de ces systèmes, ainsi que la spécification des exigences d'intégrité de sécurité de ces mêmes systèmes). (Voir la CEI 61508-2 et la CEI 61508-3).

7.11.2 Exigences

Les exigences qui doivent être satisfaites sont contenues dans la CEI 61508-2 et la CEI 61508-3.

7.12 Dispositifs externes de réduction de risque – spécification et réalisation

NOTE Cette phase correspond à la case 11 de la Figure 2.

7.12.1 Objectif

L'objectif des exigences de ce paragraphe est de créer des dispositifs externes de réduction de risque permettant de satisfaire aux exigences de fonctions de sécurité et aux exigences d'intégrité de sécurité spécifiées pour de tels systèmes.

7.12.2 Exigences

La spécification permettant de satisfaire aux exigences de fonctions de sécurité et aux exigences d'intégrité de sécurité pour les dispositifs externes de réduction de risque n'est pas traitée par la présente norme.

NOTE Les dispositifs externes de réduction de risque sont basés sur une technologie autre qu'électrique/électronique/électronique programmable (par exemple, hydraulique, pneumatique, etc.) ou peuvent être des structures physiques (par exemple, un système de vidange, un pare-feu ou un faisceau). Ils ont été inclus dans le cycle de vie de sécurité global afin d'assurer que la réduction du risque par les systèmes E/E/PE relatifs à la sécurité a été déterminée dans le cadre de la réduction du risque par les dispositifs externes de réduction de risque.

7.13 Installation et mise en service globales

NOTE 1 Cette phase correspond à la case 12 de la Figure 2.

NOTE 2 Les exigences spécifiées dans ce paragraphe sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 3 Des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risque afin d'obtenir une sécurité fonctionnelle.

7.13.1 Objectifs

7.13.1.1 Le premier objectif des exigences de ce paragraphe est d'installer les systèmes E/E/PE relatifs à la sécurité.

7.13.1.2 Le second objectif des exigences de ce paragraphe est d'assurer la mise en service des systèmes E/E/PE relatifs à la sécurité.

7.13.2 Exigences

7.13.2.1 Les activités d'installation doivent être réalisées conformément au plan pour l'installation des systèmes E/E/PE relatifs à la sécurité (voir 7.9).

7.13.2.2 L'information documentée pendant l'installation doit comprendre

– un dossier sur les activités d'installation,
– la résolution des défaillances et incompatibilités.

7.13.2.3 Les activités de mise en service doivent être réalisées conformément au plan pour la mise en service des systèmes E/E/PE relatifs à la sécurité.

7.13.2.4 L'information documentée pendant la mise en service doit comprendre:

– un dossier sur les activités de mise en service,
– les références des rapports de défaillance,
– la résolution des défaillances et incompatibilités.

7.14 Validation globale de la sécurité

NOTE 1 Cette phase correspond à la case 13 de la Figure 2.

NOTE 2 Les exigences spécifiées dans ce paragraphe sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 3 Des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risque afin d'obtenir une sécurité fonctionnelle.

7.14.1 Objectif

L'objectif des exigences de ce paragraphe est de valider le fait que les systèmes E/E/PE relatifs à la sécurité satisfont à la spécification des exigences globales de sécurité en termes d'exigences globales relatives aux fonctions de sécurité et d'exigences globales d'intégrité de sécurité, en tenant compte de l'allocation des exigences de sécurité pour les systèmes E/E/PE relatifs à la sécurité, définies conformément à 7.6.

7.14.2 Exigences

7.14.2.1 Les activités de validation doivent être réalisées conformément au plan de validation globale de la sécurité pour les systèmes E/E/PE relatifs à la sécurité (voir 7.8).

7.14.2.2 Tous les équipements utilisés pour des mesures quantitatives, dans le cadre des activités de validation, doivent être étalonnés par rapport à une spécification se référant à un étalon national ou à la spécification du fournisseur.

7.14.2.3 L'information documentée pendant la validation doit comprendre

– un dossier des activités de validation, sous forme chronologique,
– la version de la spécification utilisée pour les exigences globales de sécurité,
– la fonction de sécurité validée (par essai ou par analyse),
– les outils et les équipements utilisés ainsi que les données d'étalonnage,
– les résultats des activités de validation,
– l'identification de la configuration de l'entité soumise à l'essai, les procédures appliquées et l'environnement d'essai,
– les divergences entre les résultats prévus et les résultats réels.

7.14.2.4 Lorsque des différences surviennent entre les résultats prévus et les résultats réels, l'analyse effectuée et les décisions prises concernant la poursuite de la validation ou bien l'émission d'une demande de modification et le retour à une partie antérieure de la validation doivent être documentées.

7.15 Exploitation, maintenance et réparation globales

NOTE 1 Cette phase correspond à la case 14 de la Figure 2.

NOTE 2 Les mesures organisationnelles dont il est question dans ce paragraphe permettent la mise en œuvre efficace des exigences techniques et ont pour unique but la réalisation et le maintien de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité. Les exigences techniques nécessaires au maintien de la sécurité fonctionnelle sont spécifiées comme partie intégrante des informations communiquées par le fournisseur du système E/E/PE relatif à la sécurité et ses éléments et composants.

NOTE 3 Les exigences de sécurité fonctionnelle pendant les activités de maintenance et de réparation peuvent être différentes de celles requises pendant l'exploitation.

NOTE 4 Il convient de ne pas supposer que les procédures d'essai développées pour l'installation et la mise en service initiales peuvent être utilisées sans vérifier leur validité et leur praticabilité dans le cadre d'exploitations «en ligne» de l'EUC.

NOTE 5 Les exigences spécifiées dans ce paragraphe sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 6 Des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risque afin d'obtenir une sécurité fonctionnelle.

7.15.1 Objectif

7.15.1.1 Le premier objectif des exigences de ce paragraphe est d'assurer que la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité est maintenue au niveau spécifié.

7.15.1.2 Le second objectif des exigences de ce paragraphe est d'assurer que les exigences techniques, nécessaires à l'exploitation, la maintenance et la réparation globales des systèmes E/E/PE relatifs à la sécurité sont spécifiées et fournies aux personnes responsables de l'exploitation et de la maintenance futures de ces systèmes.

7.15.2 Exigences

7.15.2.1 Les éléments suivants doivent être mis en œuvre:

– le plan pour l'exploitation et la maintenance des systèmes E/E/PE relatifs à la sécurité (voir 7.7),

– les procédures d'exploitation, de maintenance et de réparation pour les systèmes E/E/PE relatifs à la sécurité.

7.15.2.2 La mise en œuvre des points spécifiés en 7.15.2.1 doit comprendre les actions suivantes:

– la mise en œuvre des procédures,

– le suivi des programmes de maintenance,

– la conservation des documents,

– la conduite régulière d'audits de la sécurité fonctionnelle (voir 6.2.7),

– la documentation des modifications qui ont été effectuées sur les systèmes E/E/PE relatifs à la sécurité.

NOTE 1 Un exemple de modèle d'activités d'exploitation et de maintenance est présenté à la Figure 7.

NOTE 2 Un exemple de modèle de gestion de l'exploitation et de la maintenance est présenté à la Figure 8.

7.15.2.3 La documentation chronologique de l'exploitation, de la réparation et de la maintenance des systèmes E/E/PE relatifs à la sécurité doit être maintenue et doit contenir les informations suivantes:

– les résultats des audits et des essais de la sécurité fonctionnelle,

– un enregistrement de l'heure et de l'origine des sollicitations des systèmes E/E/PE relatifs à la sécurité (en exploitation réelle), ainsi que les performances de ces systèmes lorsqu'ils ont été soumis à ces sollicitations, et les anomalies découvertes lors de la maintenance périodique,

– un enregistrement des modifications apportées à l'EUC, à son système de commande et aux systèmes E/E/PE relatifs à la sécurité.

7.15.2.4 Les exigences exactes concernant la documentation chronologique dépendent du produit ou de l'application spécifique et doivent le cas échéant, être détaillées dans les normes internationales de produit et d'application sectorielle.

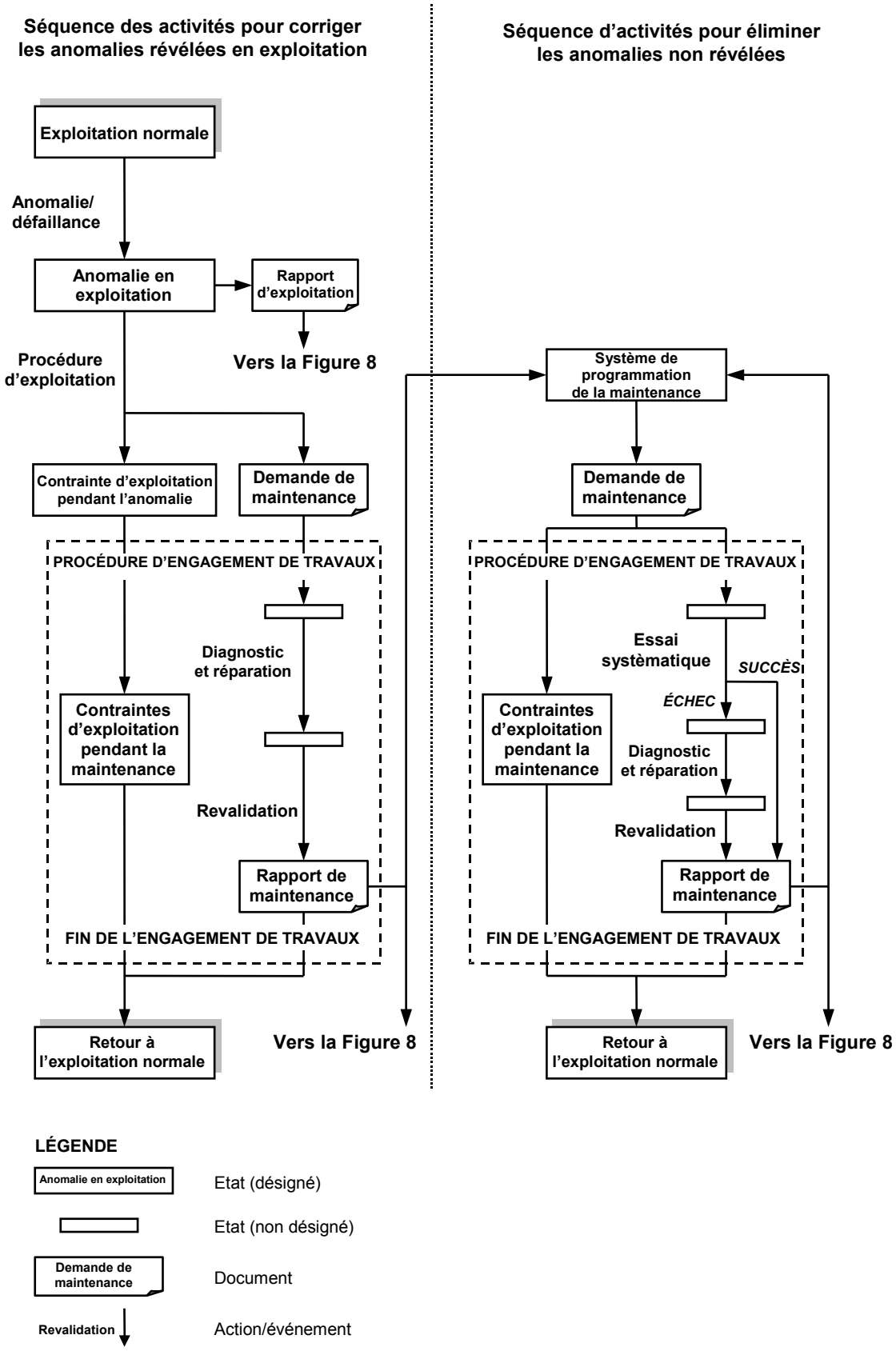


Figure 7 – Exemple de modèle d'activités d'exploitation et de maintenance

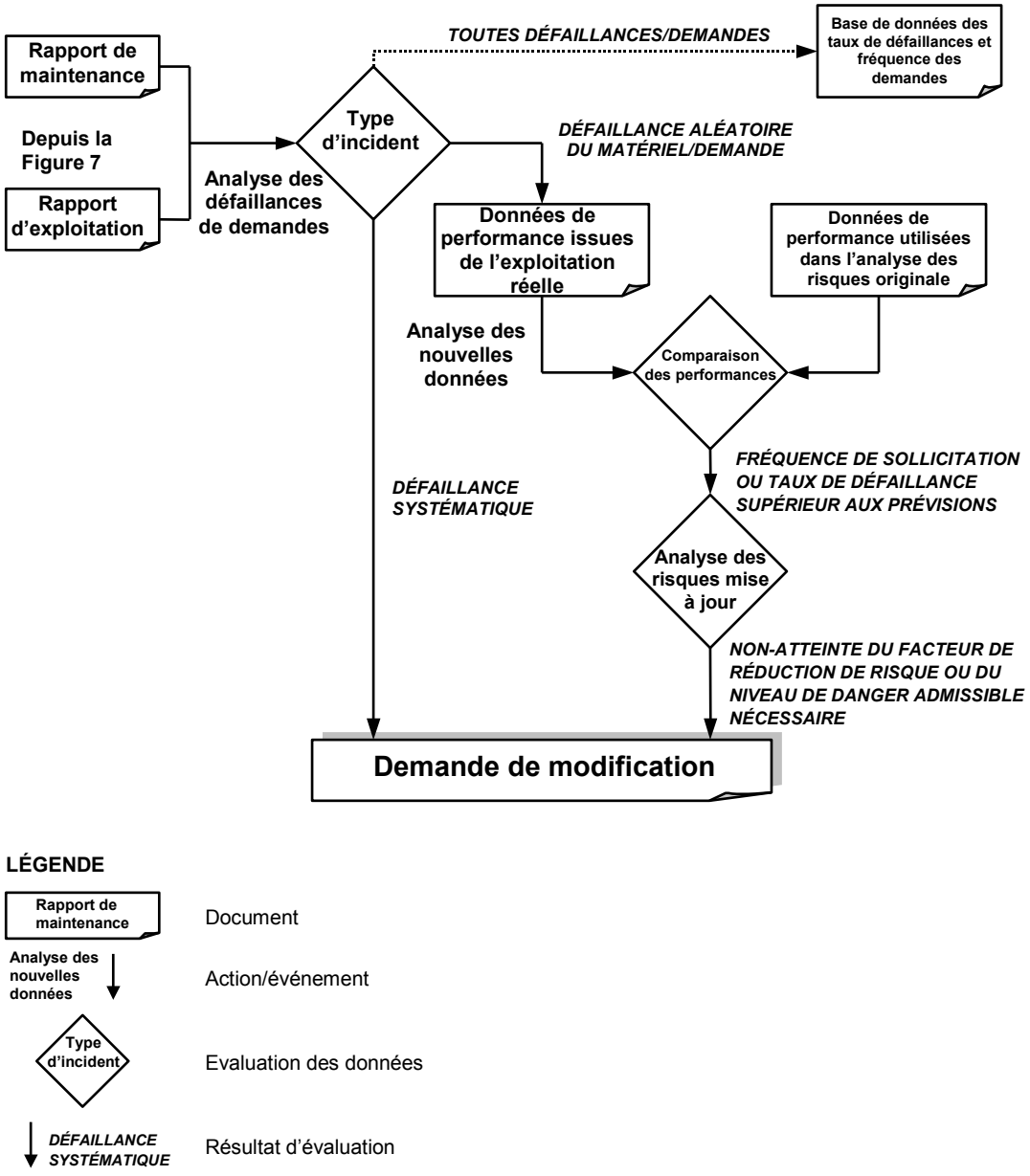


Figure 8 – Exemple de modèle de gestion d'exploitation et de maintenance

7.16 Modification et remise à niveau globales

NOTE 1 Cette phase correspond à la case 15 de la Figure 2.

NOTE 2 Les mesures organisationnelles dont il est question dans ce paragraphe permettent la mise en œuvre efficace des exigences techniques et ont pour unique but la réalisation et le maintien de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité. Les exigences techniques nécessaires au maintien de la sécurité fonctionnelle sont spécifiées comme partie intégrante des informations communiquées par le fournisseur du système E/E/PE relatif à la sécurité et de ses éléments et composants.

NOTE 3 Les exigences spécifiées dans ce paragraphe sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 4 Pour obtenir la sécurité fonctionnelle, des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risques.

7.16.1 Objectif

L'objectif des exigences de ce paragraphe est de définir les procédures nécessaires pour assurer que la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité est appropriée, à la fois pendant et après la phase de modification et de remise à niveau.

7.16.2 Exigences

7.16.2.1 Avant d'entreprendre toute activité de modification ou de remise à niveau, les procédures doivent être programmées (voir 6.2.8).

NOTE Un exemple de modèle de procédure pour les modifications est présenté à la Figure 9.

7.16.2.2 La phase de modification et de remise à niveau ne doit pouvoir être initiée que par l'émission d'une demande officielle selon les procédures pour la gestion de la sécurité fonctionnelle (voir 6.2.8). Cette demande doit détailler les points suivants:

– les dangers déterminés qui peuvent être concernés,

– la modification proposée (à la fois matérielle et logicielle),

– les motifs de cette modification.

NOTE Le motif de cette demande de modification peut provenir, par exemple:

a) d'une sécurité fonctionnelle inférieure à celle spécifiée,

b) d'une anomalie systématique mise en évidence par expérimentation,

c) d'une législation de sécurité nouvelle ou modifiée,

d) des modifications apportées à l'EUC ou à son utilisation,

e) d'une modification des exigences globales de sécurité,

f) d'une analyse des performances d'exploitation et de maintenance, indiquant que ces performances sont inférieures à celles prévues,

g) des audits de sécurité fonctionnelle systématiques.

7.16.2.3 Une analyse d'impact doit être réalisée. Cette dernière doit comprendre une évaluation de l'impact de l'activité de modification ou de remise à niveau proposée sur la sécurité fonctionnelle de tout système E/E/PE relatif à la sécurité. L'évaluation doit inclure une analyse des dangers et des risques suffisante pour déterminer l'étendue et la profondeur que doivent couvrir les phases ultérieures du cycle de vie de sécurité global du système E/E/PE ou du logiciel. L'évaluation doit aussi prendre en compte l'impact des autres activités de modification ou de remise à niveau menées en parallèle, et doit également prendre en compte la sécurité fonctionnelle à la fois pendant et après les activités de modification et de remise à niveau.

7.16.2.4 Les résultats décrits en 7.16.2.3 doivent être documentés.

7.16.2.5 L'autorisation d'effectuer l'activité de modification ou de remise à niveau requise doit dépendre des résultats de l'analyse d'impact.

7.16.2.6 Toutes les modifications ayant un impact sur la sécurité fonctionnelle de tout système E/E/PE relatif à la sécurité doit entraîner un retour à la phase appropriée du cycle de vie de sécurité global des systèmes E/E/PE relatifs à la sécurité ou des logiciels. Toutes les phases ultérieures doivent alors être exécutées conformément aux procédures spécifiées pour les phases spécifiques conformément aux exigences de la présente norme.

NOTE 1 Il peut être nécessaire de mettre en œuvre une analyse complète des dangers et des risques, qui peut générer un besoin de niveaux d'intégrité de sécurité qui sont différents de ceux actuellement spécifiés pour les fonctions de sécurité mises en œuvre par les systèmes E/E/PE relatifs à la sécurité.

NOTE 2 Il convient de ne pas supposer que les procédures d'essai développées pour l'installation et la mise en service initiales peuvent être utilisées sans vérifier leur validité et leur praticabilité dans le cadre d'exploitations «en ligne» de l'EUC.

7.16.2.7 Une documentation chronologique doit être établie et tenue à jour. Elle doit contenir les détails de toutes les modifications et remises à niveau, et doit faire référence:

– à la demande de modification ou de remise à niveau,

– à l'analyse d'impact,

– à la revérification et à la revalidation des données et des résultats,

– à tous les documents affectés par l'activité de modification et de remise à niveau.

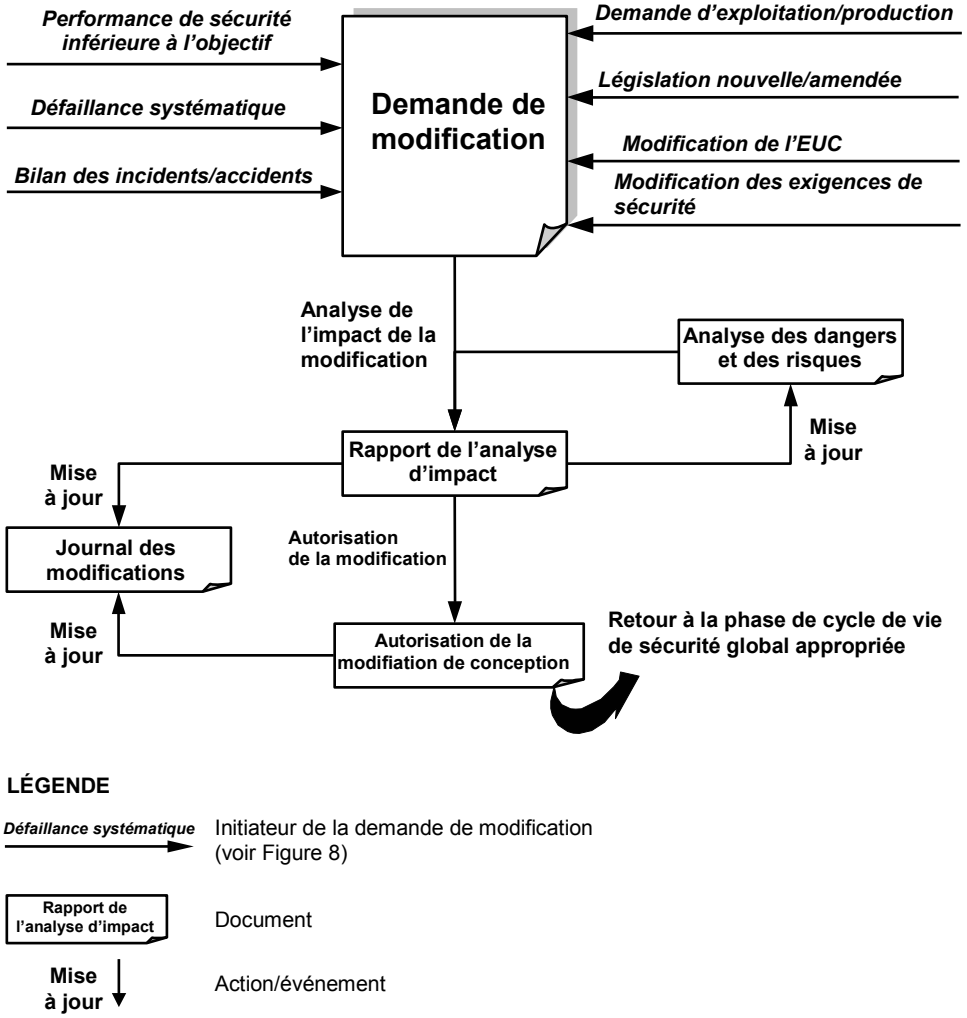


Figure 9 – Exemple de modèle de procédure de modification

7.17 Mise hors service ou au rebut

NOTE 1 Cette phase correspond à la case 16 de la Figure 2.

NOTE 2 Les exigences spécifiées dans ce paragraphe sont spécifiques aux systèmes E/E/PE relatifs à la sécurité. Il convient de les prendre en considération dans le cadre des dispositifs externes de réduction de risque, en tenant particulièrement compte des hypothèses déjà formulées concernant ces dispositifs qui doivent être maîtrisés tout au long de la durée de vie de l'EUC.

NOTE 3 Des exigences similaires sont nécessaires pour tous les dispositifs externes de réduction de risque afin d'obtenir une sécurité fonctionnelle.

7.17.1 Objectif

L'objectif des exigences de ce paragraphe est de définir les procédures nécessaires pour assurer que la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité est appropriée aux circonstances pendant et après les activités de mise hors service ou au rebut de l'EUC.

7.17.2 Exigences

7.17.2.1 Avant d'entreprendre toute activité de mise hors service ou au rebut, une analyse d'impact doit être effectuée. Elle doit comprendre une évaluation de l'impact de l'activité proposée de mise hors service ou au rebut sur la sécurité fonctionnelle de tout système E/E/PE relatif à la sécurité associé à l'EUC. L'analyse d'impact doit aussi prendre en compte

les EUC adjacents et l'impact sur leurs systèmes E/E/PE relatifs à la sécurité. L'évaluation doit inclure une analyse des dangers et des risques suffisante pour déterminer l'étendue et la profondeur nécessaires que doivent couvrir les phases ultérieures du cycle de vie de sécurité global du système E/E/PE ou du logiciel.

7.17.2.2 Les résultats décrits en 7.17.2.1 doivent être documentés.

7.17.2.3 La phase de mise hors service ou au rebut ne doit pouvoir être initiée que par l'émission d'une demande officielle selon les procédures de gestion de la sécurité fonctionnelle (voir Article 6).

7.17.2.4 L'autorisation d'effectuer la mise hors service ou au rebut demandée doit dépendre des résultats de l'analyse d'impact.

7.17.2.5 Avant d'entreprendre la mise hors service ou au rebut, un plan doit être préparé. Ce dernier doit comporter les procédures applicables:

– à l'arrêt définitif des systèmes E/E/PE relatifs à la sécurité,
– au démantèlement des systèmes E/E/PE relatifs à la sécurité.

7.17.2.6 Si l'une des activités de mise hors service ou au rebut a un impact sur la sécurité fonctionnelle de tout système E/E/PE relatif à la sécurité, cela doit entraîner un retour à la phase appropriée du cycle de vie de sécurité global des systèmes E/E/PE ou des logiciels. Toutes les phases ultérieures doivent alors être exécutées conformément aux procédures spécifiées dans la présente norme pour les niveaux d'intégrité de sécurité relatifs aux fonctions de sécurité mises en œuvre par les systèmes E/E/PE relatifs à la sécurité.

NOTE 1 Il peut être nécessaire de mettre en œuvre une analyse complète des dangers et des risques qui peut générer un besoin de niveaux d'intégrité de sécurité différents pour les fonctions de sécurité mises en œuvre par les systèmes E/E/PE relatifs à la sécurité.

NOTE 2 Les exigences de sécurité fonctionnelle pendant la phase de mise hors service ou au rebut peuvent être différentes de celles requises lors de la phase d'exploitation.

7.17.2.7 Une documentation chronologique doit être établie et tenue à jour. Elle doit contenir les documents détaillant les activités de mise hors service ou au rebut, et doit faire référence:

– au plan utilisé pour les activités de mise hors service ou au rebut,
– à l'analyse d'impact.

7.18 Vérification

7.18.1 Objectif

L'objectif des exigences de ce paragraphe est de démontrer, pour chaque phase des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel (par des revues, analyses et/ou essais), que les données de sortie satisfont en tout point aux objectifs et exigences spécifiés pour cette phase.

7.18.2 Exigences

7.18.2.1 Pour chaque phase des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel, un plan pour la vérification doit être établi en parallèle avec le développement de cette phase.

7.18.2.2 Le plan de vérification doit documenter ou faire référence aux critères, techniques et outils devant être utilisés dans les activités de vérification.

7.18.2.3 La vérification doit être effectuée selon le plan de vérification.

NOTE La sélection des techniques et des mesures pour la vérification ainsi que le degré d'indépendance pour les activités de vérification dépendent d'un certain nombre de facteurs et ils peuvent être spécifiés dans les normes internationales de produit et d'application sectorielle.

Ces facteurs peuvent inclure, par exemple

– la taille du projet,
– le degré de complexité,
– le degré de nouveauté de la conception,
– le degré de nouveauté technologique.

7.18.2.4 L'information concernant les activités de vérification doit être collectée et documentée comme élément de preuve attestant que la phase en cours de vérification a été en tout point correctement réalisée.

8 Evaluation de la sécurité fonctionnelle

8.1 Objectif

L'objectif des exigences de ce paragraphe est de spécifier les activités nécessaires pour, sur la base de la conformité aux articles pertinents de la présente norme, analyser et juger de l'adéquation de la sécurité fonctionnelle réalisée par le(s) système(s) E/E/PE relatif(s) à la sécurité ou des entités conformes (par exemple, éléments/sous-systèmes).

8.2 Exigences

8.2.1 Une ou plusieurs personnes doivent être désignées pour exécuter une ou plusieurs évaluations de la sécurité fonctionnelle, afin d'élaborer un jugement sur la pertinence:

– de la sécurité fonctionnelle réalisée par les systèmes E/E/PE relatifs à la sécurité, dans leur environnement particulier, compte tenu des articles pertinents de la présente norme,
– de la conformité aux articles appropriés de la présente norme, obtenue dans le cas d'éléments/sous-systèmes.

8.2.2 Les responsables de cette évaluation de la sécurité fonctionnelle doivent pouvoir contacter toutes les personnes impliquées dans toute activité du cycle de vie de sécurité global du système E/E/PE ou du logiciel, et avoir accès à toutes les informations et à tous les équipements (à la fois matériels et logiciels) pertinents.

NOTE Il est admis qu'il peut ne pas être possible de contacter les personnes précédemment impliquées dans une phase du cycle de vie de sécurité, la confiance devant alors être nécessairement accordée aux personnes actuellement responsables.

8.2.3 Une évaluation de la sécurité fonctionnelle doit être appliquée à toutes les phases des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel, y compris la documentation, la vérification et la gestion de la sécurité fonctionnelle.

8.2.4 Les responsables de l'évaluation de la sécurité fonctionnelle doivent prendre en compte les activités menées et les données de sortie obtenues au cours de chaque phase des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel, et doivent juger dans quelle mesure la sécurité fonctionnelle adéquate a été réalisée sur la base des objectifs et des exigences de la présente norme.

8.2.5 Toutes les déclarations pertinentes de conformité formulées par les fournisseurs et les autres parties responsables de la réalisation de la sécurité fonctionnelle doivent être incluses dans l'évaluation de cette sécurité.

NOTE Ces déclarations peuvent être formulées pour un système de fonctionnement ou pour la contribution à la sécurité fonctionnelle des activités et/ou équipements dans chaque phase des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel.

8.2.6 Une évaluation de la sécurité fonctionnelle peut être effectuée après chaque phase des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel, ou après un certain nombre de phases du cycle de vie de sécurité, sous réserve de l'exigence prioritaire stipulant qu'une évaluation de la sécurité fonctionnelle doit être réalisée avant que les dangers déterminés ne soient présents.

8.2.7 Une évaluation de la sécurité fonctionnelle doit inclure l'évaluation de la preuve attestant que le ou les audits de la sécurité fonctionnelle a (ont) été effectué(s) (en tout ou en partie) conformément à son domaine d'application.

8.2.8 Chaque évaluation de la sécurité fonctionnelle doit tenir compte au moins des éléments suivants:

– le travail effectué depuis l'évaluation de la sécurité fonctionnelle précédente,
– les plans ou la stratégie pour la mise en œuvre ultérieure d'évaluations de la sécurité fonctionnelle des cycles de vie de sécurité globaux des systèmes E/E/PE et du logiciel,
– les recommandations des évaluations de la sécurité fonctionnelle précédentes et l'étendue des changements réalisés pour les satisfaire.

8.2.9 Chaque évaluation de la sécurité fonctionnelle doit faire l'objet d'une planification. Le plan doit préciser toutes les informations nécessaires pour faciliter une évaluation efficace, y compris:

– le domaine d'application de l'évaluation de la sécurité fonctionnelle,
– les entités impliquées,
– les ressources requises,
– les responsables de l'évaluation de la sécurité fonctionnelle,
– le degré d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle,
– la compétence de chaque personne impliquée dans l'évaluation de la sécurité fonctionnelle,
– les résultats de l'évaluation de la sécurité fonctionnelle,
– le processus d'association, et d'intégration, de l'évaluation de la sécurité fonctionnelle aux autres évaluations de cette dernière le cas échéant (voir 6.2.1).

NOTE 1 Lors de la définition du domaine d'application de chaque évaluation de la sécurité fonctionnelle, il est nécessaire de spécifier les documents, ainsi que leur statut de révision, qui doivent être utilisés comme données d'entrée pour chaque activité d'évaluation.

NOTE 2 Le plan peut être élaboré par les personnes responsables de l'évaluation de la sécurité fonctionnelle ou par les personnes responsables de la gestion de cette sécurité ou peut être partagé entre elles.

8.2.10 Avant d'entreprendre l'évaluation de la sécurité fonctionnelle, le plan doit être approuvé par les responsables de cette évaluation, ainsi que par les responsables de la gestion de la sécurité fonctionnelle.

8.2.11 A la fin de l'évaluation de la sécurité fonctionnelle, les personnes chargées de cette activité doivent documenter, conformément aux plans et aux conditions de l'évaluation:

– les activités menées,
– les constatations formulées,
– les conclusions tirées,
– un jugement concernant la pertinence de la sécurité fonctionnelle conformément aux exigences de la présente norme,
– les recommandations issues de l'évaluation, y compris celles concernant l'acceptation, l'acceptation conditionnelle ou le rejet.

8.2.12 Les résultats pertinents de l'évaluation de la sécurité fonctionnelle d'une entité conforme doivent être mis à disposition des personnes responsables de toute activité relative

au cycle de vie de sécurité global des systèmes E/E/PE ou du logiciel, ainsi qu'aux personnes impliquées dans la conception et l'évaluation du système E/E/PE relatif à la sécurité. Le résultat de l'évaluation de ce système doit être communiqué à l'intégrateur de ce dernier.

NOTE Une entité conforme est une entité (par exemple, un élément) faisant l'objet d'une déclaration, compte tenu des articles de la série CEI 61508.

8.2.13 Le résultat de l'évaluation de la sécurité fonctionnelle d'une entité conforme doit comporter les informations suivantes afin de faciliter la réutilisation des résultats d'évaluation dans le cadre d'un système de plus grand taille (voir Annexe D de la CEI 61508-2; Annexe D de la CEI 61508-3 et 3.8.17 de la CEI 61508-4).

a) l'identification précise de l'entité conforme, y compris la version de ses matériels et logiciels,

NOTE Si l'entité conforme a été évaluée comme partie intégrante d'une plus grande famille de systèmes ou d'équipements, il convient également de documenter l'identification précise de cette famille.

b) les conditions supposées pendant l'évaluation (par exemple, les conditions d'utilisation du système E/E/PE relatif à la sécurité),

c) la référence à la preuve documentaire sur laquelle la conclusion de l'évaluation était basée,

d) les procédures, méthodes et outils utilisés pour l'évaluation de la capabilité systématique, ainsi que la justification de son efficacité,

e) les procédures, méthodes et outils utilisés pour l'évaluation de l'intégrité de sécurité des matériels, ainsi que la justification de l'approche adoptée et la qualité des données (par exemple, le taux de défaillance/les sources de données de répartition),

f) les résultats d'évaluation obtenus par rapport aux exigences de la présente norme et à la spécification des caractéristiques de sécurité de l'entité conforme dans son manuel de sécurité,

g) les écarts admis par rapport aux exigences de la CEI 61508, avec l'explication et/ou la référence correspondante aux éléments de preuve contenus dans la documentation.

8.2.14 Les personnes chargées de l'évaluation de la sécurité fonctionnelle doivent être compétentes pour les activités à entreprendre, conformément aux exigences de 6.2.13 à 6.2.15.

8.2.15 Le degré minimal d'indépendance des personnes chargées de l'évaluation de la sécurité fonctionnelle doit être tel que spécifié dans les Tableaux 4 et 5 ci-après. Les normes internationales de produit et d'application sectorielle peuvent spécifier pour la conformité à leurs étalons, différents degrés d'indépendance par rapport à ceux spécifiés dans les Tableaux 4 et 5. Les tableaux doivent être interprétés comme suit:

– X: le degré d'indépendance spécifié est le niveau minimal pour la conséquence spécifiée (Tableau 4) ou le niveau d'intégrité de sécurité/capabilité systématique (Tableau 5). Si un niveau inférieur d'indépendance est adopté, la justification de son utilisation doit être détaillée.

– X1 et X2: voir 8.2.16.

– Y: le degré d'indépendance spécifié est considéré comme insuffisant pour la conséquence spécifiée (Tableau 4) ou le niveau d'intégrité de sécurité/capabilité systématique (Tableau 5).

8.2.16 Dans le cadre des Tableaux 4 et 5, seules les cellules marquées X, X1, X2, ou Y doivent être utilisées comme base de détermination du degré d'indépendance. Pour les cellules marquées X1 ou X2, X1 ou X2 est applicable (mais pas les deux), en fonction d'un certain nombre de facteurs spécifiques à l'application. Il convient de décrire en détail les raisons du choix de X1 ou X2. Les facteurs qui tendent à rendre X2 plus approprié que X1 sont les suivants:

– un défaut d'expérience antérieure avec une conception similaire,

– un degré de complexité plus élevé,

– une plus grande nouveauté de la conception,

– une plus grande nouveauté de la technologie.

NOTE 1 Selon l'organisation de l'entreprise et l'expertise au sein de cette entreprise, il se peut que l'exigence s'appliquant aux personnes et départements indépendants soit satisfaite par l'appel à une entité extérieure. Inversement, les entreprises qui ont des organismes internes qualifiés pour l'évaluation du risque et l'application de systèmes relatifs à la sécurité, qui sont indépendants et séparées (par l'intermédiaire de la hiérarchie et autres moyens) de celles responsables du développement principal, peuvent être capables d'utiliser leurs ressources propres pour satisfaire aux exigences s'appliquant à une entité indépendante.

NOTE 2 Voir 3.8.11, 3.8.12 et 3.8.13 de la CEI 61508-4 pour les définitions, respectivement, de «personne indépendante», «département indépendant» et «organisme indépendant».

NOTE 3 Il convient que les personnes qui effectuent une évaluation de la sécurité fonctionnelle accordent une attention toute particulière aux recommandations qu'elles formulent concernant tout élément relevant du domaine d'application de l'évaluation, dans la mesure où cela peut compromettre leur indépendance. Il est souvent approprié de formuler des recommandations concernant les aspects susceptibles d'engendrer un jugement de sécurité inappropriée, tel qu'un défaut d'éléments de preuve, mais il est habituellement inapproprié de formuler des recommandations concernant les mesures correctives spécifiques applicables à ces problèmes ou à des problèmes d'une autre nature.

8.2.17 Dans le cadre du Tableau 4, les valeurs consécutives pour le degré d'indépendance spécifié sont les suivantes:

– Conséquence A: petite blessure (par exemple, perte temporaire de fonction),

– Conséquence B: blessure grave et permanente d'une ou plusieurs personnes; mort d'une personne,

– Conséquence C: mort de plusieurs personnes,

– Conséquence D: un très grand nombre de personnes tuées.

Les conséquences spécifiées dans le Tableau 4 sont celles qui pourraient se produire en cas de défaillance de tous les dispositifs de réduction de risque, y compris les systèmes E/E/PE relatifs à la sécurité.

8.2.18 Dans le cadre du Tableau 5, les degrés minimaux d'indépendance doivent être basés sur la fonction de sécurité, exécutée par le système E/E/PE relatif à la sécurité, qui possède le plus haut niveau d'intégrité de sécurité ou pour les éléments/sous-systèmes, la capabilité systématique la plus élevée, spécifiée en termes de niveau d'intégrité de sécurité.

Tableau 4 – Degrés minimaux d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle (phases 1 à 8 et 12 à 16 incluses du cycle de vie de sécurité global (voir Figure 2))

Degré minimal d'indépendance	Conséquence (voir 8.2.17)			
	A	B	C	D
Personne indépendante	X	X1	Y	Y
Département indépendant		X2	X1	Y
Organisme indépendant			X2	X
NOTE Voir 8.2.15, 8.2.16 et 8.2.17 pour l'interprétation détaillée de ce tableau.				

Tableau 5 – Degrés minimaux d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle (phases 9 et 10 du cycle de vie de sécurité global, incluant toutes les phases des cycles de vie de sécurité du système E/E/PE et du logiciel) (voir Figures 2, 3 et 4)

Degré minimal d'indépendance	Niveau d'intégrité de sécurité/capabilité systématique			
	1	2	3	4
Personne indépendante	X	X1	Y	Y
Département indépendant		X2	X1	Y
Organisme indépendant			X2	X
NOTE Voir 8.2.15, 8.2.16 et 8.2.18 pour l'interprétation détaillée de ce tableau.				

Annexe A
(informative)

Exemple de structure de documentation

A.1 Généralités

Cette annexe fournit un exemple de structure de documentation et une méthode de spécification des documents pour structurer l'information afin de satisfaire aux exigences de l'Article 5. La documentation doit contenir l'information nécessaire et suffisante à l'exécution efficace

– de chaque phase des cycles de vie de sécurité globaux du système E/E/PE et du logiciel,

– de la gestion de la sécurité fonctionnelle (Article 6),

– des évaluations de la sécurité fonctionnelle (Article 8).

La constitution de l'information suffisante dépend d'un certain nombre de facteurs, y compris de la complexité et la taille des systèmes E/E/PE relatifs à la sécurité et les exigences relatives à l'application spécifique. La documentation nécessaire peut être spécifiée dans des normes internationales de produit et d'application sectorielle.

La quantité d'informations dans chaque document peut aller de quelques lignes à plusieurs pages et l'ensemble complet d'informations peut être divisé et présenté dans plusieurs documents physiques ou un seul document physique. La structure physique de la documentation dépend une fois encore de la taille et de la complexité des systèmes E/E/PE relatifs à la sécurité et elle tient compte des procédures de l'entreprise ainsi que des bonnes pratiques professionnelles du produit ou du secteur d'application spécifique.

L'exemple de structure de documentation indiqué dans la présente annexe est proposé pour illustrer une façon particulière de structurer l'information et la façon dont les documents peuvent être titrés. Se reporter à la référence [7] dans la Bibliographie pour de plus amples détails.

Un document est une quantité structurée d'informations destinées à la perception humaine, pouvant être échangées unitairement entre des utilisateurs et/ou des systèmes (se reporter à la référence [15] dans la Bibliographie). Ce terme ne s'applique donc pas uniquement aux documents au sens courant, mais également à des concepts comme les fichiers de données et les bases de données d'information.

Dans la présente norme, le terme «document» est généralement compris au sens «d'information» plutôt que documents physiques, sauf si le contraire est explicitement indiqué ou compris dans le contexte de l'article ou du paragraphe dans lequel il est employé. Les documents peuvent être disponibles sous différentes formes pour la présentation aux personnes (par exemple sur papier, film ou tout support de données pouvant être présenté sur des écrans).

L'exemple de structure de documentation de la présente annexe spécifie les documents en deux parties:

– **le type de document**,

– **l'activité ou l'objet.**

Le type de document est défini dans la référence [16] de la Bibliographie et caractérise son contenu, par exemple, une description de fonction ou un diagramme de circuit. L'activité ou l'objet décrit le domaine d'application du contenu, par exemple, «système de commande de pompe».

Les types de documents de base spécifiés dans la présente annexe sont

– **spécification** – spécifie une fonction, performance ou activité requise (par exemple, une spécification d'exigences),
– **description** – spécifie une fonction, une conception, une réalisation ou une activité prévues ou réelles (par exemple, une description de fonction),
– **instruction** – spécifie en détail les instructions expliquant à quel moment et comment réaliser certains travaux (par exemple, une instruction d'opérateur),
– **plan** – spécifie le plan expliquant à quel moment, comment et par qui des activités spécifiques doivent être réalisées (par exemple, un plan de maintenance),
– **diagramme** – spécifie la fonction à l'aide d'un diagramme (symboles et lignes représentant les signaux entre les symboles),
– **liste** – fournit l'information sous la forme d'une liste (par exemple, liste de codes, de signaux),
– **journal** – fournit l'information sur les événements sous la forme d'un enregistrement chronologique,
– **rapport** – décrit les résultats d'activités telles que les enquêtes, les évaluations, les essais, etc. (par exemple, un rapport d'essai),
– **demande** – fournit une description des actions demandées qui doivent être approuvées et spécifiées ultérieurement (par exemple, demande de maintenance).

Les types de documents de base peuvent avoir un suffixe, tel que spécification d'**exigences** ou spécification d'**essai**, qui caractérise davantage le contenu.

A.2 Structure du document du cycle de vie de sécurité

Les Tableaux A.1, A.2 et A.3 fournissent un exemple de structure de documentation pour structurer l'information afin de satisfaire aux exigences spécifiées à l'Article 5. Les tableaux indiquent la phase du cycle de vie de sécurité qui est principalement associée aux documents (généralement la phase dans laquelle ils sont élaborés). Les noms donnés aux documents dans les tableaux sont conformes à la syntaxe décrite succinctement en A.1.

Outre les documents énumérés dans les Tableaux A.1, A.2 et A.3, il peut exister des documents supplémentaires donnant une information détaillée supplémentaire ou une information structurée dans un but spécifique, par exemple, des listes de pièces, des listes de signaux, des listes de câbles, des tableaux de câblage, des diagrammes de boucle ou des listes de variables.

NOTE Les exemples de telles variables incluent les valeurs pour les régulateurs, les valeurs d'alarme pour les variables et les priorités dans l'exécution des tâches par l'ordinateur. Certaines valeurs des variables peuvent être données avant la livraison du système, d'autres pouvant être données lors de la mise en service ou de la maintenance.

Tableau A.1 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité global

Phase du cycle de vie de sécurité global	Information
Concept	Description (concept global)
Définition globale du domaine d'application	Description (définition globale du domaine d'application)
Analyse des dangers et des risques	Description (analyse des dangers et des risques)
Exigences globales de sécurité	Spécification (exigences globales de sécurité, comprenant: les exigences globales relatives aux fonctions de sécurité et les exigences globales relatives à l'intégrité de sécurité)
Allocation des exigences globales de sécurité	Description (allocation des exigences globales de sécurité)
Planification globale de l'exploitation et de la maintenance	Plan (exploitation et maintenance globales)
Planification globale de la validation de la sécurité	Plan (validation globale de la sécurité)
Planification globale de l'installation et de la mise en service	Plan (installation globale), Plan (mise en service globale)
Exigences de sécurité relatives aux systèmes E/E/PE	Spécification (exigences de sécurité relatives aux systèmes E/E/PE comprenant: les exigences relatives aux fonctions de sécurité et à l'intégrité de sécurité des systèmes E/E/PE)
Réalisation des systèmes E/E/PE relatifs à la sécurité	Voir Tableau A.2 et Tableau A.3
Installation et mise en service globales	Rapport (installation globale), Rapport (mise en service globale)
Validation globale de la sécurité	Rapport (validation globale de la sécurité)
Exploitation et maintenance globales	Journal (exploitation et maintenance globales)
Modification et remise à niveau globales	Demande (modification globale), Rapport (analyse d'impact de la modification ou de la remise à niveau globale, Journal (modification et remise à niveau globales)
Mise hors service ou au rebut	Rapport (analyse d'impact de la mise hors service ou au rebut globale), Plan (mise hors service ou au rebut globale), Journal (mise hors service ou au rebut globale)
Concerne toutes les phases	Plan (sécurité), Plan (vérification), Rapport (vérification), Plan (évaluation de la sécurité fonctionnelle), Rapport (évaluation de la sécurité fonctionnelle)

Tableau A.2 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité du système E/E/PE

Phase du cycle de vie de sécurité du système E/E/PE	Information
Planification de la validation des systèmes E/E/PE	Plan (Validation de la sécurité des systèmes E/E/PE)
Conception et développement des systèmes E/E/PE	
Architecture des systèmes E/E/PE	Description (conception de l'architecture des systèmes E/E/PE comprenant: l'architecture du matériel et du logiciel), spécification (essais d'intégration de l'électronique programmable), spécification (essais d'intégration du matériel électronique programmable et non électronique programmable)
Architecture du matériel	Description (conception de l'architecture du matériel), Spécification (essais d'intégration de l'architecture du matériel)
Conception du module matériel	Spécification (conception des modules matériels), Spécifications (essais des modules matériels)
Construction et/ou achat des composants	Modules matériels, Rapport (essais des modules matériels)
Intégration de l'électronique programmable	Rapport (essais d'intégration des matériels et logiciels de l'électronique programmable) (voir Tableau A.3)
Intégration des systèmes E/E/PE	Rapport (essais d'intégration de l'électronique et autres matériels programmables)
Procédures d'exploitation et de maintenance des systèmes E/E/PE	Instruction (utilisateur), Instruction (exploitation et maintenance)
Validation de la sécurité des systèmes E/E/PE	Rapport (validation de la sécurité des systèmes E/E/PE)
Modification des systèmes E/E/PE	Instruction (procédures de modification des systèmes E/E/PE), Demande (modification des systèmes E/E/PE), Rapport (analyse d'impact de modification des systèmes E/E/PE), Journal (modification des systèmes E/E/PE)
Concerne toutes les phases	Plan (sécurité des systèmes E/E/PE), Plan (vérification des systèmes E/E/PE), Rapport (vérification des systèmes E/E/PE), Plan (évaluation de la sécurité fonctionnelle des systèmes E/E/PE), Rapport (évaluation de la sécurité fonctionnelle des systèmes E/E/PE)
Concerne toutes les phases appropriées	Manuel de sécurité d'article conforme

Tableau A.3 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité du logiciel

Phase du cycle de vie de sécurité du logiciel	Information
Exigences relatives à la sécurité du logiciel	Spécification (exigences de sécurité du logiciel, comprenant: les exigences relatives aux fonctions de sécurité et à l'intégrité de sécurité du logiciel)
Planification de la validation du logiciel	Plan (validation de la sécurité du logiciel)
Conception et développement du logiciel	
Architecture du logiciel	Description (conception de l'architecture du logiciel) (voir Tableau A.2 pour la description de la conception de l'architecture du matériel), Spécification (essais d'intégration de l'architecture du logiciel), Spécification (essais d'intégration du matériel et du logiciel de l'électronique programmable), Instruction (outils de développement et manuel de codage)
Conception du système logiciel	Description (conception des systèmes logiciel), Spécification (essais d'intégration du système logiciel)
Conception du module logiciel	Spécification (conception du module logiciel), Spécification (essais du module logiciel)
Codage	Liste (code source), Rapport (essais du module logiciel), Rapport (examen des codes)
Essais du module logiciel	Rapport (essais des modules logiciels)
Intégration du logiciel	Rapport (essais d'intégration des modules logiciels), Rapport (essais d'intégration des systèmes logiciels), Rapport (essais d'intégration de l'architecture du logiciel)
Intégration de l'électronique programmable	Rapport (essais d'intégration des matériels et logiciels de l'électronique programmable)
Procédures d'exploitation et de maintenance du logiciel	Instruction (utilisateur), Instruction (exploitation et maintenance)
Validation de la sécurité du logiciel	Rapport (validation de la sécurité du logiciel)
Modification du logiciel	Instruction (procédures de modification du logiciel), Demande (modification du logiciel), Rapport (analyse d'impact de modification du logiciel), Journal (modification du logiciel)
Concerne toutes les phases	Plan (sécurité du logiciel), Plan (vérification du logiciel), Rapport (vérification du logiciel), Plan (évaluation de la sécurité fonctionnelle du logiciel), Rapport (évaluation de la sécurité fonctionnelle du logiciel)
Concerne toutes les phases appropriées	Manuel de sécurité d'article conforme

A.3 Structure physique du document

La structure physique de la documentation correspond à la façon dont les différents documents sont assemblés en documents, ensembles de documents, classeurs et groupes de classeurs. Un même document peut apparaître dans différents ensembles.

Pour un grand système complexe, il est très probable que les nombreux documents physiques soient divisés en plusieurs classeurs. Pour un petit système de faible complexité, avec un nombre limité de documents physiques, ces derniers peuvent être tous rassemblés dans un seul classeur avec différentes étiquettes intercalaires pour les différents ensembles de documents. La Figure A.1 présente des exemples de rassemblement de documents en classeurs selon les groupes d'utilisateurs.

La structure physique fournit un moyen de sélection de la documentation nécessaire pour les activités spécifiques par la personne ou le groupe de personnes réalisant ces activités. Par conséquent, certains documents physiques peuvent apparaître dans plusieurs ensembles de classeurs ou tout autre support (par exemple, les disques informatiques).

NOTE L'information requise par les documents du Tableau A.1 peut être contenue dans les divers ensembles de documents présentés à la Figure A.1. Par exemple, l'ensemble pour l'ingénierie peut contenir la description de l'analyse des dangers et des risques, ainsi que la spécification des exigences globales de sécurité.

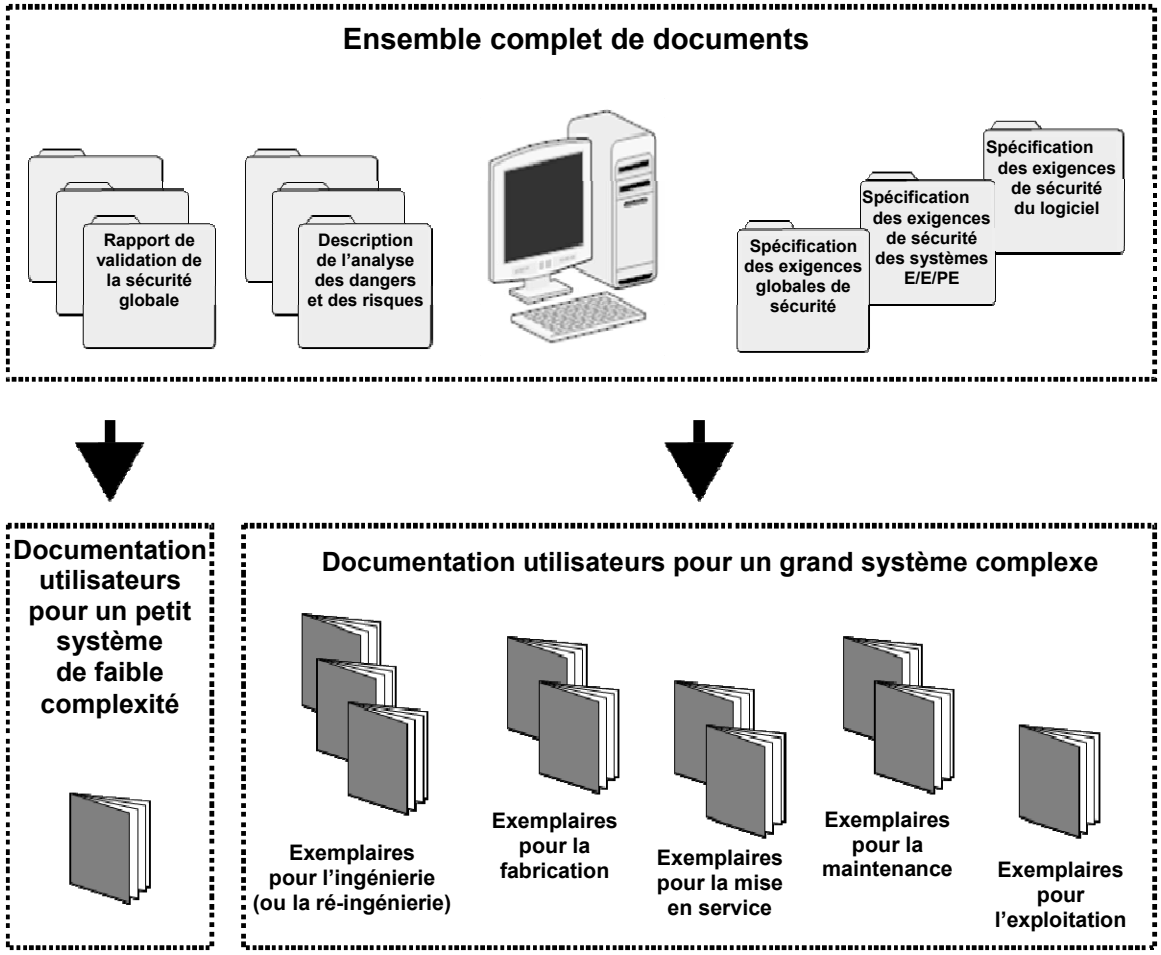


Figure A.1 – Structuration de l'information en ensembles de documents pour les groupes d'utilisateurs

A.4 Liste des documents

La liste des documents inclut typiquement les informations suivantes:

– le numéro des plans ou des documents,
– l'index de révision,
– le code de désignation du document,
– le titre,
– la date de révision,
– le support de données.

Cette liste peut prendre différents aspects, par exemple celui d'une base de données pouvant être triée selon les numéros de plan ou de document, ou le code de désignation du document. Le code de désignation du document peut contenir la désignation de référence pour la fonction, la localisation ou le produit décrit dans le document, faisant de ce code un outil de recherche d'information puissant.

Bibliographie

[1] CEI 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[2] CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[3] CEI 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional* (disponible en anglais seulement)

[4] CEI/TR 61508-0:2005, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 0: La sécurité fonctionnelle et la CEI 61508*

[5] CEI 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

[6] CEI 61508-7:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

[7] CEI 61506:1997, *Mesure et commande dans les processus industriels – Documentation des logiciels d'application*

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

[9] *Competence criteria for safety-related system practitioners*. IET. 2006 (disponible en anglais seulement)

[10] CEI 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology* (disponible en anglais seulement)

[11] CEI 60300-3-9:1995, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 9: Analyse du risque des systèmes technologiques*

[12] CEI 61882:2001, *Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application*

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

[14] NUREG/CR-47801989, Volume 2, January 1989, *Procedures for treating common cause failures in safety and reliability studies – Analytical background and techniques* (disponible en anglais seulement)

[15] CEI 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

[16] ISO 8613-1:1994, *Technologies de l'information – Architecture des documents ouverts (ODA) et format d'échange: Introduction et principes généraux*

[17] CEI 61355 (toutes les parties), *Classification et désignation des documents pour installations industrielles, systèmes et matériels*

[18] CEI 60601 (toutes les parties), *Appareils électromédicaux*

[19] CEI/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena* (disponible en anglais seulement)

[20] CEI 61508-5:2010,*Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

[21] CEI 62443 (toutes les parties), *Industrial communication networks – Network and system security* (disponible en anglais seulement)

[22] ISO/CEI/TR 19791, *Technologies de l'information – Techniques de sécurité – Evaluation de la sécurité des systèmes opérationnels*

———————

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch