IEC 61508-2

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

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

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 It also gives information on projects, withdrawn and replaced publications.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 61508-2

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

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XD
CODE PRIX

ICS 25.040.40

ISBN 978-2-88910-525-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

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 61508-2 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 2000. 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/549/FDIS	65A/573/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, though 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;
- 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 2: Requirements for electrical/electronic/programmable electronic safety-related systems

1 Scope

1.1 This part of the IEC 61508 series

a) is intended to be used only after a thorough understanding of IEC 61508-1, which provides the overall framework for the achievement of functional safety;

b) applies to any safety-related system, as defined by IEC 61508-1, that contains at least one electrical, electronic or programmable electronic element;

c) applies to all elements within an E/E/PE safety-related system (including sensors, actuators and the operator interface);

d) specifies how to refine the E/E/PE system safety requirements specification, developed in accordance with IEC 61508-1 (comprising the E/E/PE system safety functions requirements specification and the E/E/PE system safety integrity requirements specification), into the E/E/PE system design requirements specification;

e) specifies the requirements for activities that are to be applied during the design and manufacture of the E/E/PE safety-related systems (i.e. establishes the E/E/PE system safety lifecycle model) except software, which is dealt with in IEC 61508-3 (see Figures 2 to 4). These requirements include the application of techniques and measures that are graded against the safety integrity level, for the avoidance of, and control of, faults and failures;

f) specifies the information necessary for carrying out the installation, commissioning and final safety validation of the E/E/PE safety-related systems;

g) does not apply to the operation and maintenance phase of the E/E/PE safety-related systems – this is dealt with in IEC 61508-1 – however, IEC 61508-2 does provide requirements for the preparation of information and procedures needed by the user for the operation and maintenance of the E/E/PE safety-related systems;

h) specifies requirements to be met by the organisation carrying out any modification of the E/E/PE safety-related systems;

NOTE 1 This part of IEC 61508 is mainly directed at suppliers and/or in-company engineering departments, hence the inclusion of requirements for modification.

NOTE 2 The relationship between IEC 61508-2 and IEC 61508-3 is illustrated in Figure 4.

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

1.2 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 standards. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

1.3 One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply

unless specifically referred to or included in the publications prepared by those technical committees.

NOTE The functional safety of an E/E/PE safety-related system can only be achieved when all related requirements are met. Therefore, it is important that all related requirements are carefully considered and adequately referenced.

1.4 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-2 plays in the achievement of functional safety for E/E/PE safety-related systems. Annex A of IEC 61508-6 describes the application of IEC 61508-2 and IEC 61508-3.

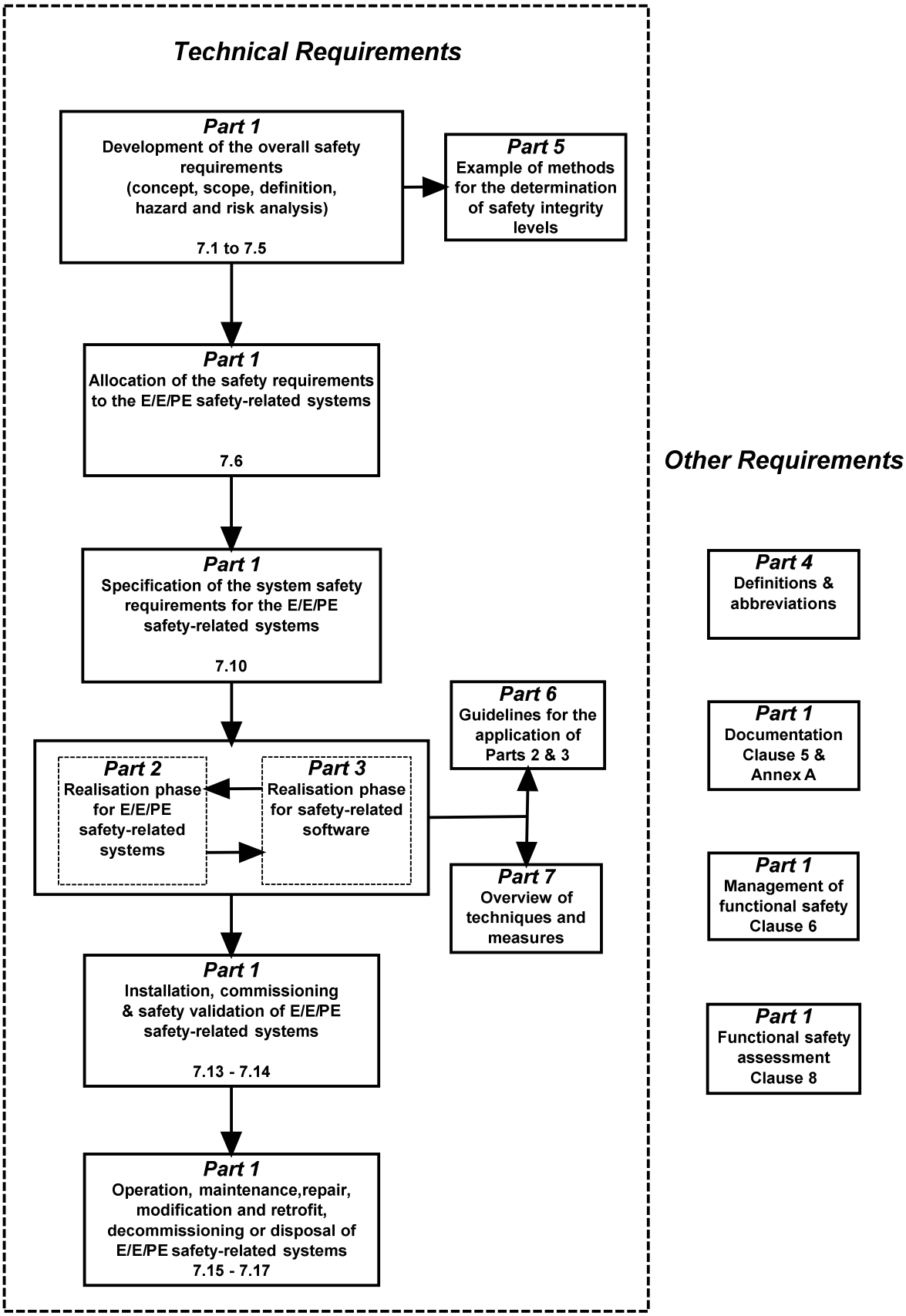


Figure 1 – Overall framework of the IEC 61508 series

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 60947-5-1, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

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*

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*

IEC 61508-1: 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

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*

EN 50205, *Relays with forcibly guided (mechanically linked) contacts*

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

The requirements for conformance to this standard are as detailed in Clause 4 of IEC 61508-1.

5 Documentation

The requirements for documentation are as detailed in Clause 5 of IEC 61508-1.

6 Management of functional safety

The requirements for management of functional safety are as detailed in Clause 6 of IEC 61508-1.

7 E/E/PE system safety lifecycle requirements

7.1 General

7.1.1 Objectives and requirements – general

7.1.1.1 This subclause sets out the objectives and requirements for the E/E/PE system safety lifecycle phases.

NOTE The objectives and requirements for the overall safety lifecycle, together with a general introduction to the structure of the standard, are given in IEC 61508-1.

7.1.1.2 For all phases of the E/E/PE system safety lifecycle, Table 1 indicates

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

7.1.2 Objectives

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

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

7.1.3 Requirements

7.1.3.1 The E/E/PE system safety lifecycle that shall be used in claiming conformance with this standard is that specified in Figure 2. A detailed V-model of the ASIC development lifecycle for the design of ASICs (see IEC 61508-4, 3.2.15) is shown in Figure 3. If another E/E/PE system safety lifecycle or ASIC development lifecycle is used, it shall be specified as part of the management of functional safety activities (see Clause 6 of IEC 61508-1), and all the objectives and requirements of each subclause of IEC 61508-2 shall be met.

NOTE 1 The relationship between and scope for IEC 61508-2 and IEC 61508-3 are shown in Figure 4.

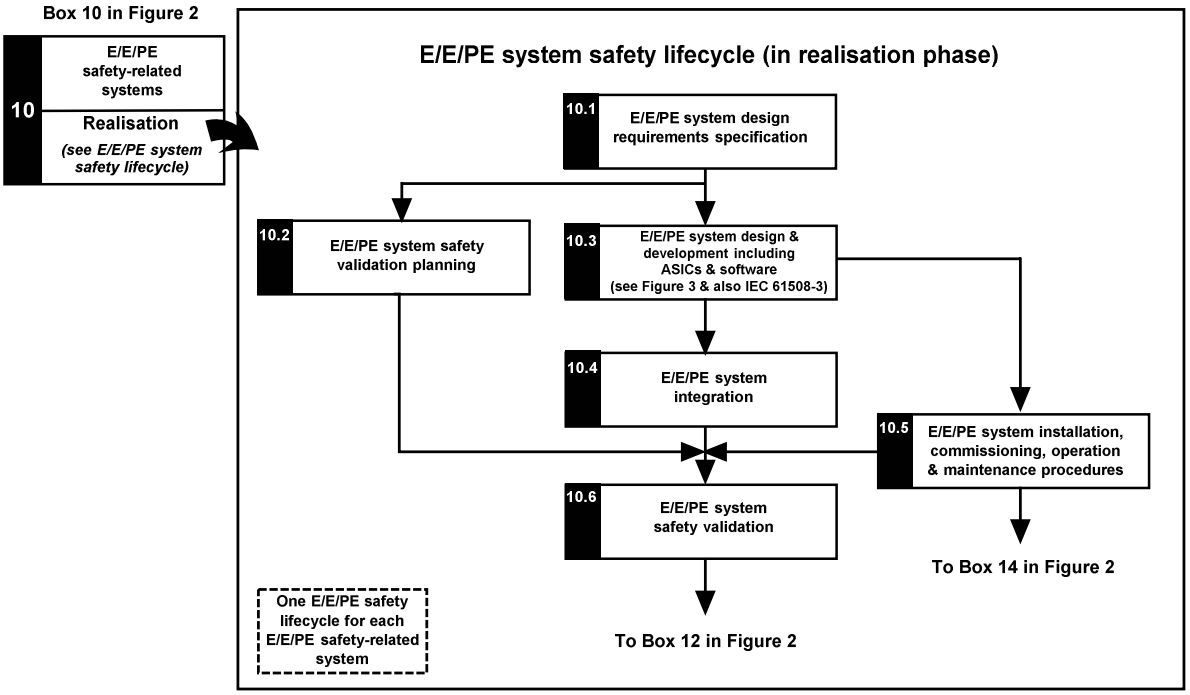
NOTE 2 There are significant similarities between the ASIC and the software design processes. IEC 61508-3 recommends the V-model for designing safety-related software. The V-model requires a clearly structured design process and a modular software structure for avoiding and controlling systematic faults. The ASIC development lifecycle for the design of ASICs in Figure 3 follows this model. At first the requirements for the ASIC specification are derived from the system requirements. ASIC architecture, ASIC design and module design follow. The results of each step on the left-hand side of the V become the input to the next step, and are also fed back to the preceding step for iteration where appropriate, until the final code is created. This code is verified against the corresponding design through post-layout simulation, module testing, module integration testing and verification of the complete ASIC. The results of any step may necessitate a revision to any of the preceding steps. Finally, the ASIC is validated after its integration into the E/E/PE safety-related system.

7.1.3.2 The procedures for management of functional safety (see Clause 6 of IEC 61508-1) shall run in parallel with the E/E/PE system safety lifecycle phases.

7.1.3.3 Each phase of the E/E/PE system safety lifecycle shall be divided into elementary activities, with the scope, inputs and outputs specified for each phase (see Table 1).

7.1.3.4 Unless justified as part of the management of functional safety activities (see Clause 6 of IEC 61508-1), the outputs of each phase of the E/E/PE system safety lifecycle shall be documented (see Clause 5 of IEC 61508-1).

7.1.3.5 The outputs for each E/E/PE system safety lifecycle phase shall meet the objectives and requirements specified for each phase (see 7.2 to 7.9).



NOTE 1 See also IEC 61508-6, A.2 b).

NOTE 2 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 of IEC 61508-1).

Figure 2 – E/E/PE system safety lifecycle (in realisation phase)

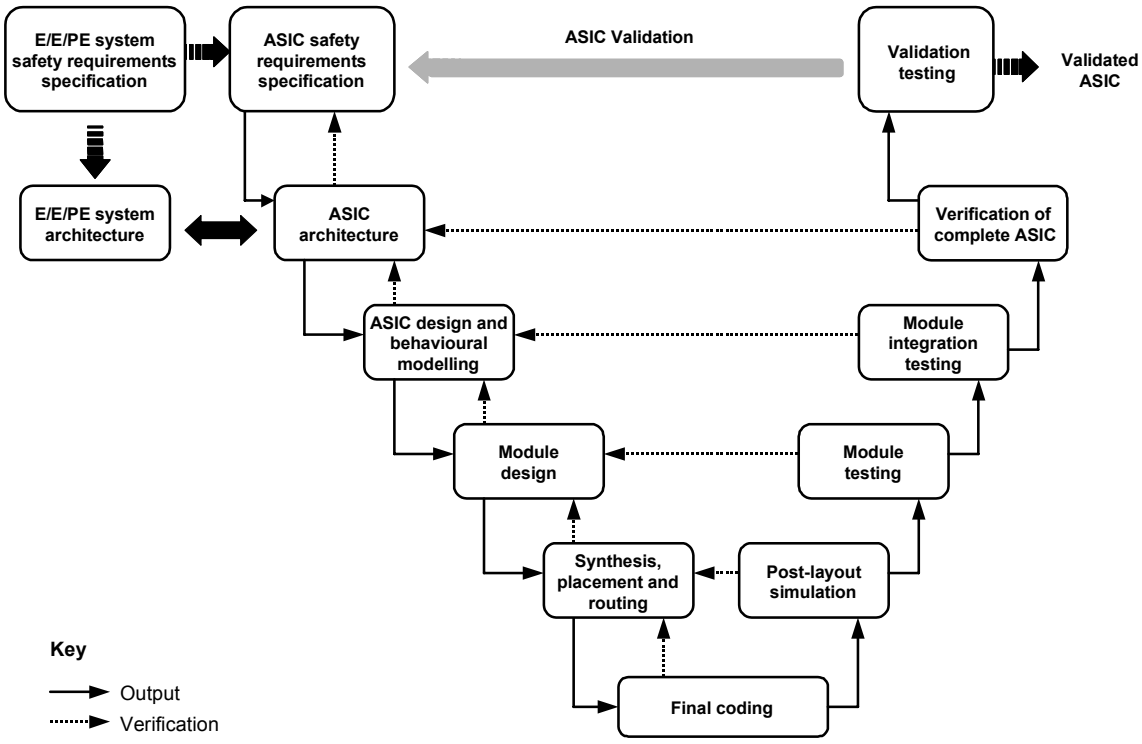


Figure 3 – ASIC development lifecycle (the V-Model)

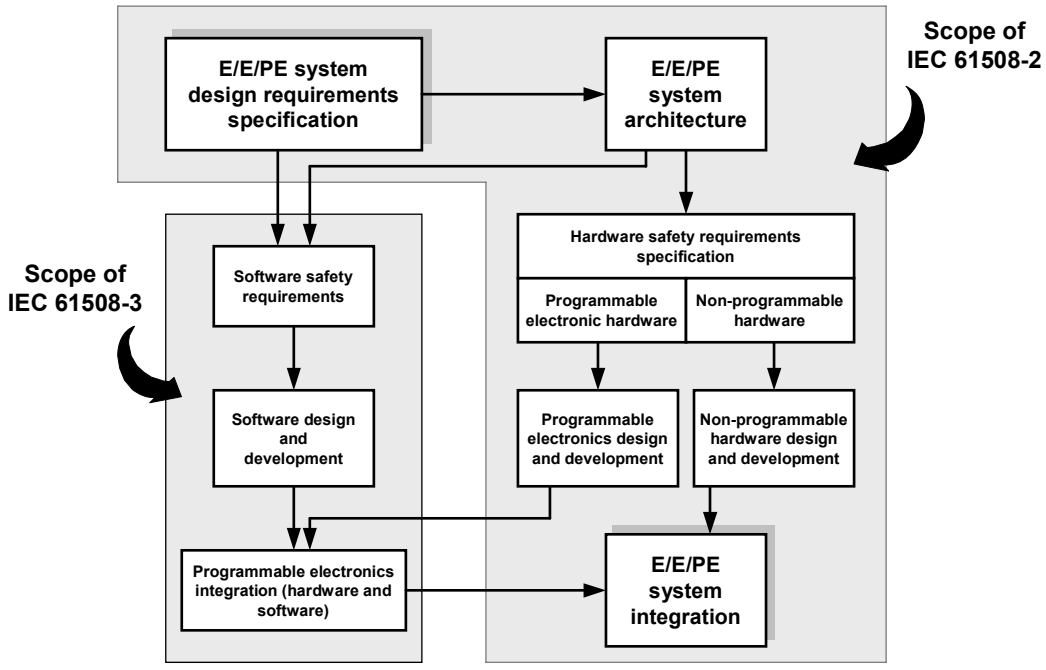


Figure 4 – Relationship between and scope of IEC 61508-2 and IEC 61508-3

Table 1 – Overview – realisation phase of the E/E/PE system safety lifecycle

Safety lifecycle phase or activity		Objectives	Scope	Require-ments sub-clause	Inputs	Outputs
Figure 2 box number	Title					
10.1	E/E/PE system design requirements specification	To specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements (see 7.10.2 of IEC 61508-1)	E/E/PE safety-related system	7.2.2	E/E/PE system safety requirements specification (see IEC 61508-1, 7.10)	E/E/PE system design requirements specification, describing the equipment and architectures for the E/E/PE system
10.2	E/E/PE system safety validation planning	To plan the validation of the safety of the E/E/PE safety-related system	E/E/PE safety-related system	7.3.2	E/E/PE system safety requirements specification and E/E/PE system design requirements specification	Plan for the safety validation of the E/E/PE safety-related systems
10.3	E/E/PE system design & development including ASICs & software (see Figure 3 & also IEC 61508-3)	To design and develop the E/E/PE safety-related system (including ASICs if appropriate) to meet the E/E/PE system design requirements specification (with respect to the safety functions requirements and the safety integrity requirements (see 7.2))	E/E/PE safety-related system	7.4.2 to 7.4.11	E/E/PE system design requirements specification	Design of the E/E/PE safety related systems in conformance with the E/E/PE system design requirements specification Plan for the E/E/PE system integration test PE system architectural information as an input to the software requirements specification
10.4	E/E/PE system integration	To integrate and test the E/E/PE safety-related system	E/E/PE safety-related system	7.5.2	E/E/PE system design E/E/PE system integration test plan Programmable electronics hardware and software	Fully functioning E/E/PE safety-related systems in conformance with the E/E/PE system design Results of E/E/PE system integration tests
10.5	E/E/PE system installation, commissioning, operation and maintenance procedures	To develop procedures to ensure that the required functional safety of the E/E/PE safety-related system is maintained during operation and maintenance	E/E/PE safety-related system EUC	7.6.2	E/E/PE system design requirements specification E/E/PE system design	E/E/PE system installation, commissioning, operation and maintenance procedures for each individual E/E/PE system
10.6	E/E/PE system safety validation	To validate that the E/E/PE safety-related system meets, in all respects, the requirements for safety in terms of the required safety functions and safety integrity	E/E/PE safety-related system	7.7.2	E/E/PE system safety requirements specification and E/E/PE system design requirements specification Plan for the safety validation of the E/E/PE safety-related systems	Fully safety validated E/E/PE safety-related systems Results of E/E/PE system safety validation

Table 1 *(continued)*

Safety lifecycle phase or activity		Objectives	Scope	Require-ments sub-clause	Inputs	Outputs
Figure 2 box number	Title					
–	E/E/PE system modification	To make corrections, enhancements or adaptations to the E/E/PE safety-related system, ensuring that the required safety integrity is achieved and maintained	E/E/PE safety-related system	7.8.2	E/E/PE system design requirements specification	Results of E/E/PE system modification
–	E/E/PE system verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	E/E/PE safety-related system	7.9.2	As above – depends on the phase Plan for the verification of the E/E/PE safety-related systems for each phase	As above – depends on the phase Results of the verification of the E/E/PE safety-related systems for each phase
–	E/E/PE system functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related system	E/E/PE safety-related system	8	Plan for E/E/PE system functional safety assessment	Results of E/E/PE system functional safety assessment

7.2 E/E/PE system design requirements specification

NOTE This phase is Box 10.1 of Figure 2.

7.2.1 Objective

The objective of the requirements of this subclause is to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

NOTE The E/E/PE system design requirements specification is normally derived from the E/E/PE system safety requirements specification by decomposing the safety functions and allocating parts of the safety function to subsystems (for example groups of sensors, logic solvers or actuators). The requirements for the subsystems may be included in the E/E/PE system design requirements specification or may be separate and referenced from the E/E/PE system design requirements specification. Subsystems may be further decomposed into elements and architectures to satisfy the design and development requirements of 7.4. The requirements for these elements may be included in the requirements for the subsystems or may be separate and referenced from the subsystem requirements.

7.2.2 General

7.2.2.1 The specification of the E/E/PE system design requirements shall be derived from the E/E/PE system safety requirements, specified in 7.10 of IEC 61508-1.

NOTE Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this is allowed in the standard, it may lead to greater complexity and increase the difficulty in carrying out E/E/PE safety lifecycle activities (for example design, validation, functional safety assessment and maintenance). See also 7.4.2.3.

7.2.2.2 The specification of the E/E/PE system design requirements shall be expressed and structured in such a way that they are:

a) clear, precise, unambiguous, verifiable, testable, maintainable and feasible;

b) written to aid comprehension by those who are likely to utilise the information at any phase of the E/E/PE safety lifecycle; and

c) traceable to the E/E/PE system safety requirements specification.

7.2.3 E/E/PE system design requirements specification

7.2.3.1 The specification of the E/E/PE system design requirements shall contain design requirements relating to safety functions (see 7.2.3.2) and design requirements relating to safety integrity (see 7.2.3.3).

7.2.3.2 The specification of the E/E/PE system design requirements shall contain details of all the hardware and software necessary to implement the required safety functions, as specified by the E/E/PE system safety functions requirements specification (see 7.10.2.6 of IEC 61508-1). The specification shall include, for each safety function:

a) requirements for the subsystems and requirements for their hardware and software elements as appropriate;

b) requirements for the integration of the subsystems and their hardware and software elements to meet the E/E/PE system safety functions requirements specification;

c) throughput performance that enables response time requirements to be met;

d) accuracy and stability requirements for measurements and controls;

e) E/E/PE safety-related system and operator interfaces;

f) interfaces between the E/E/PE safety-related systems and any other systems (either within, or outside, the EUC);

g) all modes of behaviour of the E/E/PE safety-related systems, in particular, failure behaviour and the required response (for example alarms, automatic shut-down) of the E/E/PE safety-related systems;

h) the significance of all hardware/software interactions and, where relevant, any required constraints between the hardware and the software;

NOTE Where these interactions are not known before finishing the design, only general constraints can be stated.

i) any limiting and constraint conditions for the E/E/PE safety-related systems and their associated elements, for example timing constraints or constraints due to the possibility of common cause failures;

j) any specific requirements related to the procedures for starting-up and restarting the E/E/PE safety-related systems.

7.2.3.3 The specification of the E/E/PE system design requirements shall contain details, relevant to the design, to achieve the safety integrity level and the required target failure measure for the safety function, as specified by the E/E/PE system safety integrity requirements specification (see 7.10.2.7 of IEC 61508-1), including:

a) the architecture of each subsystem required to meet the architectural constraints on the hardware safety integrity (see 7.4.4);

b) all relevant reliability modelling parameters such as the required proof testing frequency of all hardware elements necessary to achieve the target failure measure;

NOTE 1 Information on the specific application cannot be understated (see 7.10.2.1 of IEC 61508-1). 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.

c) the actions taken in the event of a dangerous failure being detected by diagnostics;

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

e) the capabilities of equipment used to meet the extremes of all environmental conditions (e.g. temperature, humidity, mechanical, electrical) that are specified as required during the E/E/PE system safety lifecycle including manufacture, storage, transport, testing, installation, commissioning, operation and maintenance;

f) the electromagnetic immunity levels that are required (see IEC/TS 61000-1-2: 2008);

NOTE 2 The required immunity levels may vary for different elements of the safety-related system, depending on physical location and power supply arrangements.

NOTE 3 Guidance may be found in EMC product standards, but it is important to recognise that higher immunity levels, or additional immunity requirements, than those specified in such standards may be necessary for particular locations or when the equipment is intended for use in harsher, or different, electromagnetic environments.

g) the quality assurance/quality control measures necessary to safety management (see 6.2.5 of IEC 61508-1);

7.2.3.4 The E/E/PE system design requirements specification shall be completed in detail as the design progresses and updated as necessary after modification.

7.2.3.5 For the avoidance of mistakes during the development of the specification for the E/E/PE system design requirements, an appropriate group of techniques and measures according to Table B.1 shall be used.

7.2.3.6 The implications imposed on the architecture by the E/E/PE system design requirements shall be considered.

NOTE This should include the consideration of the simplicity of the implementation to achieve the required safety integrity level (including architectural considerations and apportionment of functionality to configuration data or to the embedded system).

7.3 E/E/PE system safety validation planning

NOTE This phase is Box 10.2 of Figure 2. It will normally be carried out in parallel with E/E/PE system design and development (see 7.4).

7.3.1 Objective

The objective of the requirements of this subclause is to plan the validation of the safety of the E/E/PE safety-related system.

7.3.2 Requirements

7.3.2.1 Planning shall be carried out to specify the steps (both procedural and technical) that are to be used to demonstrate that the E/E/PE safety-related system satisfies the E/E/PE system safety requirements specification (see 7.10 of IEC 61508-1) and the E/E/PE system design requirements specification (see 7.2).

7.3.2.2 Planning for the validation of the E/E/PE safety-related system shall consider the following:

a) all of the requirements defined in the E/E/PE system safety requirements specification and the E/E/PE system design requirements specification;

b) the procedures to be applied to validate that each safety function is correctly implemented, and the pass/fail criteria for accomplishing the tests;

c) the procedures to be applied to validate that each safety function is of the required safety integrity, and the pass/fail criteria for accomplishing the tests;

d) the required environment in which the testing is to take place including all necessary tools and equipment (also plan which tools and equipment should be calibrated);

e) test evaluation procedures (with justifications);

f) the test procedures and performance criteria to be applied to validate the specified electromagnetic immunity limits;

NOTE Guidance on the specification of electromagnetic immunity tests for elements of safety-related systems is given in IEC/TS 61000-1-2.

g) policies for resolving validation failure.

7.4 E/E/PE system design and development

NOTE This phase is Box 10.3 of Figure 2. It will normally be carried out in parallel with E/E/PE system safety validation planning (see 7.3).

7.4.1 Objective

The objective of the requirements of this subclause is to design and develop the E/E/PE safety-related system (including ASICs if appropriate, see IEC 61508-4, 3.2.15) to meet the E/E/PE system design requirements specification (with respect to the safety functions requirements and the safety integrity requirements (see 7.2).

7.4.2 General requirements

7.4.2.1 The design of the E/E/PE safety-related system shall be created in accordance with the E/E/PE system design requirements specification (see 7.2.3), taking into account all the requirements of 7.2.3.

7.4.2.2 The design of the E/E/PE safety-related system (including the overall hardware and software architecture, sensors, actuators, programmable electronics, ASICs, embedded software, application software, data etc.), shall meet all of the requirements a) to e) as follows:

a) the requirements for hardware safety integrity comprising;
   - the architectural constraints on hardware safety integrity (see 7.4.4), and
   - the requirements for quantifying the effect of random failures (see 7.4.5);

b) the special architecture requirements for ICs with on-chip redundancy (see Annex E), where relevant, unless justification can be given that the same level of independence between different channels is achieved by applying a different set of measures;

c) the requirements for systematic safety integrity (systematic capability), which can be met by achieving one of the following compliance routes:
   - Route 1_S: compliance with the requirements for the avoidance of systematic faults (see 7.4.6 and IEC 61508-3) and the requirements for the control of systematic faults (see 7.4.7 and IEC 61508-3), or
   - Route 2_S: compliance with the requirements for evidence that the equipment is proven in use (see 7.4.10), or
   - Route 3_S (pre-existing software elements only): compliance with the requirements of IEC 61508-3, 7.4.2.12;

     NOTE The “S” subscript in the above routes designates systematic safety integrity to distinguish it from Route 1_H, and Route 2_H for hardware safety integrity.

d) the requirements for system behaviour on detection of a fault (see 7.4.8);

e) the requirements for data communication processes (see 7.4.11).

7.4.2.3 Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not cause a dangerous failure of the safety-related functions).

NOTE 1 Sufficient independence of implementation is established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

NOTE 2 Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this is allowed in the standard, it may lead to greater complexity and increase the difficulty in carrying out E/E/PE system safety lifecycle activities (for example design, validation, functional safety assessment and maintenance).

7.4.2.4 The requirements for hardware and software shall be determined by the safety integrity level of the safety function having the highest safety integrity level unless it can be shown that the implementation of the safety functions of the different safety integrity levels is sufficiently independent.

NOTE 1 Sufficient independence of implementation is established by showing that the probability of a dependent failure between the parts implementing safety functions of different integrity levels is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

NOTE 2 Where several safety functions are implemented in an E/E/PE safety-related system then it will be necessary to consider the possibility that a single fault could cause a failure of several safety functions. In such a situation, it may be appropriate to determine the requirements for hardware and software on the basis of a higher safety integrity level than is associated with any one of the safety functions, depending on the risk associated with such a failure.

7.4.2.5 When independence between safety functions is required (see 7.4.2.3 and 7.4.2.4) then the following shall be documented during the design:

a) the method of achieving independence;

b) the justification of the method.

EXAMPLE Addressing foreseeable failure modes, that may undermine independence, and their failure rates, use of FMECA or dependant failure analysis.

7.4.2.6 The requirements for safety-related software (see IEC 61508-3) shall be made available to the developer of the E/E/PE safety-related system.

7.4.2.7 The developer of the E/E/PE safety-related system shall review the requirements for safety-related software and hardware to ensure that they are adequately specified. In particular, the E/E/PE system developer shall consider the following:

a) safety functions;

b) E/E/PE safety-related system safety integrity requirements;

c) equipment and operator interfaces.

7.4.2.8 The E/E/PE safety-related system design documentation shall specify those techniques and measures necessary during the E/E/PE system safety lifecycle phases to achieve the safety integrity level.

7.4.2.9 The E/E/PE safety-related system design documentation shall justify the techniques and measures chosen to form an integrated set that satisfies the required safety integrity level.

NOTE The adoption of an overall approach employing independent type approval of the E/E/PE safety-related systems (including sensors, actuators, etc) for hardware and software, diagnostic tests and programming tools, and using appropriate languages for software wherever possible, has the potential to reduce the complexity of E/E/PE system application engineering.

7.4.2.10 During the design and development activities, the significance (where relevant) of all hardware and software interactions shall be identified, evaluated and documented.

7.4.2.11 The design shall be based on a decomposition into subsystems with each subsystem having a specified design and set of integration tests (see 7.5.2).

NOTE 1 A subsystem may be considered to comprise a single element or any group of elements. See IEC 61508-4 for definitions. A complete E/E/PE safety-related system is made up from a number of identifiable and separate subsystems, which when put together implement the safety function under consideration. A subsystem can have more than one channel (see 7.4.9.3 and 7.4.9.4).

NOTE 2 Wherever practicable, existing verified subsystems should be used in the implementation. This statement is generally valid only if there is almost 100 % mapping of the existing subsystem or element functionality, capacity and performance on to the new requirement or the verified subsystem or element is structured in such a way that the user is able to select only the functions, capacity or performance required for the specific application. Excessive functionality, capacity or performance can be detrimental to system safety if the existing subsystem or element is overly complicated or has unused features and if protection against unintended functions cannot be obtained.

7.4.2.12 When the initial design of the E/E/PE safety-related system has been completed, an analysis shall be undertaken to determine whether any reasonably foreseeable failure of the E/E/PE safety-related system could cause a hazardous situation or place a demand on any

other risk control measure. If any reasonably foreseeable failure could have either of these effects, then the first priority shall be to change the design of the E/E/PE safety-related system to avoid such failure modes. If this cannot be done, then measures shall be taken to reduce the likelihood of such failure modes to a level commensurate with the target failure measure. These measures shall be subject to the requirements of this standard.

NOTE The intention of this clause is to identify failure modes of the E/E/PE safety-related system that place a demand on other risk control measures. There may be cases where the failure rate of the specified failure modes cannot be reduced and either a new safety function will be required or the SIL of the other safety functions reconsidered taking into account the failure rate.

7.4.2.13 De-rating (see IEC 61508-7) should be considered for all hardware components. Justification for operating any hardware elements at their limits shall be documented (see IEC 61508-1, Clause 5).

NOTE Where de-rating is appropriate, a de-rating factor of approximately two-thirds is typical.

7.4.2.14 Where the design of an E/E/PE safety-related system includes one or more ASICs to implement a safety function, an ASIC development lifecycle (see 7.1.3.1) shall be used.

7.4.3 Synthesis of elements to achieve the required systematic capability

7.4.3.1 To meet the requirements for systematic safety integrity, the designated safety-related E/E/PE system may, in the circumstances described in this section, be partitioned into elements of different systematic capability.

NOTE 1 The systematic capability of an element determines the potential for systematic faults of that element to lead to a failure of the safety function. The concept of systematic capability of an element is applicable to both hardware and software elements.

NOTE 2 Subclause 7.6.2.7 of IEC 61508-1 recognises the value of independence and diversity at the level of a safety function and the E/E/PE safety related systems to which it could be allocated. These concepts can also be applied at the detailed design level where an assembly of elements implementing a safety function can potentially achieve a better systematic performance than the individual elements.

7.4.3.2 For an element of systematic capability SC N (N=1, 2, 3), where a systematic fault of that element does not cause a failure of the specified safety function but does so only in combination with a second systematic fault of another element of systematic capability SC N, the systematic capability of the combination of the two elements can be treated as having a systematic capability of SC (N + 1) providing that sufficient independence exists between the two elements (see 7.4.3.4).

NOTE The independence of elements can be assessed only when the specific application of the elements is known in relation to the defined safety functions.

7.4.3.3 The systematic capability that can be claimed for a combination of elements each of systematic capability SC N can at most be SC (N+1). A SC N element may be used in this way only once. It is not permitted to achieve SC (N+2) and higher by successively building assemblies of SC N elements.

7.4.3.4 Sufficient independence, in the design between elements and in the application of elements, shall be justified by common cause failure analysis to show that the likelihood of interference between elements and between the elements and the environment is sufficiently low in comparison with the safety integrity level of the safety function under consideration.

NOTE 1 For systematic capability, with respect to hardware design, realisation, operation and maintenance, possible approaches to the achievement of sufficient independence include:

– functional diversity: use of different approaches to achieve the same results;

– diverse technologies: use of different types of equipment to achieve the same results);

– common parts/services: ensuring that there are no common parts or services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;

– common procedures: ensuring that there are no common operational, maintenance or test procedures.

NOTE 2 Independence of application means that elements will not adversely interfere with each other's execution behaviour such that a dangerous failure would occur.

NOTE 3 For independence of software elements see 7.4.2.8 and 7.4.2.9 of IEC 61508-3.

7.4.4 Hardware safety integrity architectural constraints

NOTE 1 The equation, relating to the hardware safety integrity constraints, are specified in Annex C and the safety integrity constraints are summarized in Table 2 and Table 3

NOTE 2 Clause A.2 of IEC 61508-6 gives an overview of the necessary steps in achieving required hardware safety integrity, and shows how this subclause relates to other requirements of this standard.

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing one of two possible routes (to be implemented at system or subsystem level):

– Route 1_H based on hardware fault tolerance and safe failure fraction concepts; or,
– Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

Application standards based on the IEC 61508 series may indicate the preferred Route (i.e. Route 1_H or Route 2_H).

NOTE 3 The "H" subscript in the above routes designates hardware safety integrity to distinguish it from Route 1_S , Route 2_S and Route 3_S for systematic safety integrity.

7.4.4.1 General requirements

7.4.4.1.1 With respect to the hardware fault tolerance requirements

a) a hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function (for further clarification see Note 1 and Table 2 and Table 3). In determining the hardware fault tolerance no account shall be taken of other measures that may control the effects of faults such as diagnostics; and
b) where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault;
c) when determining the hardware fault tolerance achieved, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented (see Note 2).

NOTE 1 The constraints on hardware safety integrity have been included in order to achieve a sufficiently robust architecture, taking into account the level of element and subsystem complexity (see 7.4.4.1.1 and 7.4.4.1.2). The highest allowable safety integrity level for the safety function implemented by the E/E/PE safety-related system, derived through applying these requirements, is the maximum that is permitted to be claimed for the safety function even though, in some cases reliability calculations show that a higher safety integrity level could be achieved. It should also be noted that even if the hardware fault tolerance is achieved for all subsystems, a reliability calculation will still be necessary to demonstrate that the specified target failure measure has been achieved and this may require that the hardware fault tolerance be increased to meet design requirements.

NOTE 2 The hardware fault tolerance requirements apply to the subsystem architecture that is used under normal operating conditions. The hardware fault tolerance requirements may be relaxed while the E/E/PE safety-related system is being repaired on-line. However, the key parameters relating to any relaxation should have been previously evaluated (for example MTTR compared to the probability of a demand).

NOTE 3 Certain faults may be excluded because if an element clearly has a very low probability of failure by virtue of properties inherent to its design and construction (for example, a mechanical actuator linkage), then it would not normally be considered necessary to constrain (on the basis of hardware fault tolerance) the safety integrity of any safety function that uses the element.

NOTE 4 The choice of the route is application and sector dependent and the following should be considered when selecting the Route:

– a safe failure of one function may create a new hazard or be an additional cause for an existing hazard;
– redundancy may not be practicable for all functions;

– repair is not always possible or rapid (e.g. not feasible within a time that is negligible compared to the proof test interval).

NOTE 5 Special architecture requirements for ICs with on-chip redundancy are given in Annex E.

7.4.4.1.2 An element can be regarded as type A if, for the components required to achieve the safety function

a) the failure modes of all constituent components are well defined; and

b) the behaviour of the element under fault conditions can be completely determined; and

c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.9.3 to 7.4.9.5).

7.4.4.1.3 An element shall be regarded as type B if, for the components required to achieve the safety function,

a) the failure mode of at least one constituent component is not well defined; or

b) the behaviour of the element under fault conditions cannot be completely determined; or

c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.9.3 to 7.4.9.5).

NOTE This means that if at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.

7.4.4.1.4 When estimating the safe failure fraction of an element, intended to be used in a subsystem having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if:

– the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or,

– when operating in high demand mode of operation, the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.

7.4.4.1.5 When estimating the safe failure fraction of an element which,

– has a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation; or,

– is implementing a safety function, or part of a safety function, operating in low demand mode of operation,

credit shall only be taken for the diagnostics if the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

7.4.4.2 Route 1_H

7.4.4.2.1 To determine the maximum safety integrity level that can be claimed, with respect to a specified safety function, the following procedure shall be followed:

1) Define the subsystems making up the E/E/PE safety-related system.

2) For each subsystem determine the safe failure fraction for all elements in the subsystem separately (i.e. on an individual element basis with each element having a hardware fault tolerance of 0). In the case of redundant element configurations, the SFF may be calculated by taking into consideration the additional diagnostics that may be available (e.g. by comparison of redundant elements).

3) For each element, use the achieved safe failure fraction and hardware fault tolerance of 0 to determine the maximum safety integrity level that can be claimed from column 2 of Table 2 (for Type A elements) and column 2 of Table 3 (for Type B elements).

4) Use the method in 7.4.4.2.3 and 7.4.4.2.4 for determining the maximum safety integrity level that can be claimed for the subsystem.

5) The maximum safety integrity level that can be claimed for an E/E/PE safety-related system shall be determined by the subsystem that has achieved the lowest safety integrity level.

7.4.4.2.2 For application to subsystems comprising elements that meet the specific requirements detailed below, as an alternative to applying the requirements of 7.4.4.2.1 2) to 7.4.4.2.1 4), the following is applicable:

1) the subsystem is comprised of more than one element; and

2) the elements are of the same type; and

3) all the elements have achieved safe failure fractions that are in the same range (see Note 1 below) specified in Tables 2 or 3;then the following procedure may be followed,

   a) determine the safe failure fraction of all individual elements. In the case of redundant element configurations, the SFF may be calculated by taking into consideration the additional diagnostics that may be available (e.g. by comparison of redundant elements);

   b) determine the hardware fault tolerance of the subsystem;

   c) determine the maximum safety integrity level that can be claimed for the subsystem if the elements are type A from Table 2;

   d) determine the maximum safety integrity level that can be claimed for the subsystem if the elements are type B from Table 3.

NOTE 1 The range indicated in 3) above refers to Tables 2 and 3 where the safe failure fraction is classified into one of four ranges (i.e. (<60 %); (60 % to <90 %); (90% to <99 %) and (≥99 %)). All SFFs would need to be in the same range (e.g. all in the range (90 % to <99 %)).

EXAMPLE 1 To determine the maximum allowable safety integrity level that has been achieved, for the specified safety function, by a subsystem having a hardware fault tolerance of 1, where an element safety function is implemented through parallel elements, the following approach may be adopted providing the subsystem meets the requirements of 7.4.4.2.2. In this example, all the elements are type B and the safe failure fractions of the elements are in the (90 % to < 99 %) range.

From Table 3, it can be seen by inspection, that for a hardware fault tolerance equal to 1, with safe failure fractions of both elements in the (90 % to <99 %) range, the maximum allowable safety integrity level for the specified safety function is SIL 3.

EXAMPLE 2 To determine the required hardware fault tolerance for a subsystem, for the specified safety function, where an element safety function is implemented through parallel elements, the following approach may be adopted providing the subsystem meets the requirements of 7.4.4.2.2. In this example, all the elements are type A and the safe failure fractions of the elements are in the (60 % to <90 % range). The safety integrity level of the safety function is SIL 3.

From Table 2, it can be seen by inspection, that to meet the requirement of SIL 3, the required hardware fault tolerance needs to equal 1. This means that two elements in parallel are necessary.

Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 This table, in association with 7.4.4.2.1 and 7.4.4.2.2, is used for the determination of the maximum SIL that can be claimed for a subsystem: given the fault tolerance of the subsystem and the SFF to the elements used.

i. For general application to any subsystem see 7.4.4.2.1.

ii. For application to subsystems comprising elements that meet the specific requirements of 7.4.4.2.2. To claim that a subsystem meets a specified SIL directly from this table it will be necessary to meet all the requirements in 7.4.4.2.2.

NOTE 2 The table, in association with 7.4.4.2.1 and 7.4.4.2.2,can also be used:

i. For the determination of the hardware fault tolerance requirements for a subsystem given the required SIL of the safety function and the SFFs of the elements to be used.

ii. For the determination of the SFF requirements for elements given the required SIL of the safety function and the hardware fault tolerance of the subsystem.

NOTE 3 The requirements in 7.4.4.2.3 and 7.4.4.2.4 are based on the data specified in this table and Table 3.

NOTE 4 See Annex C for details of how to calculate safe failure fraction.

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 This table, in association with 7.4.4.2.1 and 7.4.4.2.2, is used for the determination of the maximum SIL that can be claimed for a subsystem given the fault tolerance of the subsystem and the SFF to the elements used.

i. For general application to any subsystem see 7.4.4.2.1.

ii. For application to subsystems comprising elements that meet the specific requirements of 7.4.4.2.2. To claim that a subsystem meets a specified SIL directly from this table it will be necessary to meet all the requirements in 7.4.4.2.2.

NOTE 2 The table, in association with 7.4.4.2.1 and 7.4.4.2.2,can also be used:

i. For the determination of the hardware fault tolerance requirements for a subsystem given the required SIL of the safety function and the SFFs of the elements to be used.

ii. For the determination of the SFF requirements for elements given the required SIL of the safety function and the hardware fault tolerance of the subsystem.

NOTE 3 The requirements in 7.4.4.2.3 and 7.4.4.2.4 are based on the data specified in this table and Table 2.

NOTE 4 See Annex C for details of how to calculate safe failure fraction.

NOTE 5 When using 7.4.4.2.1 for the combination of type B elements, with a hardware fault tolerance of 1, in which both elements have a safe failure fraction of less than 60 %, the maximum allowable safety integrity level for a safety function carried out by the combination is SIL 1.

7.4.4.2.3 In an E/E/PE safety-related subsystem where a number of element safety functions are implemented through a serial combination of elements (such as in Figure 5), the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by the element that has achieved the lowest safety integrity level for the achieved safe failure fraction for a hardware fault tolerance of 0. To illustrate the method, assume an architecture as indicated in Figure 5 and see example below.

EXAMPLE (see Figure 5): Assume an architecture where a number of element safety functions are performed by a subsystem comprising a single channel of elements 1, 2 and 3 and the elements meet the requirements of Tables 2 and 3 as follows:

– Element 1 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1;

– Element 2 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;

– Element 3 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1;

– Both element 1 and element 3 restrict the maximum SIL that can be claimed, for the achieved hardware fault tolerance and safe failure fraction to just SIL 1.

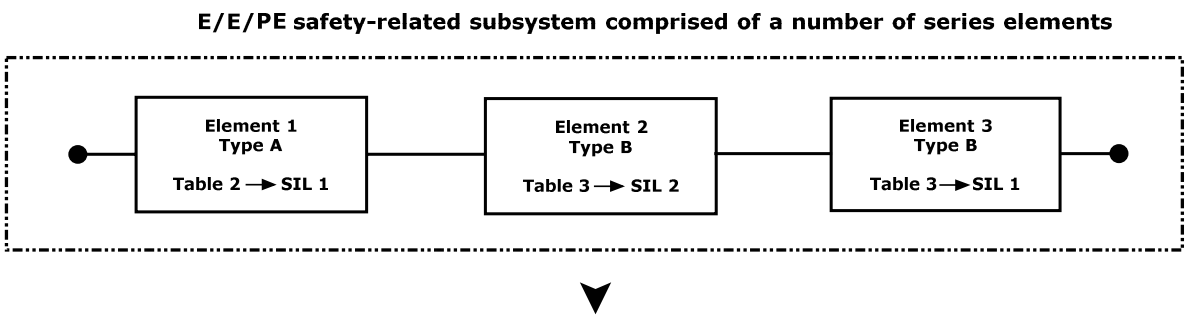


Figure 5 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements, see 7.4.4.2.3)

7.4.4.2.4 In an E/E/PE safety-related subsystem where an element safety function is implemented through a number of channels (combination of parallel elements) having a hardware fault tolerance of N, the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by:

a) grouping the serial combination of elements for each channel and then determining the maximum safety integrity level that can be claimed for the safety function under consideration for each channel (see 7.4.4.2.3); and

b) selecting the channel with the highest safety integrity level that has been achieved for the safety function under consideration and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of the subsystem.

To illustrate the method, assume architecture as indicated in Figure 6 and see example below.

NOTE 1 N is the hardware fault tolerance of the combination of parallel elements (see 7.4.4.1.1).

NOTE 2 See example below regarding the application of this subclause.

EXAMPLE The grouping and analysis of these combinations may be carried out in various ways. To illustrate one possible method, assume an architecture in which a particular safety function is performed by two subsystems, X and Y, where subsystem X consists of elements 1, 2, 3 and 4, and subsystem Y consists of a single element 5, as shown in Figure 6. The use of parallel channels in subsystem X ensures that elements 1 and 2 implement the part of the safety function required of subsystem X independently from elements 3 and 4, and vice-versa. The safety function will be performed:

– in the event of a fault in either element 1 or element 2 (because the combination of elements 3 and 4 is able to perform the required part of the safety function); or

– in the event of a fault in either element 3 or element 4 (because the combination of elements 1 and 2 is able to perform the required part of the safety function).

The determination of the maximum safety integrity level that can be claimed, for the safety function under consideration, is detailed in the following steps.

For subsystem X, in respect of the specified safety function under consideration, each element meets the requirements of Tables 2 and 3 as follows:

– Element 1 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 3;

– Element 2 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;

– Element 3 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2;

– Element 4 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 1.

Elements are combined to give a maximum hardware safety integrity level for the safety function under consideration, for subsystem X as follows:

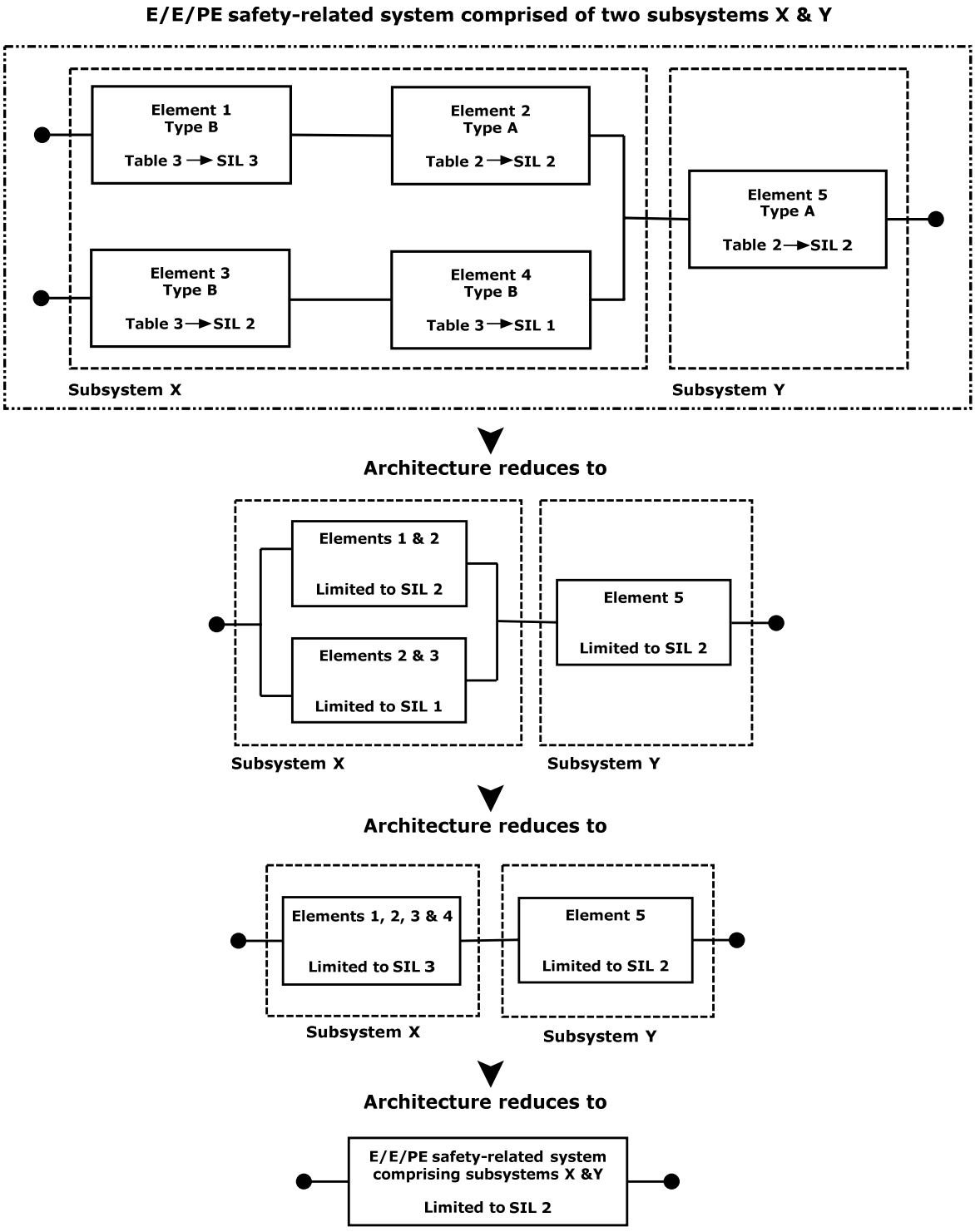
a) Combining elements 1 and 2: The hardware fault tolerance and safe failure fraction achieved by the combination of elements 1 and 2 (each separately meeting the requirements for SIL 3 and SIL 2 respectively) meets the requirements of SIL 2 (determined by element 2; see 7.4.4.2.3);

b) Combining elements 3 and 4: The hardware fault tolerance and safe failure fraction achieved by the combination of elements 3 and 4 (each separately meeting the requirements for SIL 2 and SIL 1 respectively) meets the requirements of SIL 1 (determined by element 4 see 7.4.4.2.3);

c) Further combining the combination of elements 1 and 2 with the combination of elements 3 and 4: the maximum safety integrity level that can be claimed for the safety function under consideration is determined by selecting the channel with the highest safety integrity level that has been achieved and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of elements. In this case the subsystem comprises two parallel channels with a hardware fault tolerance of 1. The channel with the highest safety integrity level, for the safety function under consideration was that comprising elements 1 and 2 which achieved the requirements for SIL 2. Therefore, the maximum safety integrity level for the subsystem for a hardware fault tolerance of 1 is (SIL 2 + 1) = SIL 3 (see 7.4.4.2.4).

For subsystem Y, element 5 achieves the requirements, for a hardware fault tolerance of 0 and, for a specific safe failure fraction, for SIL 2.

For the complete E/E/PE safety-related system (comprising two subsystems X and Y that have achieved the requirements, for the safety function under consideration, of SIL 3 and SIL 2 respectively), the maximum safety integrity level that can be claimed for an E/E/PE safety-related system is determined by the subsystem that has achieved the lowest safety integrity level (7.4.4.2.1 5)). Therefore, for this example, the maximum safety integrity level, that can be claimed for the E/E/PE safety-related system, for the safety function under consideration, is SIL 2.



NOTE 1 Elements 1 and 2 implement the part of the safety function required of subsystem X independently from elements 3 and 4, and vice versa.

NOTE 2 The subsystems implementing the safety function will be across the entire E/E/PE safety-related system in terms of ranging from the sensors to the actuators.

Figure 6 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprised of two subsystems X & Y, see 7.4.4.2.4)

7.4.4.3 Route 2_H

7.4.4.3.1 The minimum hardware fault tolerance for each subsystem of an E/E/PE safety-related system implementing a safety function of a specified safety integrity level shall be as follows:

NOTE In the following clauses, unless otherwise specified, the safety function may be operating in either a low demand mode of operation or a high demand or continuous mode of operation.

a) a hardware fault tolerance of 2 for a specified safety function of SIL 4 unless the conditions in 7.4.4.3.2 apply.

b) a hardware fault tolerance of 1 for a specified safety function of SIL 3 unless the conditions in 7.4.4.3.2 apply.

c) a hardware fault tolerance of 1 for a specified safety function of SIL 2, operating in a high demand or continuous mode of operation, unless the conditions in 7.4.4.3.2 apply.

d) a hardware fault tolerance of 0 for a specified safety function of SIL 2 operating in a low demand mode of operation.

e) a hardware fault tolerance of 0 for a specified safety function of SIL 1.

7.4.4.3.2 For type A elements only, if it is determined that by following the HFT requirements specified in 7.4.4.3.1, for the situation where an HFT greater than 0 is required, it would introduce additional failures and lead to a decrease in the overall safety of the EUC, then a safer alternative architecture with reduced HFT may be implemented. In such a case this shall be justified and documented. The justification shall provide evidence that:

a) compliance with the HFT requirements specified in 7.4.4.3.1 would introduce additional failures and lead to a decrease in the overall safety of the EUC; and

b) if the HFT is reduced to zero, the failure modes, identified in the element performing the safety function, can be excluded because the dangerous failure rate(s) of the identified failure mode(s) are very low compared to the target failure measure for the safety function under consideration (see 7.4.4.1.1 c)). That is, the sum of the dangerous failure frequencies of all serial elements, on which fault exclusion is being claimed, should not exceed 1 % of the target failure measure. Furthermore the applicability of fault exclusions shall be justified considering the potential for systematic faults

NOTE Fault tolerance is the preferred solution to achieve the required confidence that a robust architecture has been achieved. When 7.4.4.3.2 applies, the purpose of the justification is to demonstrate that the proposed alternative architecture provides an equivalent or better solution. This may depend on the technical field and/or the application. Examples include: back-up arrangements (e.g., analytical redundancy, replacing a failed sensor output by physical calculation results from other sensors outputs); using more reliable items of the same technology (if available); changing for a more reliable technology; decreasing common cause failure impact by using diversified technology; increasing the design margins; constraining the environmental conditions (e.g. for electronic components); decreasing the reliability uncertainty by gathering more field feedback or expert judgement.

7.4.4.3.3 If Route 2_H is selected, then the reliability data used when quantifying the effect of random hardware failures (see 7.4.5) shall be:

a) based on field feedback for elements in use in a similar application and environment; and,

b) based on data collected in accordance with international standards (e.g., IEC 60300-3-2 or ISO 14224:); and,

c) evaluated according to:

   i) the amount of field feedback; and,

   ii) the exercise of expert judgement; and where needed,

   iii) the undertaking of specific tests;

in order to estimate the average and the uncertainty level (e.g., the 90 % confidence interval or the probability distribution (see Note 2)) of each reliability parameter (e.g., failure rate) used in the calculations.

NOTE 1 End-users are encouraged to organize relevant component reliability data collections as described in published standards.

NOTE 2 The 90 % confidence interval of a failure rate λ is the interval [$\lambda_{5\ \%}$, $\lambda_{95\ \%}$] in which its actual value has a probability of 90 % to belong to. λ has a probability of 5 % to be better than $\lambda_{5\ \%}$ and worse than $\lambda_{95\ \%}$. On a pure statistical basis, the average of the failure rate may be estimated by using the "maximum likelihood estimate" and the confidence bounds ($\lambda_{5\ \%}$, $\lambda_{95\ \%}$) may be calculated by using the χ^2 function. The accuracy depends on the cumulated observation time and the number of failures observed. The Bayesian approach may be used to handle statistical observations, expert judgement and specific test results. This can be used to fit relevant probabilistic distribution functions for further use in Monte Carlo simulation.

If route 2_H is selected, then the reliability data uncertainties shall be taken into account when calculating the target failure measure (i.e. PFD_{avg} or PFH) and the system shall be improved until there is a confidence greater than 90 % that the target failure measure is achieved.

7.4.4.3.4 All type B elements used in Route 2_H shall have, as a minimum, a diagnostic coverage of not less than 60 %.

7.4.5 Requirements for quantifying the effect of random hardware failures

NOTE Clause A.2 of IEC 61508-6, gives an overview of the necessary steps in achieving required hardware safety integrity, and shows how this subclause relates to other requirements of this standard.

7.4.5.1 For each safety function, the achieved safety integrity of the E/E/PE safety-related system due to random hardware failures (including soft-errors) and random failures of data communication processes shall be estimated in accordance with 7.4.5.2 and 7.4.11, and shall be equal to or less than the target failure measure as specified in the E/E/PE system safety requirements specification (see IEC 61508-1, 7.10).

NOTE In order to demonstrate that this has been achieved, it is necessary to carry out a reliability prediction for the relevant safety function using an appropriate technique (see 7.4.5.2) and compare the result to the target failure measure of the relevant safety function (see IEC 61508-1).

7.4.5.2 The estimate of the achieved failure measure for each safety function, as required by 7.4.5.1, shall take into account:

a) the architecture of the E/E/PE safety-related system, in terms of its subsystems, as it relates to each safety function under consideration;

NOTE 1 This involves deciding which failure modes of the elements of the subsystems are in a series configuration (i.e. any failure causes failure of the relevant safety function to be carried out) and which are in a parallel configuration (i.e. coincident failures are necessary for the relevant safety function to fail).

b) the architecture of each subsystem of the E/E/PE safety-related system, in terms of its elements, as it relates to each safety function under consideration;

c) the estimated failure rate of each subsystem and its elements in any modes that would cause a dangerous failure of the E/E/PE safety-related system but are detected by diagnostic tests (see 7.4.9.4 to 7.4.9.5). Justification for the failure rates should be given considering the source of the data and its accuracy or tolerance. This may include consideration and the comparison of data from a number of sources and the selection of failure rates from systems most closely resembling that under consideration. Failure rates used for quantifying the effect of random hardware failures and calculating safe failure fraction or diagnostic coverage shall take into account the specified operating conditions.

NOTE 2 To take into account the operating conditions it will normally be necessary to adjust failure rates from data bases for example due to contact load or temperature.

d) the susceptibility of the E/E/PE safety-related system and its subsystems to common cause failures (see Notes 3 and 4). There shall be a justification of the assumptions made;

NOTE 3 Failures due to common cause effects may result from effects other than actual failures of hardware elements (e.g. electromagnetic interference, decoding errors, etc). However, such failures are considered, for the purposes of this standard, in the quantification of the effect of random hardware failures. Staggering the testing of elements decreases the likelihood of common cause failure.

NOTE 4 In the case of common cause failures being identified between the E/E/PE safety–related systems and demand causes or other protection layers there will need to be confirmation that this has been taken into account when the safety integrity level and target failure measure requirements have been determined. For methods of determining common cause factors see IEC 61508-6, Annex D.

e) the diagnostic coverage of the diagnostic tests (determined according to Annex C), the associated diagnostic test interval and the rate of dangerous unrevealed failure of the diagnostics due to random hardware failures of each subsystem. Where relevant, only those diagnostic tests that meet the requirements of 7.4.5.3 shall be considered. The MTTR and MRT (see 3.6.21 and 3.6.22 of IEC 61508-4), shall be considered in the reliability model.

NOTE 5 When establishing the diagnostic test interval, the intervals between all of the tests that contribute to the diagnostic coverage will need to be considered.

f) the intervals at which proof tests are undertaken to reveal dangerous faults;

g) whether the proof test is likely to be 100 % effective;

NOTE 6 An imperfect proof test will result in a safety function that is not restored to 'as good as new' and therefore the probability of failure will increase. Justification should be given for the assumptions made, in particular, the renewable period of the elements or the effect on the risk reduction over the life of the safety function should be included. It will be necessary to consider the test duration if the item is tested off-line whilst testing is being undertaken.

h) the repair times for detected failures;

NOTE 7 The mean repair time (MRT) is one part of the mean time to restoration (MTTR), (see 3.6.22 and 3.6.21of IEC 61508-4), which will also include the time taken to detect a failure and any time period during which repair is not possible (see Annex B of IEC 61508-6, for an example of how the MTTR and the MRT can be used to calculate the probability of failure). The repair can be considered to be instantaneous only when the EUC is shut-down or in a safe state during repair. For situations where the repair cannot be carried out whilst the EUC is shut down and in a safe state, it is particularly important that full account is taken of the time period when no repair can be carried out, especially when this is relatively large. All relevant factors relating to repairs should be taken into account.

i) the effect of random human error if a person is required to take action to achieve the safety function.

NOTE 8 The random nature of human error should be considered in cases where a person is alerted to an unsafe condition and is required to take action and the probability of human error should be included in the overall calculation.

j) the fact that a number of modelling methods are available and that the most appropriate method is a matter for the analyst and will depend on the circumstances. Available methods include cause consequence analysis (B.6.6.2 of IEC 61508-7;), fault tree analysis (B.6.6.5 of IEC 61508-7;), Markov models (Annex B of IEC 61508-6 and B.6.6.6 of IEC 61508-7), reliability block diagrams (Annex B of IEC 61508-6 and B.6.6.7 of IEC 61508-7;) and Petri nets (Annex B of IEC 61508-6 and B.2.3.3 of IEC 61508-7).

NOTE 9 Annex B of IEC 61508-6 describes a simplified approach that may be used to estimate the average probability of a dangerous failure on demand of a safety function due to random hardware failures in order to determine that an architecture meets the required target failure measure.

NOTE 10 Clause A.2 of IEC 61508-6 gives an overview of the necessary steps in achieving required hardware safety integrity, and shows how this subclause relates to other requirements of this standard.

NOTE 11 It is necessary to quantify separately for each safety function the reliability of the E/E/PE safety-related systems because different element failure modes will apply and the architecture of the E/E/PE safety-related systems (in terms of redundancy) may also vary.

7.4.5.3 When quantifying the effect of random hardware failures of a subsystem, having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if:

– the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or

– in high demand mode of operation the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.

7.4.5.4 The diagnostic test interval of any subsystem:

– having a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation; or

– which is implementing a safety function, or part of a safety function, operating in low demand mode of operation,

shall be such that the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

7.4.5.5 If, for a particular design, the safety integrity requirement for the relevant safety function is not achieved then:

a) determine the elements, subsystems and/or parameters contributing most to the function's calculated failure rate;

b) evaluate the effect of possible improvement measures on the identified critical elements, subsystems or parameters (for example, more reliable components, additional defences against common mode failures, increased diagnostic coverage, increased redundancy, reduced proof test interval, staggering tests, etc);

c) select and implement the applicable improvements;

d) repeat the necessary steps to establish the new probability of a random hardware failure.

7.4.6 Requirements for the avoidance of systematic faults

NOTE See 7.4.2.2 c) for details, when the requirements of this subclause apply.

7.4.6.1 An appropriate group of techniques and measures shall be used that are designed to prevent the introduction of faults during the design and development of the hardware and software of the E/E/PE safety-related system (see Table B.2 and IEC 61508-3).

NOTE This standard does not contain specific requirements relating to the avoidance of systematic faults during the design of mass-produced electronic integrated circuits such as standard microprocessors. This is because the likelihood of faults in such devices is minimised by stringent development procedures, rigorous testing and extensive experience of use with significant feedback from users. For electronic integrated circuits that cannot be justified on such a basis (for example, new devices or ASICs), the requirements for ASICs (see 7.4.6.7 and informative Annex F) will apply if they are to be used in an E/E/PE safety-related system. In case of doubt (about extensive experience of use with significant feedback from users) the requirements for “field experience” from Table B.6 should be taken into account with an effectiveness of “low” for SIL 1 and SIL 2, an effectiveness of “medium” for SIL 3 and an effectiveness of “high” for SIL 4.

7.4.6.2 In accordance with the required safety integrity level the design method chosen shall possess features that facilitate

a) transparency, modularity and other features that control complexity;

b) clear and precise expression of
   – functionality;
   – subsystem and element interfaces;
   – sequencing and time-related information;
   – concurrency and synchronisation;

c) clear and precise documentation and communication of information;

d) verification and validation.

7.4.6.3 Maintenance requirements, to ensure that the safety integrity requirements of the E/E/PE safety-related systems continue to be met, shall be formalised at the design stage.

7.4.6.4 Where applicable, automatic testing tools and integrated development tools shall be used.

7.4.6.5 During the design, E/E/PE system integration tests shall be planned. Documentation of the test planning shall include

a) the types of tests to be performed and procedures to be followed;

b) the test environment, tools, configuration and programs;

c) the pass/fail criteria.

7.4.6.6 During the design, those activities that can be carried out on the developer's premises shall be distinguished from those that require access to the user's site.

7.4.6.7 An appropriate group of techniques and measures shall be used that are essential to prevent the introduction of faults during the design and development of ASICs.

NOTE Techniques and measures that support the achievement of relevant properties are given in informative Annex F. The related ASIC development lifecycle is shown in Figure 3.

7.4.7 Requirements for the control of systematic faults

NOTE See 7.4.2.2 c) for details, when the requirements of this subclause apply.

7.4.7.1 For controlling systematic faults, the E/E/PE system design shall possess design features that make the E/E/PE safety-related systems tolerant against:

a) any residual design faults in the hardware, unless the possibility of hardware design faults can be excluded (see Table A.15);

b) environmental stresses, including electromagnetic disturbances (see Table A.16);

c) mistakes made by the operator of the EUC (see Table A.17);

d) any residual design faults in the software (see 7.4.3 of IEC 61508-3 and associated table);

e) errors and other effects arising from any data communication process (see 7.4.11).

7.4.7.2 Maintainability and testability shall be considered during the design and development activities in order to facilitate implementation of these properties in the final E/E/PE safety-related systems.

7.4.7.3 The design of the E/E/PE safety-related systems shall take into account human capabilities and limitations and be suitable for the actions assigned to operators and maintenance staff. Such design requirements shall follow good human-factor practice and shall accommodate the likely level of training or awareness of operators, for example in mass-produced E/E/PE safety-related systems where the operator is a member of the public.

NOTE 1 The design goal should be that foreseeable critical mistakes made by operators or maintenance staff are prevented or eliminated by design wherever possible, or that the action requires secondary confirmation before completion.

NOTE 2 Some mistakes made by operators or maintenance staff may not be recoverable by E/E/PE safety-related systems, for example if they are not detectable or realistically recoverable except by direct inspection, such as some mechanical failures in the EUC.

7.4.8 Requirements for system behaviour on detection of a fault

NOTE The requirements of this subclause apply to specified safety functions implemented by a single E/E/PE safety-related system where the overall safety function has not been allocated to other risk reduction measures.

7.4.8.1 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem that has a hardware fault tolerance of more than 0 shall result in either:

a) a specified action to achieve or maintain a safe state (see Note); or

b) the isolation of the faulty part of the subsystem to allow continued safe operation of the EUC whilst the faulty part is repaired. If the repair is not completed within the mean repair time (MRT), see 3.6.22 of IEC 61508-4, assumed in the calculation of the probability of random hardware failure (see 7.4.5.2), then a specified action shall take place to achieve or maintain a safe state (see Note).

NOTE The specified action required to achieve or maintain a safe state will be specified in the E/E/PE system safety requirements (see IEC 61508-1, 7.10). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC that relies, for functional safety, on the faulty subsystem.

7.4.8.2 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of 0 shall, in the case that the subsystem is used only by safety function(s) operating in the low demand mode, result in either:

a) a specified action to achieve or maintain a safe state; or

b) the repair of the faulty subsystem within the mean repair time (MRT), see 3.6.22 of IEC 61508-4,assumed in the calculation of the probability of random hardware failure (see 7.4.5.2). During this time the continuing safety of the EUC shall be ensured by additional measures and constraints. The safety integrity provided by these measures and constraints shall be at least equal to the safety integrity provided by the E/E/PE safety-related system in the absence of any faults. The additional measures and constraints shall be specified in the E/E/PE system operation and maintenance procedures (see 7.6).

NOTE The specified action required to achieve or maintain a safe state will be specified in the E/E/PE system safety requirements specification (see 7.10 of IEC 61508-1). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC that relies, for functional safety, on the faulty subsystem.

7.4.8.3 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of 0 shall, in the case of a subsystem that is implementing any safety function(s) operating in the high demand or the continuous mode, result in a specified action to achieve or maintain a safe state (see Note).

NOTE The specified action required to achieve or maintain a safe state will be specified in the E/E/PE system safety requirements (see IEC 61508-1, 7.10). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC that relies, for functional safety, on the faulty subsystem.

7.4.9 Requirements for E/E/PE system implementation

7.4.9.1 The E/E/PE safety-related system shall be implemented according to the E/E/PE system design requirements specification (7.2.3).

7.4.9.2 All subsystems and their elements that are used by one or more safety functions shall be identified and documented as safety-related subsystems and elements.

7.4.9.3 The following information shall be available for each safety-related subsystem and each element as appropriate (see also 7.4.9.4):

NOTE It will be necessary for a supplier of a subsystem or element, claimed as being compliant with IEC 61508, to make this information available to the designer of a safety-related system (or another subsystem or element) in the safety manual for compliant items, see Annex D.

a) a functional specification of the subsystem and its elements as appropriate;

b) any instructions or constraints relating to the application of the subsystem and its elements, that should be observed in order to prevent systematic failures of the subsystem;

c) the systematic capability of each element (see 7.4.2.2 c));

d) identification of the hardware and/or software configuration of the element to enable configuration management of the E/E/PE safety-related system in accordance with 6.2.1 of IEC 61508-1;

e) documentary evidence that the subsystem and its elements have been verified as meeting their specified functional requirements and systematic capabilities in accordance with the E/E/PE design requirements specification (see 7.2.3).

7.4.9.4 The following information shall be available for each safety-related element that is liable to random hardware failure (see also 7.4.9.3 and 7.4.9.5):

NOTE 1 It will be necessary for a supplier of an element, claimed as being compliant with IEC 61508 series, to make this information available to the designer of a safety-related system in the element safety manual, see Annex D.

a) the failure modes of the element (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the safety function and that are not detected by diagnostic tests internal to the element or are not detectable by diagnostics external to the element (see 7.4.9.5);

b) for every failure mode in a), an estimated failure rate with respect to specified operating conditions;

c) the failure modes of the element (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the safety function and that are detected by diagnostic tests internal to the element or are detectable by diagnostics external to the element (see 7.4.9.5);

d) for every failure mode in c), an estimated failure rate with respect to specified operating conditions;

e) any limits on the environment of the element that should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures;

f) any limit on the lifetime of the element that should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures;

g) any periodic proof test and/or maintenance requirements;

h) for every failure mode in c) that is detected by diagnostics internal to the element, the diagnostic coverage derived according to Annex C (see Note 2);

i) for every failure mode in c) that is detected by diagnostics internal to the element, the diagnostic test interval (see Note 2);

NOTE 2 The diagnostic coverage and diagnostic test interval is required to allow credit to be claimed for the action of the diagnostic tests performed in the element in the hardware safety integrity model of the E/E/PE safety-related system (see 7.4.5.2, 7.4.5.3 and 7.4.5.4).

j) the failure rate of the diagnostics, due to random hardware failures;

k) any additional information (for example repair times) that is necessary to allow the derivation of the mean repair time (MRT), see 3.6.22 of IEC 61508-4,following detection of a fault by the diagnostics;

l) all information that is necessary to enable the derivation of the safe failure fraction (SFF) of the element as applied in the E/E/PE safety-related system, determined according to Annex C, including the classification as type A or type B according to 7.4.4;

m) the hardware fault tolerance of the element.

7.4.9.5 The estimated failure rates, due to random hardware failures, for elements (see 7.4.9.4 a) and c)) can be determined either

a) by a failure modes and effects analysis of the design using element failure data from a recognised industry source; or

b) from experience of the previous use of the element in a similar environment (see 7.4.10).

NOTE 1 Any failure rate data used should have a confidence level of at least 70 %. The statistical determination of confidence level is defined in reference [9] of the Bibliography. For an equivalent term: “significance level”, see reference [10].

NOTE 2 If site-specific failure data are available then this is preferred. If this is not the case then generic data may have to be used.

NOTE 3 Although a constant failure rate is assumed by most probabilistic estimation methods this only applies provided that the useful lifetime of elements is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time) the results of most probabilistic calculation methods are therefore meaningless. Thus any probabilistic estimation should include a specification of the elements’ useful lifetimes. The useful lifetime is highly dependent on the element itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive). Experience has shown that the useful lifetime often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

7.4.9.6 Suppliers shall provide a safety manual for compliant items, in accordance with Annex D, for each compliant item that they supply and for which they claim compliance with IEC 61508 series.

7.4.9.7 The supplier shall document a justification for all the information that is provided in each safety manual for compliant items.

NOTE 1 It is essential that the claimed safety performance of an element is supported by sufficient evidence. Unsupported claims do not help establish the correctness and integrity of the safety function to which the element contributes.

NOTE 2 There may be commercial or legal restrictions on the availability of the evidence. These restrictions are outside the scope of this standard. If such restrictions deny the functional safety assessment adequate access to the evidence, then the element is not suitable for use in E/E/PE safety-related systems.

7.4.10 Requirements for proven in use elements

NOTE See 7.4.2.2 c) for details, when the requirements of this subclause apply.

7.4.10.1 An element shall only be regarded as proven in use when it has a clearly restricted and specified functionality and when there is adequate documentary evidence to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required safety integrity levels of the safety functions that use the element is achieved. Evidence shall be based on analysis of operational experience of a specific configuration of the element together with suitability analysis and testing.

NOTE Suitability analysis and testing focuses on the demonstration of the element's performance within the intended application. The results of existing analysis and testing should be taken into account. This includes functional behaviour, accuracy, behaviour in the case of a fault, time response, response to overload, usability (e.g., avoidance of human error) and maintainability.

7.4.10.2 The documentary evidence required by 7.4.10.1 shall demonstrate that:

a) the previous conditions of use (see Note 1) of the specific element are the same as, or sufficiently close to, those that will be experienced by the element in the E/E/PE safety-related system;

NOTE 1 The conditions of use (operational profile) include all the factors that may trigger systematic faults in the hardware and software of the element. For example environment, modes of use, functions performed, configuration, interfaces to other systems, operating system, translator, human factors. Rigorous conditions for similarity of operational profile may be found in IEC 61784-3.

b) the dangerous failure rate has not been exceeded in previous use.

NOTE 2 See IEC 61508-7, Annex D, for guidelines on the use of a probabilistic approach to determining software safety integrity for pre-developed software based on operational experience

NOTE 3 The collection of evidence for proven in use elements requires an effective system for reporting failures.

7.4.10.3 When there is any difference between the previous conditions of use and those that will be experienced in the E/E/PE safety-related system, then an impact analysis on the differences shall be carried out using a combination of appropriate analytical methods and testing, in order to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required safety integrity level(s) of the safety function(s) that use the element is achieved.

7.4.10.4 A proven in use safety justification shall be documented, using the information available from 7.4.10.2, that the element supports the required safety function with the required systematic safety integrity. This shall include:

a) the suitability analysis and testing of the element for the intended application;

b) the demonstration of equivalence between the intended operation and the previous operation experience, including the impact analysis on the differences;

c) the statistical evidence.

7.4.10.5 The following factors shall be taken into account when determining whether or not the above requirements (7.4.10.1 to 7.4.10.4) have been met, in terms of both the coverage and degree of detail of the available information (see also 4.1 of IEC 61508-1):

a) the complexity of the element;

b) the systematic capability required for the element;

c) the novelty of design.

7.4.10.6 There shall be satisfactory evidence that, the existing element's functions that are not covered by the proven in use demonstration, cannot adversely affect the safety integrity of the element functions that are used.

NOTE This requirement can be achieved by ensuring that the functions are physically or electrically disabled or that software to implement these functions is excluded from the operational configuration, or by other forms of arguments and evidence.

7.4.10.7 Any future modification of a proven in use element shall comply with the requirements of 7.8, and IEC 61508-3.

7.4.11 Additional requirements for data communications

7.4.11.1 When data communication is used in the implementation of a safety function then the failure measure (such as the residual error rate) of the communication process shall be estimated taking into account transmission errors, repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade. This failure measure shall be taken into account when estimating the failure measure of the safety function due to random failures (see 7.4.5).

NOTE The term: "masquerade" means that the true source of a message is not correctly identified. For example, a message from a non-safety element is incorrectly identified as a message from a safety element.

7.4.11.2 The techniques and measures necessary to ensure the required failure measure (such as the residual error rate) of the communication process (see 7.4.11.1) shall be implemented according to the requirements of this standard and IEC 61508-3. This allows two possible approaches:

– the entire communication channel shall be designed, implemented and validated according to the IEC 61508 series and IEC 61784-3 or IEC 62280 series. This a so-called 'white channel' (see Figure 7 a); or

– parts of the communication channel are not designed or validated according to the IEC 61508 series. This is a so-called 'black channel' (see Figure 7 b). In this case, the measures necessary to ensure the failure performance of the communication process shall be implemented in the E/E/PE safety-related subsystems or elements that interface with the communication channel in accordance with the IEC 61784-3 or IEC 62280 series as appropriate.

Figure 7 (a) White channel

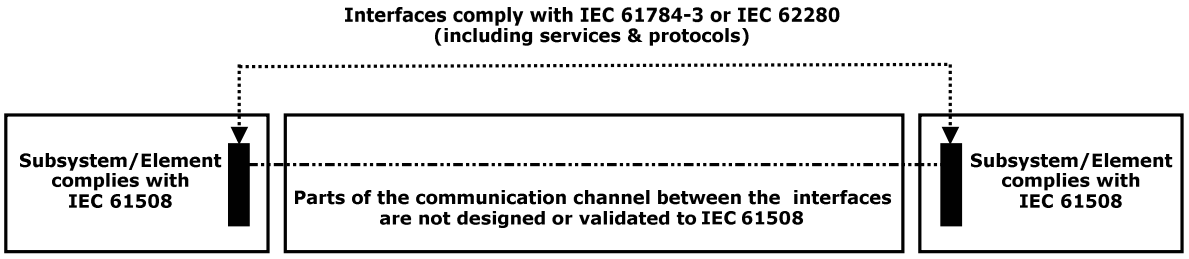


Figure 7 (b) Black channel

Figure 7 – Architectures for data communication

7.5 E/E/PE system integration

NOTE This phase is Box 10.4 of Figure 2.

7.5.1 Objective

The objective of the requirements of this subclause is to integrate and test the E/E/PE safety-related system.

7.5.2 Requirements

7.5.2.1 The E/E/PE safety-related system shall be integrated according to the specified E/E/PE system design and shall be tested according to the specified E/E/PE system integration tests (see 7.4.2.11).

7.5.2.2 As part of the integration of all modules into the E/E/PE safety-related system, the E/E/PE safety-related system shall be tested as specified (see 7.4). These tests shall show that all modules interact correctly to perform their intended function and are designed not to perform unintended functions.

NOTE 1 This does not imply testing of all input combinations. Testing all equivalence classes (see B.5.2 of IEC 61508-7) may suffice. Static analysis (see B.6.4 of IEC 61508-7), dynamic analysis (see B.6.5 of IEC 61508-7) or failure analysis (see B.6.6 of IEC 61508-7) may reduce the number of test cases to an acceptable level. The requirements are easier to fulfil if the E/E/PE safety-related system is developed using structured design (see B.3.2 of 61508-7) or semi-formal methods (see B.2.3 of 61508-7).

NOTE 2 Where the development uses formal methods (see B.2.2 of IEC 61508-7) or formal proofs or assertions (see C.5.12 and C.3.3 of 61508-7), such tests may be reduced in scope.

NOTE 3 Statistical evidence may be used as well (see B.5.3 of IEC 61508-7).

7.5.2.3 The integration of safety-related software into the E/E/PE safety-related system shall be carried out according to 7.5 of IEC 61508-3.

7.5.2.4 Appropriate documentation of the integration testing of the E/E/PE safety-related system shall be produced, stating the test results and whether the objectives and criteria specified during the design and development phase have been met. If there is a failure, the reasons for the failure and its correction shall be documented.

7.5.2.5 During the integration and testing, any modifications or change to the E/E/PE safety-related system shall be subject to an impact analysis which shall identify all subsystems and elements affected and the necessary re-verification activities.

7.5.2.6 The E/E/PE system integration testing shall document the following information:

a) the version of the test specification used;

b) the criteria for acceptance of the integration tests;

c) the version of the E/E/PE safety-related system being tested;

d) the tools and equipment used along with calibration data;

e) the results of each test;

f) any discrepancy between expected and actual results;

g) the analysis made and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur.

7.5.2.7 For the avoidance of faults during the E/E/PE system integration, an appropriate group of techniques and measures according to Table B.3 shall be used.

7.6 E/E/PE system operation and maintenance procedures

NOTE This phase is Box 10.5 of Figure 2.

7.6.1 Objective

The objective of the requirements of this subclause is to develop procedures to ensure that the required functional safety of the E/E/PE safety-related system is maintained during operation and maintenance.

7.6.2 Requirements

7.6.2.1 E/E/PE system operation and maintenance procedures shall be prepared. They shall specify the following:

a) the routine actions that need to be carried out to maintain the as-designed functional safety of the E/E/PE safety-related system, including routine replacement of elements with a pre-defined life, for example cooling fans, batteries; etc.

b) the actions and constraints that are necessary (for example, during installation, start-up, normal operation, routine testing, foreseeable disturbances, faults or failures, and shut-down) to prevent an unsafe state and/or reduce the consequences of a harmful event;

c) the documentation that needs to be maintained on system failure and demand rates on the E/E/PE safety-related system;

d) the documentation that needs to be maintained showing results of audits and tests on the E/E/PE safety-related system;

e) the maintenance procedures to be followed when faults or failures occur in the E/E/PE safety-related system, including:

   – procedures for fault diagnoses and repair;

   – procedures for revalidation;

   – maintenance reporting requirements;

   – procedures to re-validate if original equipment items are no longer available or have been superseded by new versions.

f) the procedures for reporting maintenance performance shall be specified. In particular:

   – procedures for reporting failures;

   – procedures for analysing failures;

g) the tools necessary for maintenance and revalidation and procedures for maintaining the tools and equipment.

NOTE 1 It may be beneficial, for reasons of both safety and economics, to integrate the E/E/PE system operation and maintenance procedures with the EUC overall operation and maintenance procedures.

NOTE 2 The E/E/PE system operation and maintenance procedures should include the software modification procedures (see IEC 61508-3, 7.8).

7.6.2.2 The E/E/PE safety-related system operation and maintenance procedures shall be continuously upgraded from inputs such as (1) the results of functional safety audits and (2) tests on the E/E/PE safety-related system.

7.6.2.3 The routine maintenance actions required to maintain the required functional safety (as designed) of the E/E/PE safety-related system shall be determined by a systematic method. This method shall determine unrevealed failures of all safety-related elements (from sensors through to final elements) that would cause a reduction in the safety integrity achieved. Suitable methods include:

– examination of fault trees;

– failure mode and effect analysis.

NOTE 1 A consideration of human factors is a key element in determining the actions required and the appropriate interface(s) with the E/E/PE safety-related system.

NOTE 2 Proof tests will be carried out with a frequency necessary to achieve the target failure measure.

NOTE 3 The frequency of the proof tests, the diagnostic test interval and the time for subsequent repair will be dependent upon several factors (see Annex B of IEC 61508-6), including:

– the target failure measure associated with the safety integrity level;

– the architecture;

– the diagnostic coverage of the diagnostic tests, and

– the expected demand rate.

NOTE 4 The frequency of the proof tests and the diagnostic test interval are likely to have a crucial bearing on the achievement of hardware safety integrity. One of the principal reasons for carrying out hardware reliability analysis (see 7.4.5.2) is to ensure that the frequencies of the two types of tests are appropriate for the target hardware safety integrity.

NOTE 5 Manufacturer's maintenance requirements should be followed and sole reliance should not be placed on reliability centred maintenance methods until it can be fully justified (e.g. by reliability analysis that demonstrates that the E/E/PE safety-related system's target failure measures are satisfied).

7.6.2.4 The E/E/PE system operation and maintenance procedures shall be assessed for the impact they may have on the EUC.

7.6.2.5 For the avoidance of faults and failures during the E/E/PE system operation and maintenance procedures, an appropriate group of techniques and measures according to Table B.4 shall be used.

7.7 E/E/PE system safety validation

NOTE This phase is Box 10.6 of Figure 2.

7.7.1 Objective

The objective of the requirements of this subclause is to validate that the E/E/PE safety-related system meets in all respects the requirements for safety in terms of the required safety functions and safety integrity (see 7.2 above and 7.10 of IEC 61508-1).

7.7.2 Requirements

7.7.2.1 The validation of the E/E/PE system safety shall be carried out in accordance with a prepared plan (see also 7.7 of IEC 61508-3).

NOTE 1 The E/E/PE system safety validation is shown on the E/E/PE system safety lifecycle as being carried out prior to installation but, in some cases, the E/E/PE system safety validation cannot be carried out until after installation (for example, when the application software development is not finalised until after installation).

NOTE 2 Validation of a programmable electronic safety-related system comprises validation of both hardware and software. The requirements for validation of software are contained in IEC 61508-3.

7.7.2.2 All test measurement equipment used for validation shall be calibrated against a standard traceable to a national standard, if available, or to a well-recognised procedure. All test equipment shall be verified for correct operation.

7.7.2.3 The adequate implementation of each safety function specified in the E/E/PE system safety requirements (see 7.10 of IEC 61508-1), the E/E/PE system design requirements (see 7.2), and all the E/E/PE system operation and maintenance procedures shall be validated by test and/or analysis. If adequate independence or decoupling between individual elements or subsystems cannot be demonstrated analytically, the related combinations of functional behaviour shall be tested.

NOTE As the number of necessary test combinations can get very large, a restructuring of the system may be required at this occasion.

7.7.2.4 Appropriate documentation of the E/E/PE system safety validation testing shall be produced which shall state for each safety function:

a) the version of the E/E/PE system safety validation plan being used;

b) the safety function under test (or analysis), along with the specific reference to the requirement specified during E/E/PE system safety validation planning;

c) tools and equipment used, along with calibration data;

d) the results of each test;

e) discrepancies between expected and actual results.

NOTE Separate documentation is not needed for each safety function, but the information in a) to e) must apply to every safety function and where it differs by safety function the relationship must be stated.

7.7.2.5 When discrepancies occur (i.e. the actual results deviate from the expected results by more than the stated tolerances), the results of the E/E/PE system safety validation testing shall be documented, including:

a) the analysis made; and

b) the decision taken on whether to continue the test or issue a change request and return to an earlier part of the validation test.

7.7.2.6 The supplier or developer shall make available results of the E/E/PE system safety validation testing to the developer of the EUC and the EUC control system so as to enable them to meet the requirements for overall safety validation in IEC 61508-1.

7.7.2.7 For the avoidance of faults during the E/E/PE system safety validation an appropriate group of techniques and measures according to Table B.5 shall be used.

7.8 E/E/PE system modification

7.8.1 Objective

The objective of the requirements of this subclause is to make corrections, enhancements or adaptations to the E/E/PE safety-related system, ensuring that the required safety integrity is achieved and maintained.

7.8.2 Requirements

7.8.2.1 Appropriate documentation shall be established and maintained for each E/E/PE system modification activity. The documentation shall include:

a) the detailed specification of the modification or change;

b) an analysis of the impact of the modification activity on the overall system, including hardware, software (see IEC 61508-3), human interaction and the environment and possible interactions;

c) all approvals for changes;

d) progress of changes;

e) test cases for subsystems and elements including revalidation data;

f) E/E/PE system configuration management history;

g) deviation from normal operations and conditions;

h) necessary changes to system procedures;

i) necessary changes to documentation.

7.8.2.2 Manufacturers or system suppliers that claim compliance with all or part of this standard shall maintain a system to initiate changes as a result of defects being detected in hardware or software and to inform users of the need for modification in the event of the defect affecting safety.

7.8.2.3 Modifications shall be performed with at least the same level of expertise, automated tools (see 7.4.4.2 of IEC 61508-3), and planning and management as the initial development of the E/E/PE safety-related systems.

7.8.2.4 After modification, the E/E/PE safety-related systems shall be reverified and revalidated.

NOTE See also 7.16.2.6 of IEC 61508-1.

7.9 E/E/PE system verification

7.9.1 Objective

The objective of the requirements of this subclause is to test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.

NOTE For convenience all verification activities have been drawn together under 7.9, but they are actually performed for each relevant phase.

7.9.2 Requirements

7.9.2.1 The verification of the E/E/PE safety-related systems shall be planned concurrently with the development (see 7.4), for each phase of the E/E/PE system safety lifecycle, and shall be documented.

7.9.2.2 The E/E/PE system verification planning shall refer to all the criteria, techniques and tools to be utilised in the verification for that phase.

7.9.2.3 The E/E/PE system verification planning shall specify the activities to be performed to ensure correctness and consistency with respect to the products and standards provided as input to that phase.

7.9.2.4 The E/E/PE system verification planning shall consider the following:

a) the selection of verification strategies and techniques;

b) the selection and utilisation of the test equipment;

c) the selection and documentation of verification activities;

d) the evaluation of verification results gained from verification equipment direct and from tests.

7.9.2.5 In each design and development phase it shall be shown that the functional and safety integrity requirements are met.

7.9.2.6 The result of each verification activity shall be documented, stating either that the E/E/PE safety-related systems have passed the verification, or the reasons for the failures. The following shall be considered:

a) items that do not conform to one or more relevant requirements of the E/E/PE system safety lifecycle (see 7.2);

b) items that do not conform to one or more relevant design standards (see 7.4);

c) items that do not conform to one or more relevant safety management requirements (see Clause 6).

7.9.2.7 For E/E/PE system design requirements verification, after E/E/PE system design requirements have been established (see 7.2), and before the next phase (design and development) begins, verification shall:

a) determine whether the E/E/PE system design requirements are adequate to satisfy the E/E/PE system safety requirements specification (see 7.10 of IEC 61508-1) for safety, functionality, and other requirements specified during safety planning; and

b) check for incompatibilities between:
   - the E/E/PE system safety requirements (see 7.10 of IEC 61508-1);
   - the E/E/PE system design requirements (see 7.2);
   - the E/E/PE system tests (see 7.4); and
   - the user documentation and all other system documentation.

7.9.2.8 For E/E/PE system design and development verification, after E/E/PE system design and development (see 7.4) has been completed and before the next phase (integration) begins, verification shall:

a) determine whether the E/E/PE system tests are adequate for the E/E/PE system design and development;

b) determine the consistency and completeness (down to and including module level) of the E/E/PE system design and development with respect to the E/E/PE system safety requirements (see 7.10 of IEC 61508-1); and

c) check for incompatibilities between:
   - the E/E/PE system safety requirements (see 7.10 of IEC 61508-1);
   - the E/E/PE system design requirements (see 7.2);
   - the E/E/PE system design and development (see 7.4); and
   - the E/E/PE system tests (see 7.4).

NOTE 1 Table B.5 recommends safety validation, failure analysis and testing techniques that are also applicable to verification.

NOTE 2 Verification that the diagnostic coverage has been achieved will take into account Table A.1, which gives the faults and failures that must be detected.

7.9.2.9 For E/E/PE system integration verification, the integration of the E/E/PE safety-related system shall be verified to establish that the requirements of 7.5 have been achieved.

7.9.2.10 Test cases and their results shall be documented.

8 Functional safety assessment

The requirements for functional safety assessment are as detailed in Clause 8 of IEC 61508-1.

Annex A
(normative)

Techniques and measures for E/E/PE safety-related systems – control of failures during operation

A.1 General

This annex shall be used in conjunction with 7.4. It limits the maximum diagnostic coverage that may be claimed for relevant techniques and measures. For each safety integrity level, the annex recommends techniques and measures for controlling random hardware, systematic, environmental and operational failures. More information about architectures and measures can be found in Annex B of IEC 61508-6 and Annex A of IEC 61508-7.

It is not possible to list every individual physical cause of a failure in complex hardware for two main reasons:

– the cause/effect relationship between faults and failures is often difficult to determine;
– the emphasis on failures changes from random to systematic when complex hardware and software is used.

Failures in E/E/PE safety-related systems may be categorised, according to the time of their origin, into:

– failures caused by faults originating **before or during system installation** (for example, software faults include specification and program faults, hardware faults include manufacturing faults and incorrect selection of elements); and
– failures caused by faults or human errors originating **after system installation** (for example random hardware failures, or failures caused by incorrect use).

In order to avoid or control such failures when they occur, a large number of measures are normally necessary. The structure of the requirements in Annexes A and B results from dividing the measures into those used to **avoid failures** during the different phases of the E/E/PE system safety lifecycle (Annex B), and those used to **control failures** during operation (this Annex). The measures to control failures are built-in features of the E/E/PE safety-related systems.

Diagnostic coverage and safe failure fraction are determined on the basis of Table A.1 and according to procedures detailed in Annex C. Tables A.2 to A.14 support the requirements of Table A.1 by recommending techniques and measures for diagnostic tests and recommending maximum levels of diagnostic coverage that can be achieved using them. The tables do not replace any of the requirements of Annex C. Tables A.2 to A.14 are not exhaustive. Other measures and techniques may be used, provided evidence is produced to support the claimed diagnostic coverage. If high diagnostic coverage is being claimed then, as a minimum, at least one technique of high diagnostic coverage should be applied from each of these tables.

Similarly, Tables A.15 to A.17 recommends techniques and measures for each safety integrity level for controlling systematic failures. Table A.15 recommends overall measures to control systematic failures (see also IEC 61508-3), Table A.16 recommends measures to control environmental failures and Table A.17 recommends measures to control operational failures. Most of these control measures can be graded according to Table A.18.

All techniques and measures in these tables are described in Annex A of IEC 61508-7. Software techniques and measures required for each safety integrity level are given in IEC 61508-3. Guidelines for determining the architecture for an E/E/PE safety-related system are given in Annex B of IEC 61508-6.

Following the guidelines in this annex does not guarantee by itself the required safety integrity. It is important to consider the following:

– the consistency of the chosen techniques and measures, and how well they will complement each other; and

– which techniques and measures are most appropriate for the specific problems encountered during the development of each particular E/E/PE safety-related system.

A.2 Hardware safety integrity

Table A.1 provides the requirements for faults or failures that shall be detected by techniques and measures to control hardware failures, in order to achieve the relevant level of diagnostic coverage (see also Annex C). Tables A.2 to A.14 support the requirements of Table A.1 by recommending techniques and measures for diagnostic tests and recommending maximum levels of diagnostic coverage that can be achieved using them. These tests may operate continuously or periodically. The tables do not replace any of the requirements of 7.4. Tables A.2 to A.14 are not exhaustive. Other measures and techniques may be used, provided evidence is produced to support the claimed diagnostic coverage.

NOTE 1 The overview of techniques and measures associated with these tables is in Annex A of IEC 61508-7. The relevant subclause is referenced in the second column of Tables A.2 to A.14.

NOTE 2 The designations low, medium and high diagnostic coverage are quantified as 60 %, 90 % and 99 % respectively.

Table A.1 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction

Component	See table(s)	Requirements for diagnostic coverage claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Electromechanical devices	A.2	Does not energize or de-energize	Does not energize or de-energize	Does not energize or de-energize
		Welded contacts	Individual contacts welded	Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent)
				No positive opening (for position switches this failure is not assumed if they are built and tested according to IEC 60947-5-1, or equivalent)
Discrete hardware	A.3, A.7, A.9			
Digital I/O		Stuck-at (see Note 1)	DC fault model (see Note 2)	DC fault model drift and oscillation
Analogue I/O		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation
Power supply		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation
Bus	A.3			
General	A.7	Stuck-at of the addresses	Time out	Time out
Memory management unit (MMU)	A.8	Stuck-at of data or addresses	Wrong address decoding	Wrong address decoding
			Change of addresses caused by soft-errors in the MMU registers (see Notes 3 and 4)	Change of addresses caused by soft-errors in the MMU registers
Direct memory access (DMA)		No or continuous access	DC fault model for data and addresses	All faults that affect data in the memory
			Change of information caused by soft-errors in the DMA registers	Wrong access time
			Wrong access time	
Bus-arbitration (see Note 5)		Stuck-at of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration
Central Processing Unit (CPU)	A.4, A.10			
Register, internal RAM		Stuck-at for data and addresses	DC fault model for data and addresses	DC fault model for data and addresses
			Change of information caused by soft-errors	Dynamic cross-over for memory cells
				Change of information caused by soft-errors
				No, wrong or multiple addressing
Coding and execution including flag register		Wrong coding or no execution	Wrong coding or wrong execution	No definite failure assumption
Address calculation		Stuck-at	DC fault model	No definite failure assumption
			Change of addresses caused by soft-errors	
Program counter, stack pointer		Stuck-at	DC fault model	DC fault model
			Change of addresses caused by soft-errors	Change of addresses caused by soft-errors

Table A.1 *(continued)*

Component	See table(s)	Requirements for diagnostic coverage claimed		
		Low (60 %)	**Medium (90 %)**	**High (99 %)**
Interrupt handling	A.4			
Interrupt		No or continuous interrupts (see Note 6)	No or continuous interrupts	No or continuous interrupts
			Cross-over of interrupts	Cross-over of interrupts
Reset circuitry		Stuck-at	DC fault model	DC fault model
		Individual components do not initialize to reset state	Drift and oscillation	Drift and oscillation
			Individual components do not initialize to reset state	Individual components do not initialize to reset state
Invariable memory	A.5	Stuck-at for data and addresses	DC fault model for data and addresses	All faults that affect data in the memory
Variable memory	A.6	Stuck-at for data and addresses	DC fault model for data and addresses	DC fault model for data and addresses
			Change of information caused by soft-errors	Dynamic cross-over for memory cells
				Change of information caused by soft-errors
				No, wrong or multiple addressing
Clock (quartz, oscillator, PLL)	A.11	Sub- or super-harmonic	Incorrect frequency	Incorrect frequency
		Period jitter	Period jitter	Period jitter
Communication and mass storage	A.12	Wrong data or addresses	All faults that affect data in the memory	All faults that affect data in the memory
		No transmission	Wrong data or addresses	Wrong data or addresses
			Wrong transmission time	Wrong transmission time
			Wrong transmission sequence	Wrong transmission sequence
Sensors	A.13	Stuck-at	DC fault model	DC fault model
			Drift and oscillation	Drift and oscillation
Final elements	A.14	Stuck-at	DC fault model	DC fault model
			Drift and oscillation	Drift and oscillation

NOTE 1 "Stuck-at" is a fault category that can be described with continuous "0" or "1" or "on" at the pins of an element.

NOTE 2 "DC fault model" includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines. For integrated circuits, short circuit between any two connections (pins) is considered.

NOTE 3 The soft-error rate (SER) for low energized semiconductors is known to be more than one order of magnitude higher (50x..500x) than the hard-error rate (permanent damage of the device).

NOTE 4 Causes of soft errors are: alpha particles from package decay, neutrons, external EMI noise and internal cross-talk. The effect of soft-errors can only be mastered by safety integrity measures at runtime. Safety integrity measures effective for random hardware failures may not be effective for soft-errors.

EXAMPLE: RAM tests, such as walk-path, galpat, etc. are not effective, whereas monitoring techniques using Parity and ECC with recurring read of the memory cells or techniques using redundancy (and comparison or voting) can be.

NOTE 5 Bus-arbitration is the mechanism for deciding which device has control of the bus.

NOTE 6 No interrupt means that no interrupt is carried out when an interrupt(s) should take place. Continuous interrupts means that continuous interrupts are carried out when they should not take place.

NOTE 7 For ASICs, this table and Tables A.2 to A.18 apply where relevant.

Table A.2 – Electrical components

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Monitoring of relay contacts	A.1.2	High	Relay switching rate should be taken into account when quantifying the effect of random failures
Comparator	A.1.3	High	High if failure modes are predominantly in a safe direction
Majority voter	A.1.4	High	Depends on the quality of the voting
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.3 – Electronic components

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Comparator	A.1.3	High	High if failure modes are predominantly in a safe direction
Majority voter	A.1.4	High	Depends on the quality of the voting
Tests by redundant hardware	A.2.1	Medium	Depends on diagnostic coverage of failure detection
Dynamic principles	A.2.2	Medium	Depends on diagnostic coverage of failure detection
Standard test access port and boundary-scan architecture	A.2.3	High	Depends on the diagnostic coverage of failure detection
Monitored redundancy	A.2.5	High	Depends on the degree of redundancy and of the monitoring
Hardware with automatic check	A.2.6	High	Depends on the diagnostic coverage of the tests
Analogue signal monitoring	A.2.7	Low	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.4 – Processing units

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Comparator	A.1.3	High	Depends on the quality of the comparison
Majority voter	A.1.4	High	Depends on the quality of the voting
Self-test by software: limited number of patterns (one channel)	A.3.1	Low	
Self-test by software: walking bit (one-channel)	A.3.2	Medium	
Self-test supported by hardware (one-channel)	A.3.3	Medium	
Coded processing (one-channel)	A.3.4	High	
Reciprocal comparison by software	A.3.5	High	Depends on the quality of the comparison
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1. NOTE 4 As a number of processing unit faults lead to a modification of flow control, diagnostic measures and techniques listed in Table A.10 may also be taken into account for processing unit faults. These diagnostic measures and techniques cover the control flow only, not the data flow.			

Table A.5 – Invariable memory ranges

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Word-protection multi-bit redundancy	A.4.1	Medium	The effectiveness of the Word-protection multi-bit redundancy depends on the inclusion of the word address into the multiple bit redundancy, and relies on respective measure to detect multi-bit common cause faults, e.g. multiple addressing (multiple row select, multiple local to global bit line switches activated), power supply issues (e.g. charge pump flaws), production row and column replacement (production yield measure to mask production faults), etc.
Modified checksum	A.4.2	Low	
Signature of one word (8-bit)	A.4.3	Medium	The effectiveness of the signature depends on the width of the signature in relation to the block length of the information to be protected
Signature of a double word (16-bit)	A.4.4	High	The effectiveness of the signature depends on the width of the signature in relation to the block length of the information to be protected
Block replication	A.4.5	High	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.6 – Variable memory ranges

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
RAM test checkerboard or march	A.5.1	Low	
RAM test walk-path	A.5.2	Medium	
RAM test galpat or transparent galpat	A.5.3	High	
RAM test Abraham	A.5.4	High	
Parity-bit for RAM	A.5.5	Low	
RAM monitoring with a modified Hamming code, or detection of data failures with error-detection-correction codes (EDC)	A.5.6	Medium	The effectiveness of the RAM monitoring with a modified Hamming code, or detection of data failures with error detection-correction codes (EDC) depends on the inclusion of the address into the Hamming code, and relies on respective measure to detect multi-bit common cause faults, e.g. multiple addressing (multiple row select, multiple local to global bit line switches activated), production row and column replacement (production yield measure to mask production faults), etc.
Double RAM with hardware or software comparison and read/write test	A.5.7	High	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1. NOTE 4 For RAM that is read/written only infrequently (for example during configuration) the measures A.4.1 to A.4.4 of IEC 61508-7 are effective if they are executed after each read/write access.			

Table A.7 – I/O units and interface (external communication)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Test pattern	A.6.1	High	
Code protection	A.6.2	High	
Multi-channel parallel output	A.6.3	High	Only if dataflow changes within diagnostic test interval
Monitored outputs	A.6.4	High	Only if dataflow changes within diagnostic test interval
Input comparison/voting (1oo2, 2oo3 or better redundancy)	A.6.5	High	Only if dataflow changes within diagnostic test interval
Antivalent signal transmission	A.11.4	High	For example transmission of inverted signals.
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.8 – Data paths (internal communication)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
One-bit hardware redundancy	A.7.1	Low	In case of multiplane crossbar switch type of data path, the given effectiveness can only be assumed if the address and control lines are covered by the safety measures.
Multi-bit hardware redundancy	A.7.2	Medium	In case of multiplane crossbar switch type of data path, the given effectiveness can only be assumed if the address and control lines are covered by the safety measures.
Complete hardware redundancy	A.7.3	High	
Inspection using test patterns	A.7.4	High	
Transmission redundancy	A.7.5	High	Effective only against transient faults
Information redundancy	A.7.6	High	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.9 – Power supply

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Overvoltage protection with safety shut-off or switch-over to second power unit	A.8.1	Low	
Voltage control (secondary) with safety shut-off or switch-over to second power unit	A.8.2	High	
Power-down with safety shut-off or switch-over to second power unit	A.8.3	High	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.10 – Program sequence (watch-dog)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Watch-dog with separate time base without time-window	A.9.1	Low	
Watch-dog with separate time base and time-window	A.9.2	Medium	
Logical monitoring of program sequence	A.9.3	Medium	Depends on the quality of the monitoring
Combination of temporal and logical monitoring of programme sequences	A.9.4	High	
Temporal monitoring with on-line check	A.9.5	Medium	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.11 – Clock

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Watch-dog with separate time base without time-window	A.9.1	Low	
Watch-dog with separate time base and time-window	A.9.2	High	Depends on time restriction for the time-window
Logical monitoring of program sequence	A.9.3	Medium	Only effective against clock failures if external temporal events influence the logical program flow
Temporal and logical monitoring	A.9.4	High	
Temporal monitoring with on-line check	A.9.5	Medium	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.12 – Communication and mass-storage

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Information exchange between E/E/PE safety-related system and process	A.6	See Table A.7	See I/O units and interface
Information exchange between E/E/PE safety-related systems	A.7	See Table A.8	See data paths/bus
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.13 – Sensors

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Analogue signal monitoring	A.2.7	Low	
Test pattern	A.6.1	High	
Input comparison/voting (1oo2, 2oo3 or better redundancy)	A.6.5	High	Only if dataflow changes within diagnostic test interval
Reference sensor	A.12.1	High	Depends on diagnostic coverage of failure detection
Positive-activated switch	A.12.2	High	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Table A.14 – Final elements (actuators)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Monitoring of relay contacts	A.1.2	High	Relay switching rate should be taken into account when quantifying the effect of random failures
Test pattern	A.6.1	High	
Monitoring	A.13.1	High	Depends on diagnostic coverage of failure detection
Cross-monitoring of multiple actuators	A.13.2	High	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

A.3 Systematic safety integrity

The following tables give recommendations for techniques and measures to:

– control failures caused by hardware design (see Table A.15);

– control failures due to environmental stress or influences (see Table A.16); and

– control failures during operation (see Table A.17).

In Tables A.15 to A.17, recommendations are made and requirements are given by safety integrity level, stating firstly the importance of the technique or measure and secondly the effectiveness required if it is used. The importance is signified as follows:

– M: the technique or measure is required (mandatory) for this safety integrity level;

– HR: the technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used then the rationale behind not using it shall be detailed;

– R: the technique or measure is recommended for this safety integrity level;

– -: the technique or measure has no recommendation for or against being used;

– NR: the technique or measure is positively not recommended for this safety integrity level; If this technique or measure is used then the rationale behind using it shall be detailed.

The required effectiveness is signified as follows:

– Low: if used, the technique or measure shall be used to the extent necessary to give at least low effectiveness against systematic failures;

– Medium: if used, the technique or measure shall be used to the extent necessary to give at least medium effectiveness against systematic failures;

– High: if used, the technique or measure shall be used to the extent necessary to give high effectiveness against systematic failures.

Guidance on levels of effectiveness for most techniques and measures is given in Table A.18.

If a measure is not mandatory, it is in principle replaceable by other measures (either individually or in combination); this is governed by the shading, as explained in the table.

All techniques and measures given here are built-in features of the E/E/PE safety-related systems, which may help to control failures on-line. Procedural and organisational techniques and measures are necessary throughout the E/E/PE system safety lifecycle to avoid introducing faults, and validation techniques to test the E/E/PE safety-related systems' behaviour against expected external influences are necessary to demonstrate that the built-in features are appropriate for the specific application (see Annex B).

Annex D of IEC 61508-6 gives information on common cause failures.

NOTE Most of the measures in Tables A.15 to A.17 can be used with varying effectiveness according to Table A.18, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and high effectiveness.

Table A.15 – Techniques and measures to control systematic failures caused by hardware design

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Failure detection by on-line monitoring (see Note 4)	A.1.1	R low	R low	R medium	R high
	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
	Standard test access port and boundary-scan architecture	A.2.3	R low	R low	R medium	R high
	Code protection	A.6.2	R low	R low	R medium	R high
	Diverse hardware	B.1.4	– low	– low	R medium	R high

At least one of the techniques in the light grey shaded group, or one of the techniques specified in Table A.3 of IEC 61508-3, is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding this table.

NOTE 2 The measures can be used to varying effectiveness according to Table A.18, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annexes A, B and C of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shutdown systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

Table A.16 – Techniques and measures to control systematic failures caused by environmental stress or influences

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as a.c. power supply frequency variation that can lead to dangerous failure	A.8	M low	M medium	M medium	M high
	Separation of electrical energy lines from information lines (see Note 4)	A.11.1	M	M	M	M
	Increase of interference immunity	A.11.3	M low	M low	M medium	M high
	Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	M low	M high	M high	M high
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
	Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
	Idle current principle (where continuous control is not needed to achieve or maintain a safe state of the EUC)	A.1.5	R	R	R	R
	Measure to detect breaks and shorts in signal lines		R	R	R	R
	Failure detection by on-line monitoring (see Note 5)	A.1.1	R low	R low	R medium	R high
	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
	Code protection	A.6.2	R low	R low	R medium	R high
	Antivalent signal transmission	A.11.4	R low	R low	R medium	R high
	Diverse hardware (see Note 6)	B.1.4	– low	– low	– medium	R high
	Software architecture	**7.4.3 of IEC 61508-3**	See Tables A.2 and C.2 of IEC 61508-3			

This table is divided into three groups, as indicated by the sidebar shading. All techniques marked "R" in the grey and black shaded groups are replaceable by other techniques within that group, but at least one of the techniques in the grey shaded group and at least one of the techniques of the black shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding Table A.15.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to Table A.18, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annexes A and B of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 Separation of electrical energy lines from information lines is not necessary if the information is transported optically, nor is it necessary for low power energy lines that are designed for energising elements of the E/E/PE system and carrying information from or to these elements.

NOTE 5 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

NOTE 6 Diverse hardware is not required if it has been demonstrated, by validation and extensive operational experience, that the hardware is sufficiently free of design faults and sufficiently protected against common cause failures to fulfil the target failure measures.

Table A.17 – Techniques and measures to control systematic operational failures

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Modification protection	B.4.8	M low	M medium	M high	M high
	Failure detection by on-line monitoring (see Note 4)	A.1.1	R low	R low	R medium	R high
	Input acknowledgement	B.4.9	R low	R low	R medium	R high
	Failure assertion programming	C.3.3	See Tables A.2 and C.2 of IEC 61508-3			

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding Table A.15.

NOTE 2 Two of these measures in this table can be used to varying effectiveness according to Table A.18, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annexes A, B, and C of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 For E/E/PE safety-related systems operating in a low-demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

Table A.18 – Effectiveness of techniques and measures to control systematic failures

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Failure detection by on-line monitoring (see Note)	A.1.1	Trigger signals from the EUC and its control system are used to check the proper operation of the E/E/PE safety-related systems (only time behaviour with an upper time limit)	E/E/PE safety-related systems are retriggered by temporal and logical signals from the EUC and its control system (time window for temporal watch-dog function)
Tests by redundant hardware (see Note)	A.2.1	Additional hardware tests the trigger signals of the E/E/PE safety-related systems (only time behaviour with an upper time limit), this hardware switches a secondary final element	Additional hardware is retriggered by temporal and logical signals of the E/E/PE safety-related systems (time window for temporal watch-dog); voting between multiple channels
Standard test access port and boundary-scan architecture	A.2.3	Testing the used solid-state logic, during the proof test, through defined boundary scan tests	Diagnostic test of solid-state logic, according to the functional specification of the E/E/PE safety-related systems; all functions are checked for all integrated circuits
Code protection	A.6.2	Failure detection via time redundancy of signal transmission	Failure detection via time and information redundancy of signal transmission
Measures against voltage breakdown, voltage variations, overvoltage and low voltage	A.8	Overvoltage protection with safety shut-off or switch-over to secondary power unit	Voltage control (secondary) with safety shut-off or switch-over to secondary power unit; or power-down with safety shut-off or switch-over to secondary power unit
Program sequence monitoring	A.9	Temporal or logical monitoring of the program sequence	Temporal and logical monitoring of the program sequence at very many checking points in the program
Measures against temperature increase	A.10	Detecting over-temperature	Actuation of the safety shut-off via thermal fuse; or several levels of over-temperature sensing and alarms; or connection of forced-air cooling and status indication
Increase of interference immunity (see Note)	A.11.3	Noise filter at power supply and critical inputs and outputs; shielding, if necessary	Filter against electromagnetic injection that is normally not expected; shielding
Measures against physical environment	A.14	Generally accepted practice according to the application	Techniques referred to in standards for a particular application
Diverse hardware	B.1.4	Two or more items carrying out the same function but being different in design	Two or more items carrying out different functions
Modification protection	B.4.8	Modification requires specific tools	Modification requires use of key lock or dedicated tool with password
Input acknowledgement	B.4.9	Echoing of input actions back to the operator	Checking strict rules for the input of data by the operator, rejecting incorrect inputs
NOTE In the cases of the techniques with references A.1.1, A.2.1, A.11.3, and A.14 for high effectiveness of the technique or measure it is assumed that the low effectiveness approaches are also used.			

Annex B
(normative)

Techniques and measures for E/E/PE safety-related systems – avoidance of systematic failures during the different phases of the lifecycle

Tables B.1 to B.5 in this annex recommend, for each safety integrity level, techniques and measures to avoid failures in E/E/PE safety-related systems. More information about the techniques and measures can be found in Annex B of IEC 61508-7. Requirements for measures to control failures during operation are given in Annex A and described in Annex A of IEC 61508-7.

It is not possible to list every individual cause of systematic failures, originating throughout the safety life cycle, or every remedy, for two main reasons:

– the effect of a systematic fault depends on the lifecycle phase in which it was introduced; and

– the effectiveness of any single measure to avoid systematic failures depends on the application.

A quantitative analysis for the avoidance of systematic failures is therefore impossible.

Failures in E/E/PE safety-related systems may be categorised, according to the lifecycle phase in which a causal fault is introduced, into:

– failures caused by faults originating *before or during system installation* (for example, software faults include specification and program faults, hardware faults include manufacturing faults and incorrect selection of elements); and

– failures caused by faults originating *after system installation* (for example random hardware failures, or failures caused by incorrect use).

In order to avoid or control such failures when they occur, a large number of measures are normally necessary. The structure of the requirements in Annexes A and B results from dividing the measures into those used to *avoid failures* during the different phases of the E/E/PE system safety lifecycle (this annex), and those used to *control failures* during operation (Annex A). The measures to control failures are built-in features of the E/E/PE safety-related systems, while the measures to avoid failures are performed during the safety lifecycle.

In Tables B.1 to B.5, recommendations are made and requirements are given by safety integrity level, stating firstly the importance of the technique or measure and secondly the effectiveness required if it is used. The importance is signified as follows:

– M: the technique or measure is required (mandatory) for this safety integrity level.

– HR: the technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used then the rationale behind not using it shall be detailed;

– R: the technique or measure is recommended for this safety integrity level.

– -: the technique or measure has no recommendation for or against being used;

– NR: the technique or measure is positively not recommended for this safety integrity level. If this technique or measure is used then the rationale behind using it shall be detailed;

The required effectiveness is signified as follows:

– Low: if used, the technique or measure shall be used to the extent necessary to give at least low effectiveness against systematic failures;

– Medium: if used, the technique or measure shall be used to the extent necessary to give at least medium effectiveness against systematic failures;
– High: the technique or measure shall be used to the extent necessary to give high effectiveness against systematic failures.

NOTE Most of the measures in Tables B.1 to B.5 can be used with varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

If a measure is not mandatory, it is in principle replaceable by other measures (either individually or in combination); this is governed by the shading, as explained in each table.

Following the guidelines in this annex does not guarantee by itself the required safety integrity. It is important to consider the following:

– the consistency of the chosen techniques and measures, and how well they will complement each other;
– which techniques and measures are appropriate, for every phase of the development lifecycle; and
– which techniques and measures are most appropriate for the specific problems encountered during the development of each different E/E/PE safety-related system.

Table B.1 – Techniques and measures to avoid mistakes during specification of E/E/PE system design requirements (see 7.2)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Separation of E/E/PE system safety functions from non-safety functions	B.1.3	HR low	HR low	HR medium	HR high
	Structured specification	B.2.1	HR low	HR low	HR medium	HR high
	Inspection of the specification	B.2.6	– low	HR low	HR medium	HR high
	Semi-formal methods	B.2.3, see also Table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	R low	R low	R medium	R high
	Computer aided specification tools	B.2.4	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

All techniques marked “R” in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in Table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding this table.

NOTE 2 The measures in this table can be used to varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.2 – Techniques and measures to avoid introducing faults during E/E/PE system design and development (see 7.4)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Observance of guidelines and standards	B.3.1	M high	M high	M high	M high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Structured design	B.3.2	HR low	HR low	HR medium	HR high
	Modularisation	B.3.4	HR low	HR low	HR medium	HR high
	Use of well-tried components	B.3.3	R low	R low	R medium	R high
	Semi-formal methods	B.2.3, see also Table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	– low	R low	R medium	R high
	Computer-aided design tools	B.3.5	– low	R low	R medium	R high
	Simulation	B.3.6	– low	R low	R medium	R high
	Inspection of the hardware or walk-through of the hardware	B.3.7 B.3.8	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in Table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding Table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.3 – Techniques and measures to avoid faults during E/E/PE system integration (see 7.5)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Functional testing	B.5.1	M high	M high	M high	M high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Black-box testing	B.5.2	R low	R low	R medium	R high
	Field experience	B.5.4	R low	R low	R medium	R high
	Statistical testing	B.5.3	– low	– low	R medium	R high

All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in Table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding Table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.4 – Techniques and measures to avoid faults and failures during E/E/PE system operation and maintenance procedures (see 7.6)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Operation and maintenance instructions	B.4.1	HR high	HR high	HR high	HR high
	User friendliness	B.4.2	HR high	HR high	HR high	HR high
	Maintenance friendliness	B.4.3	HR high	HR high	HR high	HR high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Limited operation possibilities	B.4.4	– low	R low	HR medium	HR high
	Protection against operator mistakes	B.4.6	– low	R low	HR medium	HR high
	Operation only by skilled operators	B.4.5	– low	R low	R medium	HR high

All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.

The verification of this safety lifecycle phase shall be done by checklists (see B.2.5 of IEC 61508-7) or inspection (see B.2.6 of IEC 61508-7).

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding Table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.5 – Techniques and measures to avoid faults during E/E/PE system safety validation (see 7.7)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Functional testing	B.5.1	HR high	HR high	HR high	HR high
	Functional testing under environmental conditions	B.6.1	HR high	HR high	HR high	HR high
	Interference surge immunity testing	B.6.2	HR high	HR high	HR high	HR high
	Fault insertion testing (when required diagnostic coverage ≥ 90 %)	B.6.10	HR high	HR high	HR high	HR high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Static analysis, dynamic analysis and failure analysis	B.6.4 B.6.5 B.6.6	– low	R low	R medium	R high
	Simulation and failure analysis	B.3.6 B.6.6	– low	R low	R medium	R high
	Worst-case analysis, dynamic analysis and failure analysis	B.6.7 B.6.5 B.6.6	– low	– low	R medium	R high
	Static analysis and failure analysis (see Note 4)	B.6.4 B.6.6	R low	R low	NR	NR
	Expanded functional testing	B.6.8	– low	HR low	HR medium	HR high
	Black-box testing	B.5.2	R low	R low	R medium	R high
	Fault insertion testing (when required diagnostic coverage < 90 %)	B.6.10	R low	R low	R medium	R high
	Statistical testing	B.5.3	– low	– low	R medium	R high
	Worst-case testing	B.6.9	– low	– low	R medium	R high
	Field experience	B.5.4	R low	R low	R medium	NR

This table is divided into three groups, as indicated by the sidebar shading. All techniques marked "R" in the grey and black shaded groups are replaceable by other techniques within that group, but at least one of the techniques of the grey shaded group (analytical techniques) and at least one of the techniques of the black shaded group (testing techniques) is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding Table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

NOTE 4 Static analysis and failure analysis is not recommended for SIL 3 and SIL 4, because these techniques are not sufficient unless used in combination with dynamic analysis.

Table B.6 – Effectiveness of techniques and measures to avoid systematic failures

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Project management (see Note)	B.1.1	Definition of actions and responsibilities; scheduling and resource allocation; training of relevant personnel; consistency checks after modifications	Validation independent from design; project monitoring; standardised validation procedure; configuration management; failure statistics; computer aided engineering; computer-aided software engineering
Documentation (see Note)	B.1.2	Graphical and natural language descriptions, for example block-diagrams, flow-diagrams	Guidelines for consistent content and layout across organization; contents checklists; computer-aided documentation management, formal change control
Separation of E/E/PE system safety functions from non–safety functions	B.1.3	Well-defined interfaces between E/E/PE safety-related systems and non-safety-related systems	Total separation of E/E/PE safety-related systems from non-safety-related systems, i.e. no write access of non-safety-related systems to E/E/PE safety-related systems and separate physical locations to avoid common cause influences
Structured specification	B.2.1	Manual hierarchical separation into sub-requirements; description of the interfaces	Hierarchical separation described using computer-aided engineering tools; automatic consistency checks; refinement down to functional level
Formal methods	B.2.2	Used by personnel experienced in formal methods	Used by personnel experienced in formal methods in similar applications, with computer support tools
Semi-formal methods	B.2.3	Describing some critical parts with semi-formal methods	Describing total E/E/PE safety-related systems with different semi-formal methods to show different aspects; consistency check between the methods
Computer-aided specification tools	B.2.4	Tools without preference for one particular design method	Model-oriented procedures with hierarchical subdivision; description of all objects and their relationships; common data base; automatic consistency checks
Checklists	B.2.5	Prepared checklists for all safety life-cycle phases; concentration on the main safety issues	Prepared detailed checklists for all safety life-cycle phases
Inspection of the specification	B.2.6	Inspection of the safety requirements specification by an independent person	Inspection and re-inspection by an independent organisation using a formal procedure with correction of all faults found
Structured design	B.3.2	Hierarchical circuit design, produced manually	Reuse of tested circuit parts; traceability between specification, design, circuit diagram and parts lists; computer-aided; based on defined methods (see also 7.4.6)
Use of well-tried components (see Note)	B.3.3	Sufficient over-dimensioning; constructive characteristics	Proven in use (see 7.4.10)
Modularization (see Note)	B.3.4	Modules of limited size; each module functionally isolated	Re-use of well-proven modules; easily comprehensible modules; each module has a maximum of one input, one output, and one failure exit

Table B.6 *(continued)*

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Computer-aided design tools	B.3.5	Computer support for complex phases of the safety lifecycle	Use of tools that are proven in use (see 7.4.10) or validated; general computer-aided development for all phases of the safety lifecycle
Simulation	B.3.6	Modelling at a module level, including boundary data of peripheral units	Modelling on a component level, including boundary data
Inspection of the hardware	B.3.7	Inspection by a person independent of the design	Inspection and re-inspection by an independent organisation using a formal procedure with correction of all faults found
Walk-through of the hardware	B.3.8	Walk-through includes a person independent of the design	Walk-through includes an independent organisation and follows a formal procedure with correction of all faults found
Limited operation possibilities (see Note)	B.4.4	Key-operated switch or password to govern change of operating mode	Defined, robust procedure for allowing operation
Operation only by skilled operators	B.4.5	Basic training in the type of safety systems being operated, plus two years' relevant on-the-job experience	Yearly training of all operators; each operator has at least five years' experience with safety-related devices at lower safety integrity levels
Protection against operator mistakes (see Note)	B.4.6	Input acknowledgement	Confirmation and consistency checks on each input command
Black-box testing (see Note)	B.5.2	Equivalence classes and input partition testing, boundary value testing, using pre-written test cases	Test case execution from cause consequence diagrams, combining critical cases at extreme operating boundaries
Statistical testing (see Note)	B.5.3	Statistical distribution of all input data	Test reports by tools; very many test cases; distribution of the input data according to real-life application conditions and assumed failure models
Field experience (see Note)	B.5.4	10 000 h operation time; at least one year's experience with at least 10 devices in different applications; statistical accuracy 95 %; no safety critical failures	10 million h operation time; at least two years' experience with at least 10 devices in different applications; statistical accuracy 99,9 %; detailed documentation of all changes (including minor) during past operation
Surge immunity testing	B.6.2		Surge immunity shall be demonstrably higher than the boundary values for real operating conditions
Static analysis	B.6.4	Based on block diagrams; highlighting weak points; specifying test cases	Based on detailed diagrams; predicting expected behaviour during test cases; using testing tools

Table B.6 *(continued)*

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Dynamic analysis	B.6.5	Based on block diagrams; highlighting weak points; specifying test cases	Based on detailed diagrams; predicting expected behaviour during test cases; using testing tools
Failure analysis	B.6.6	At module level, including boundary data of the peripheral units	At component level, including boundary data
Worst-case analysis	B.6.7	Performed on safety functions; derived using boundary value combinations for real operating conditions	Performed on non-safety functions; derived using boundary value combinations for real operating conditions
Expanded functional testing	B.6.8	Test that all safety functions are maintained in the case of static input states caused by faulty process or operating conditions	Test that all safety functions are maintained in the case of static input states and/or unusual input changes, caused by faulty process or operating conditions (including those that may be very rare)
Worst-case testing	B.6.9	Test that safety functions are maintained for a combination of boundary values found in real operating conditions	Test that non-safety functions are maintained for a combination of the boundary values found in real operating conditions
Fault insertion testing	B.6.10	At subunit level including boundary data or the peripheral units	At component level including boundary data
NOTE In the cases of the techniques with references B.1.1, B.1.2, B.3.3, B.3.4, B.4.4, B.4.6, B.5.2, B.5.3, B.5.4, B.6.7 and B.6.9, for high effectiveness of the technique or measure, it is assumed that the low effectiveness approaches are also used.			

Annex C
(normative)

Diagnostic coverage and safe failure fraction

C.1 Calculation of diagnostic coverage and safe failure fraction of a hardware element

The diagnostic coverage and safe failure fraction of an element (see 3.8.6 and 3.6.15 of IEC 61508-4) shall be calculated as follows:

a) Carry out a failure mode and effect analysis to determine the effect of each failure mode of each component or group of components in the element on the behaviour of the E/E/PE safety-related systems in the absence of diagnostic tests. Sufficient information shall be available (see Notes 1 and 2) to enable the failure mode and effects analysis to be undertaken so as to enable an adequate level of confidence to be established commensurate with the safety integrity requirements.

NOTE 1 In order to undertake this analysis the following information is required:

– a detailed block diagram of the E/E/PE safety-related system describing the element together with the interconnections for that part of the E/E/PE safety-related system which will affect the safety function(s) under consideration;

– the hardware schematics of the element describing each component or group of components and the interconnections between components;

– the failure modes and rates of each component or group of components and associated percentages of the total failure probability corresponding to safe and dangerous failures.

NOTE 2 The required rigour of this analysis will depend on a number of factors (see IEC 61508-1, 4.1). In particular, the safety integrity level of the safety functions involved will need to be taken into account. For higher safety integrity levels it is expected that the failure modes and effects analysis is very specific according to particular component types and application environments. Also, a thorough and detailed analysis is very important for an element that is to be used in a hardware architecture having zero hardware fault tolerance.

b) Categorize each failure mode according to whether it leads (in the absence of diagnostic tests) to:
   – a safe failure; or
   – a dangerous failure;

c) No-effect and no-part failures shall not play any part in the calculation of the diagnostic coverage or the safe failure fraction.

d) From an estimate of the failure rate of each component or group of components, (λ), (see Note 4) and the results of the failure mode and effect analysis, for each component or group of components, calculate the safe failure rate (λ_S), and the dangerous failure rate (λ_D). When one of these failure rates is not constant, its average over the period shall be estimated and used in DC and SFF calculations.

NOTE 3 The failure rate of each component or group of components can be estimated using data from a recognised industry source, taking the application environment into account. However, application specific data is preferred, particularly in cases where the element consists of a small number of components and where any error in estimating the probability of safe and dangerous failures of a particular component could have a significant impact on the estimation of the safe failure fraction.

e) For each component or group of components, estimate the fraction of dangerous failures that will be detected by the diagnostic tests (see C.2) and therefore the dangerous failure rate that is detected by the diagnostic tests, (λ_{Dd}).

f) For the element, calculate the total dangerous failure rate, ($\Sigma\lambda_D$), the total dangerous failure rate that is detected by the diagnostic tests, ($\Sigma\lambda_{Dd}$), and the total safe failure rate, ($\Sigma\lambda_S$).

g Calculate the diagnostic coverage of the element as ($\Sigma\lambda_{Dd}/\Sigma\lambda_D$).

h) Calculate safe failure fraction of the element as:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

NOTE 4 The above equation is applicable when the failure rates are based on constant failure rates (see 3.6.15 of IEC 61508-4 for the definitive formula).

NOTE 5 The diagnostic coverage (if any) of each element in the E/E/PE safety-related system is taken into account in the estimation of the achieved failure measure for each safety function (see 7.4.5.2). The safe failure fraction is taken into account when determining the architectural constraints on hardware safety integrity (see 7.4.4).

The analysis used to determine the diagnostic coverage and safe failure fraction shall include all of the components, including electrical, electronic, electromechanical, mechanical etc, that are necessary to allow the element to process the safety function(s) as required by the E/E/PE safety-related system. All of the possible dangerous modes of failure that will lead to an unsafe state, prevent a safe response when such a response is demanded or otherwise compromise the safety integrity of the E/E/PE safety-related systems, shall be considered for each of the components.

Table A.1 sets out the faults or failures to be detected during operation or to be analysed in the derivation of the safe failure fraction.

If field data is used to support the failure modes and effects analysis it shall be sufficient to support the safety integrity requirements. As a minimum, a statistical single-sided lower confidence limit of at least 70 % is required.

NOTE 6 An example of calculation of diagnostic coverage and safe failure fraction is included in Annex C of IEC 61508-6.

NOTE 7 Alternative methods are available for calculating diagnostic coverage involving, for example, simulation of faults using a computer model containing details of both the circuitry of the E/E/PE safety-related systems and the electronic components used in its design (for example, down to the transistor level in an integrated circuit).

C.2 Determination of diagnostic coverage factors

In the calculation of diagnostic coverage for an element (see C.1) it is necessary to estimate, for each component or group of components, the fraction of dangerous failures that are detected by the diagnostic tests. The diagnostic tests that can contribute to the diagnostic coverage include, but are not limited to:

– comparison checks, for example monitoring and comparison of redundant signals;
– additional built-in test routines, for example checksums on memory;
– test by external stimuli, for example sending a pulsed signal through control paths;
– continuous monitoring of an analogue signal, for example, to detect out of range values indicative of sensor failure.

In order to calculate diagnostic coverage it is necessary to determine those failure modes that are detected by the diagnostic tests. It is possible that open-circuit or short-circuit failures for simple components (resistors, capacitors, transistors) can be detected with a coverage of 100 %. However, for more complex type B elements, see 7.4.4.1.3, account should be taken of the limitations to diagnostic coverage for the various components shown in Table A.1. This analysis shall be carried out for each component, or group of components, of each element and for each element of the E/E/PE safety-related system.

NOTE 1 Tables A.2 to A.14 recommend techniques and measures for diagnostic tests and recommend maximum diagnostic coverage that can be claimed. These tests may operate continuously or periodically (depending on the diagnostic test interval). The tables do not replace any of the requirements of this annex.

NOTE 2 Diagnostic tests can provide significant benefits in the achievement of functional safety of an E/E/PE safety-related system. However, care must be exercised not to unnecessarily increase the complexity which, for example, may lead to increased difficulties in verification, validation, functional safety assessment, and

maintenance and modification activities. Increased complexity may also make it more difficult to maintain the long-term functional safety of the E/E/PE safety-related system.

The calculations to obtain the diagnostic coverage, and the ways it is used, assume that the EUC can operate safely in the presence of an otherwise dangerous fault that is detected by the diagnostic tests. If this assumption is not correct then the E/E/PE safety-related system shall be treated as operating in a high demand or a continuous mode of operation (see 7.4.8.3, 7.4.5.3 and 7.4.5.4).

NOTE 3 The definition of diagnostic coverage is given in 3.8.6 of IEC 61508-4. It is important to note that alternative definitions of the diagnostic coverage are sometimes assumed but these are not applicable within this standard.

NOTE 4 The diagnostic tests used to detect a dangerous failure within an element may be implemented by another element within the E/E/PE safety-related system.

NOTE 5 Diagnostic tests may operate either continuously or periodically, depending on the diagnostic test interval. There may be some cases or times where a diagnostic test should not be run due to the possibility of a test affecting the system state in an adverse manner. In this case, no benefits in the calculations may be claimed from the diagnostic tests.

Annex D
(normative)

Safety manual for compliant items

D.1 General

The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard.

D.2 Contents

D.2.1 The safety manual shall specify the functions of the compliant item. These may be used to support a safety function of a safety-related system or functions in a subsystem or element. The specification should clearly describe both the functions and the input and output interfaces.

For every compliant item, the safety manual shall contain:

a) a functional specification of the functions capable of being performed;

b) identification of the hardware and/or software configuration of the compliant item to enable configuration management of the E/E/PE safety-related system in accordance with 6.2.1 of IEC 61508-1.

c) constraints on the use of the compliant item and/or assumptions on which analysis of the behaviour or failure rates of the item are based.

D.2.2 For every function, the safety manual shall contain:

a) the failure modes of the compliant item (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the function and that are not detected by diagnostics internal to the compliant item;

b) for every failure mode in a), an estimated failure rate;

c) the failure modes of the compliant item (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the function and that are detected by diagnostics internal to the compliant item;

d) the failure modes of the diagnostics, internal to the compliant item (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the diagnostics to detect failures of the function;

e) for every failure mode in c) and d), the estimated failure rate;

f) for every failure mode in c) that is detected by diagnostics internal to the compliant item, the diagnostic test interval;

g) for every failure mode in c) the outputs of the compliant item initiated by the internal diagnostics;

NOTE 1 The outputs of the internal diagnostics could be used to initiate additional measures (technical/procedural) to the E/E/PE safety-related system, subsystem or element to achieve or maintain a safe state of the EUC.

h) any periodic proof test and/or maintenance requirements;

i) for those failure modes, in respect of a specified function, that are capable of being detected by external diagnostics, sufficient information shall be provided to facilitate the development of an external diagnostics capability. The information shall include details of failure modes and for those failure modes the failure rates;

j) the hardware fault tolerance;

k) the classification as type A or type B of that part of the compliant item that provides the function (see 7.4.4.1.2 and 7.4.4.1.3);

NOTE 2 Failure modes can only be classified as being safe or dangerous when the application of the compliant item is known in relation to the hazards of the EUC. For example, if a sensor is applied in such a way that a high output is used to signal a hazard of the EUC (for example high pressure), then a failure mode that prevents the correct indication of the hazard (for example output stuck low) would be classified as dangerous whereas a failure mode that causes the sensor output to go high would be classified as safe. This depends on how the sensor signal is interpreted by the safety-related system logic and so cannot be specified without constraining the way that the sensor is applied.

Also, the level of diagnostic coverage claimed for a compliant item may vary from one application to another depending on the extent of any diagnostics in the system logic or external signal processing that may supplement any internal diagnostics of the compliant item.

It follows that any estimate of the hardware fault tolerance or the safe failure fraction can only be made if constraints are placed on the application of the compliant item. These constraints are outside the control of the supplier of the compliant item. Therefore, no claims shall be made in the safety manual, in respect of the hardware fault tolerance or the safe failure fraction or any other functional safety characteristic that is dependent on knowledge of safe and dangerous failure modes, unless the underlying assumptions, as to what constitute safe and dangerous failure modes, are clearly specified.

D.2.3 For every function of the compliant item that is liable to systematic failure, the manual shall contain:

a) the systematic capability of the compliant item or that part of the element that provides the function;

b) any instructions or constraints relating to the application of the compliant item, relevant to the function, that should be observed in order to prevent systematic failures of the compliant item.

NOTE The systematic safety integrity indicated by the systematic capability can be achieved only when the instructions and constraints are observed. Where violations occur, the claim for systematic capability is partially or wholly invalid.

D.2.4 For additional requirements relating to software compliant items see 7.4.2.12 and Annex D of IEC 61508-3.

Annex E
(normative)

Special architecture requirements for integrated circuits (ICs) with on-chip redundancy

E.1 General

This annex is referenced by 7.4.2.2 b).

To allow the use of on-chip redundancy for ICs with one common semi-conductor substrate, a set of requirements is given below. For safety reasons this approach has a conservative nature, for example it is limited up to SIL 3 and a set of restrictive requirements have been specified. The following requirements are related to digital ICs only. For mixed-mode and analogue ICs no general requirements can be given at the moment. Common cause analysis (see IEC 61508-1, 7.6.2.7) may exclude the use of on-chip redundancy for an individual application. On-chip redundancy as used in this standard means a duplication (or triplication etc.) of functional units to establish a hardware fault tolerance greater than zero. According to 7.4.4.1.1 a) in determining the hardware fault tolerance no account is taken of measures that may control the effects of faults such as diagnostics.

A subsystem with a hardware fault tolerance greater than 0 can be realised using one single IC semi-conductor substrate (on-chip redundancy). In this case all of the following requirements a) to q) shall be fulfilled and the design of the E/E/PE system and the IC shall be such as to meet these requirements. An IC with on-chip redundancy shall have its own compliant item safety manual (see Annex D).

a) The highest safety integrity level that can be claimed for a safety function using an IC as described above is limited to SIL 3.

NOTE 1 At the present state of the art, knowledge and experience, it is not feasible to consider and take measures against all effects related to said element (single IC) to gain sufficient confidence for SIL 4.

b) The systematic capability shall not be increased by combination of elements (see 7.4.3.2).

c) To avoid common cause failure(s), the effects of increasing temperature, for example due to random hardware fault(s), shall be considered. At least one of the measures listed in Table E.2, no. 6 shall be applied. In a design where a local fault can cause a safety critical temperature increase, appropriate measures shall be taken.

NOTE 2 While in a power design a local fault can cause a significant temperature increase, the impact of a local short circuit in a logic circuit can be negligible. Examples to be considered in digital circuits include the device pad area and voltage regulators.

d) Separate physical blocks on substratum of the IC shall be established for each channel and each monitoring element such as a watchdog. The blocks shall include bond wires and pin-out. Each channel shall have its own separated inputs and outputs which shall not be routed through another channel/block.

NOTE 3 This does not exclude internal connections between blocks by wiring between output and input cells of different blocks (see also Table E.1, 3a and 3b).

NOTE 4 Input and outputs include, but are not limited to:

– DFT signals (Design for Testability, e.g. scan chains);
– Clock signals and clock enable signals;
– Power supply;
– Reset signals;
– Configuration and mode selection signals;
– Debug and trace signals.

e) Appropriate measures shall be taken to avoid dangerous failure caused by faults of the power supply including common cause failures.

NOTE 5 Faults of the power supply include, but are not limited to:

– noise;

– disturbance propagation over the power supply lines;

– non-simultaneous power supply switch-on, that may cause effects such as latch-up or high in-rush current;

– excessive current-draw resulting from short circuit.

NOTE 6 This requirement can be fulfilled by applying adequate techniques such as:

– providing each block with its own power supply pins so that no block is supplied via the power supply of another block (for example via internal connections) and not connecting wells of separate physical blocks together inside the IC (see also Table E.2, no. 3);

– incorporation of external measures to avoid dangerous failures that may be caused by different voltages of the wells;

– detecting power supply faults by means of voltage monitors;

– using partially increased voltage tolerance;

– considering IR drop problems for the design of power lines.

f) The minimum distance between boundaries of separate physical blocks shall be sufficient to avoid short circuit and cross talk between these blocks.

NOTE 7 Short circuit typically can be caused by electro migration, via migration, contact migration, local defect gate oxide breakdown, latch-up, etc.

NOTE 8 Cross talk typically can be caused by substrate currents, capacitive coupling, etc.

NOTE 9 The minimum distance should be chosen regarding the relevant design rules with a safety factor typically between 10 and 50.

NOTE 10 Potential rings according to Table E.2 are not considered as being part of a block when estimating the distance between separate physical blocks.

g) Short circuit and/or cross-talk between adjacent lines of separate physical blocks shall not lead to a loss of a safety function or an undetected loss of a monitoring function (Table E.2, no. 5).

h) substratum shall be connected to ground whatever the IC design process used (n-well or p-well);

NOTE 11 For p-wells, this means the use of a negative power supply. Negative logic should be avoided since its use may be susceptible to errors in design.

i) The susceptibility of an IC with on-chip redundancy to common cause failures shall be estimated by determining a β-factor according to E.3. This β-factor called β_{IC} shall be used when estimating the achieved safety integrity of the E/E/PE safety-related system according to 7.4.5.1 and will be used for the IC instead of the β-factor determined for example according to Annex D of IEC 61508-6.

j) The detection of a fault (by diagnostic tests, proof tests or by any other means) in an IC with on-chip redundancy shall result in a specified action to achieve or maintain a safe state.

NOTE 12 This requirement does not apply, if the effects of a fault can be controlled, for example by de-energization of a block.

k) The minimum diagnostic coverage of each channel shall be at least 60 %. Where a monitoring element is implemented only once, the minimum diagnostic coverage for this element shall also be at least 60 %.

l) If it is necessary to implement a watchdog, for example for program sequence monitoring and/or to guarantee the required diagnostic coverage or safe failure fraction one channel shall not be used as a watchdog of another channel, except when functionally diverse channels are used.

m) When testing for electromagnetic compatibility without additional safety margin, the function carried out by the IC shall not be interfered (for example performance criterion A

as described in EMC immunity standards, see for example IEC 61000-6-2 or IEC 61326-3-1).

n) When testing for electromagnetic compatibility with additional safety margins, the safety function (including IC) shall comply with the "FS" criterion as defined in IEC 61326-3-1

o) Appropriate measures shall be taken to avoid dangerous failure caused by oscillations of digital input ports connected to external asynchronous digital signals, e.g. introduction of respective multiple clock synchronization stages.

p) The common cause potential of common resources such as boundary scan circuitries and arrays of special function registers shall be analyzed.

q) The requirements a) to p) list common cause initiators specific to ICs with on-chip redundancy. Other relevant common cause initiators shall be considered as specified in this International Standard.

NOTE 13 In general the above requirements restrict the use of on-chip redundancy to ICs designed with a full-custom or semi-custom approach such as ASICs, microcontrollers or other specialised SoCs (systems on chip). Other designs such as Gate Arrays, FPGAs etc. may not meet all requirements.

Use of ICs with on-chip redundancy as described above shall only be permitted if a full common cause analysis (CCA) has been undertaken. This analysis shall cover the complete range of potential common cause failures arising from design, fabrication, construction, procedural and environmental factors. In particular, the loss of physical separation between channels as a result of the use of ICs with on-chip redundancy shall be subject to special scrutiny. The final SIL level assigned to the E/E/PE safety-related system shall be dependent upon the results of this CCA.

NOTE 14 The use of physical separation (i.e. segregation) of "channels" can provide defence against a wide range of common mode failures in redundant systems.

NOTE 15 The CCA methodology proposed is structured into the following steps:

1. Identify potential common cause initiators (CCI). Consider effects listed in this annex and other foreseeable physical CCI and logical CCI (shared resources and signals).
2. Identify the redundant blocks on the IC which will suffer from CCI amongst them.
3. Qualitatively list and evaluate the safety measures against the individual CCI identified in step 1 for each pair of redundant blocks identified in step 2.
4. Quantitatively answer the Tables E.1 and E.2 for each pair of redundant blocks identified in step 2 and evaluate the specific ß factor.
5. Use the specific ß factors in the probabilistic modelling.

E.2 Additional requirements for SIL 3 on-chip redundancy

For SIL 3 on-chip redundancy the following requirements shall be met in addition to the requirements given in E.1:

a) documented evidence that all application specific environmental conditions are in accordance with that taken into account during specification, analysis, verification and validation shall be provided;

b) external measures that can achieve or maintain a safe state of the E/E/PE system. These measures shall achieve medium effectiveness (see also A.3) as minimum. All measures implemented inside the IC to monitor for effects of systematic and/or common cause failures shall use these external measures to achieve or maintain a safe state of the E/E/PE system.

E.3 β-factor

The susceptibility of the IC with on-chip redundancy to common cause failures shall be estimated by determining the β-factor β_{IC}, which is special to ICs with on-chip redundancy (see also E.1, i)). The estimation shall be based upon the following:

a) a basic β-factor called $\beta_{B\text{-}IC}$ of 33 %;

b) estimation of the increase of the basic β-factor, $\beta_{B\text{-}IC}$, by the design using Table E.1; and

c) estimation of the decrease of the basic β-factor, $\beta_{B\text{-}IC}$, by the design using Table E.2.

β_{IC} is estimated by adding $\beta_{B\text{-}IC}$ and all scores from Table E.1 and afterwards subtracting all scores from Table E.2. The estimated final β_{IC} shall not exceed 25 %.

NOTE 1 This β-factor called β_{IC} will be used when estimating the achieved safety integrity of the E/E/PE safety-related system according to 7.4.5.1 and will be used for the IC instead of the β-factor determined for example according to Annex D of IEC 61508-6.

NOTE 2 A specific analysis of the available failure data for the IC design methodology applied should be undertaken to substantiate that the chosen β-factor is conservative. Only ICs with mature design and implementation processes should be used.

Table E.1 – Techniques and measures that increase $\beta_{B\text{-}IC}$

	Technique/measure	Delta β-factor [%]	Remark
1	Watchdog on-chip used as monitoring element	5	Monitoring elements used for watchdog function and necessary to guarantee the required DC or SFF should be realised external to the IC preferably under the aspect of common cause failures. The use of a watchdog(s) on-chip may result in a higher DC or SFF compared to external realization. See also E.2 b).
2	Monitoring elements on-chip other than watchdog, for example clock monitoring	5	Monitoring elements used for example for clock monitoring and necessary to guarantee the required DC or SFF should be realised external to the IC preferably under the aspect of common cause failures. The use of a monitoring element(s) on-chip may result in a higher DC or SFF compared to external realization.
3a	Internal connections between blocks by wiring between output and input cells of separate physical blocks without cross-over in different layers	2	Comparison of conditions and results between separate physical blocks should be realised external to the IC preferably. Analysis of possible common cause failures including FMEA of stuck-at-faults of internal connections is required. Effects of temperature increase due to faults shall be taken into account in particular. Verification of the layout should be carried out by analysis of the final layout, for example with the help of tools.
3b	Internal connections between blocks by wiring between output and input cells of separate physical blocks with cross-over	4	Comparison of conditions and results between separate physical blocks should be realised external to the IC preferably. Analysis of possible common cause failures including FMEA of stuck-at-faults and short circuit of internal connections is required. Effects of temperature increase due to faults shall be taken into account in particular.
Alternate techniques/measures are indicated by a letter following the number. Only one of the alternate techniques/measures can be selected. Techniques and measures listed in this table are not exhaustive. Other techniques and measures may be used, provided evidence is given to support the claimed delta β-factor. If evidence can be provided that measures were taken to mitigate the impact of common cause failures, other delta β-factors may be used. General advice from Annex D of IEC 61508-6 should be observed in such cases. NOTE The interface signals between the redundant blocks are generally composed of multiple layers. Irrespective of the composition of a signal, whether it is solely constructed with only one metal layer or it is a mix of multiple layers, *the whole interface signal will be considered as a single wire*. To minimise possible interference of both channels by one fault none of the interface signals should cross over with the rest of the interface signals.			

Table E.2 – Techniques and measures that decrease β_{B-IC}

	Technique/measure	Delta β-factor [%]	Remark
1a	Diverse measures to control failures in different channels	4	
1b	Diversity in function and measures to control failures in different channels	6	
2	Testing the E/E/PE system for electromagnetic compatibility with additional safety margin not interfering the function of the E/E/PE system (for example performance criterion A)	5	Performance criterion A is described in EMC immunity standards, see for example IEC 61000-6-2 or IEC 61326-3-1.
3	Providing each block with its own power supply pins so that no block is supplied via the power supply of another block (for example via internal connections) and not connecting wells of separate physical blocks inside the IC	6	External measures have to be taken to avoid dangerous failures that might be caused by different voltages of the wells.
4	Structures that isolate and decouple physical locations	2 - 4	Useful to decouple separate physical blocks.
5	Ground pin between pin-out of separate physical blocks	2	If not implemented, short circuit between adjacent lines of separate physical blocks shall be carried out to test for effects of tear-off of bond wiring (see also E.1, g)). The β-factor will not be decreased in this case.
6a	High diagnostic coverage (DC ≥ 99 %) of each channel, failure detection by the technical process and achievement of safe state in adequate short time	7	May be appropriate only in exceptional case.
6b	Temperature sensors between blocks with permanent shut-down (internal or external) to safe state in adequate short time; low effectiveness without diagnostics	2	See also Table A.18, measures against temperature increase.
6c	Temperature sensors between blocks with permanent shut-down (internal or external) to safe state in adequate short time; high effectiveness with diagnostics	9	See also Table A.18, measures against temperature increase.
6d	Analysis/test of the effects of faults (for example increase of temperature). Depending on the result of the analysis/test, comparison between channels, including fault detection and achievement of safe state in adequate short time can be required	9	
6e	Design of the monitoring circuit functional at the increased temperature	7	The design of the monitoring function (e.g. watch dog) shall carry out the safety function under worst case temperature conditions.
Alternate techniques/measures are indicated by a letter following the number. Only one of the alternate techniques/measures can be selected. Techniques and measures listed in this table are not exhaustive. Other techniques and measures may be used, provided evidence is given to support the claimed delta β-factor. NOTE Techniques/measures 6a to 6e aim for controlling effects of temperature rise due to failure.			

Annex F
(informative)

Techniques and measures for ASICs – avoidance of systematic failures

F.1 General

For the design of Application Specific Integrated Circuits (ASICs) the following techniques and measures for the avoidance of failures during the ASIC-development should be applied.

NOTE 1 This informative annex is referenced by 7.4.6.7.

NOTE 2 The following techniques and measures are related to digital ASICs and user programmable ICs only. For mixed-mode and analogue ASICs no general techniques and measures can be given at the moment.

a) All design activities and test arrangements, and tools used for the functional simulation and the results of the simulation, should be documented.

b) All tools, libraries and manufacturing procedures should be proven in use. This includes:

- application of the individual tool (including different versions with equivalent features) over a substantial period of time in projects of similar or greater complexity;

NOTE 3 A substantial period of time might be 2 years in this case.

- application of common or widely used tools to ensure that information about possible bugs and restrictions is known for the given tool and/or the given version, which should be considered during use. Version control and monitoring should be carried out by the manufacturers to track existing faults;
- internal consistency and plausibility checks to avoid faults in the different databases created by different tools.

NOTE 4 User training is very important because of the rapid changes and progress in this field.

c) All activities and their results should be verified, for example by simulation, equivalence checks, timing analysis or checking the technology constraints.

d) Measures for the reproducibility and automation of the design implementation process (script based, automated work and design implementation flow) should be used.

e) For 3rd party soft-cores and hard-cores, only validated macro blocks should be used and these should comply with all constraints and proceedings defined by the macro core provider if practicable. Unless already proven in use, each macro block should be treated as newly written code, for example it should be fully validated.

f) For the design, a problem-oriented and abstract high-level design methodology and design description language should be used.

NOTE 5 The design description should use a hardware description language like VHDL or Verilog. This is the most common hardware description methodology used today in ASIC design. Both languages are defined by IEEE standards and are assumed to satisfy the recommendations for high level programming languages. The hardware description language may be used both for design description and for functional models or test benches. When used for design description, only a subset of the language may be used; this synthesisable code is often referred to as RTL (register transfer level) code. Non synthesisable code, adequate for functional models and test benches is called behavioural code.

g) Adequate testability (for manufacturing test of the full and semi-custom ASIC) should be achieved.

h) Gate and interconnection (wire) delays should be considered during test and ASIC verification steps.

i) Internal gates with tristate outputs should be avoided. If internal tristate outputs are used these outputs should be equipped with pull-ups/downs or bus-holders.

j) Before manufacturing, an adequate verification of the complete ASIC (i.e., including each verification step carried out during design and implementation to ensure correct module and chip functionality) should be carried out.

NOTE 6 The adequacy of ASIC verification depends on the test complexity of the element and the required safety integrity level.

F.2 Guidelines: Techniques and measures

An appropriate group of techniques and measures that are essential to prevent the introduction of faults during the design and development of ASICs should be used. Depending upon the technical realisation, a differentiation between full and semi-custom digital ASICs and user programmable ICs (FPGA/PLD/CPLD) is necessary. Techniques and measures that support the achievement of relevant properties are defined in Table F.1 for full and semi custom ASICs and in Table F.2 for user programmable ICs. The related ASIC development lifecycle is shown in Figure 3.

In Tables F.1 and F2 recommendations are made by safety integrity level, stating firstly the importance of the technique or measure and secondly the effectiveness recommended if it is used. The importance is signified as follows:

– HR*: the technique or measure is highly recommended for this safety integrity level. No design should exclude this technique or measure;
– HR: the technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used, then the rationale behind not using it should be detailed;
– R: the technique or measure is recommended for this safety integrity level. If this technique or measure is not used or none of possible alternatives is used, then the rationale behind not using it should be detailed;
– -: the technique or measure has no recommendation for or against being used;
– NR: the technique or measure is positively not recommended for this safety integrity level. If this technique or measure is used, then the rationale behind using it should be detailed;

The recommended effectiveness is signified as follows.

– Low: if used, the technique or measure should be used to the extent necessary to give at least low effectiveness against systematic failures;
– Medium: if used, the technique or measure should be used to the extent necessary to give at least medium effectiveness against systematic failures;
– High: the technique or measure should be used to the extent necessary to give high effectiveness against systematic failures.

Following the guidelines in this annex does not guarantee by itself the required safety integrity. It is important to consider:

– the consistency of the chosen techniques and measures, and how well they will complement each other;
– which techniques and measures are appropriate, for every phase of the development lifecycle; and
– which techniques and measures are most appropriate for the specific problems encountered during the development of each different E/E/PE safety-related system.

Table F.1 – Techniques and measures to avoid introducing faults during ASIC's design and development – full and semi-custom digital ASICs (see 7.4.6.7)

Design phase	Ref	Technique/Measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Design entry	1	Structured description	E.3	HR high	HR high	HR* high	HR* high
	2	Design description in (V)HDL (see Note)	E.1	HR high	HR high	HR* high	HR* high
	3	Schematic entry	E.2	NR	NR	NR	NR
	4	(V)HDL simulation (see Note)	E.5	HR high	HR high	HR* high	HR* high
	5	Application of proven in use (V)HDL simulators (see Note)	E.4	HR high	HR high	HR* high	HR* high
	6	Functional test on module level (using for example (V)HDL test benches) (see Note)	E.6	HR high	HR high	HR* high	HR* high
	7	Functional test on top level	E.7	HR high	HR high	HR* high	HR* high
	8	Functional test embedded in system environment	E.8	R medium	R medium	HR high	HR high
	9	Restricted use of asynchronous constructs	E.9	HR high	HR high	HR* high	HR* high
	10	Synchronisation of primary inputs and control of metastability	E.10	HR high	HR high	HR* high	HR* high
	11	Design for testability (depending on the test coverage in percent)	E.11	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	12	Modularisation	E.12	R medium	R medium	HR high	HR high
	13	Coverage of the verification scenarios	E.13	R medium	R medium	HR high	HR high
	14	Observation of coding guidelines	E.14	HR high	HR high	HR* high	HR* high
	15	Application of code checker	E.15	R	R	R	R
	16	Defensive programming	E.16	R low	R medium	HR high	HR* high
	17	Documentation of simulation results	E.17	HR low	HR medium	HR high	HR* high
	18a	Code inspection	E.18	R medium	R high	HR high	HR* high
	18b	Walk-through	E.19	R medium	R high	HR high	HR* high
	19a	Application of validated soft-cores	E.20	R medium	R high	HR* high	HR* high
	19b	Validation of soft-cores	E.21	R medium	R high	HR* high	HR* high

Table F.1 *(continued)*

Design phase	Ref	Technique/Measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Synthesis	20a	Simulation of the gate netlist to check timing constraints	E.22	R medium	R medium	R high	R high
	20b	Static analysis of the propagation delay (STA)	E.23	R medium	R medium	R high	R high
	21a	Verification of the gate netlist against a reference model by simulation	E.24	R medium	R medium	HR high	HR high
	21b	Comparison of the gate netlist with the reference model (formal equivalence check)	E.25	R medium	R medium	HR high	HR high
	22	Check of ASIC vendor requirements and constraints	E.26	HR high	HR high	HR* high	HR* high
	23	Documentation of synthesis constraints, results and tools	E.27	HR high	HR high	HR* high	HR* high
	24	Application of proven in use synthesis tools	E.28	HR* high	HR* high	HR* high	HR* high
	25	Application of proven in use target libraries	E.29	HR* high	HR* high	HR* high	HR* high
	26	Script based procedures	E.30	R medium	R medium	HR high	HR high
Test insertion and test pattern generation	27	Implementation of test structures	E.31	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	28a	Estimation of the test coverage by simulation (based on achieved test coverage in percent)	E.32	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	28b	Estimation of the test coverage by application of ATPG tool (based on achieved test coverage in percent)	E.33	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	29a	Simulation of the gate netlist, to check timing constraints	E.22	R medium	R medium	HR high	HR high
	29b	Static analysis of the propagation delay (STA)	E.23	R medium	R medium	HR high	HR high
	30a	Verification of the gate netlist against a reference model by simulation	E.24	R medium	R medium	HR high	HR high
	30b	Comparison of the gate netlist with the reference model (formal equivalence check)	E.25	R medium	R medium	HR high	HR high

Table F.1 *(continued)*

Design phase	Ref	Technique/Measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Placement, routing, layout generation	31a	Justification of proven in use for applied hard cores	E.34	HR high	HR high	HR* high	HR* high
	31b	Application of validated hard cores	E.35	HR high	HR high	HR* high	HR* high
	31c	Online testing of hard cores	E.36	HR high	HR high	HR* high	HR* high
	32a	Simulation of the gate netlist, to check timing constraints	E.22	HR high	HR high	HR* high	HR* high
	32b	Static analysis of the propagation delay (STA)	E.23	HR high	HR high	HR* high	HR* high
	33a	Verification of the gate netlist against a reference model by simulation	E.24	HR high	HR high	HR* high	HR* high
	33b	Comparison of the gate netlist with the reference model (formal equivalence check)	E.25	HR high	HR high	HR* high	HR* high
	34	Design rule check (DRC)	E.37	HR high	HR high	HR high	HR* high
	35	Verification of layout versus schematic (LVS)	E.38	HR high	HR high	HR high	HR* high
	36	Application of a proven in use design environments, application of proven in use cell libraries	E.4	HR* high	HR* high	HR* high	HR* high
	37	Additional slack (>20 %) for process technologies in use for less than 3 years	E.39	HR high	HR high	HR high	HR* high
Chip manu-facturing	38	Application of a proven in use process technology		HR high	HR high	HR* high	HR* high
	39	Proven in use manufacturing process	E.42	HR low	HR medium	HR high	HR* high
	40	Quality assurance for the process technology		HR high	HR high	HR high	HR* high
	41	Quality control of the manufacturing process	E.43	HR high	HR high	HR high	HR* high
	42	Manufacturing quality pass of the device	E.44	R low	R medium	HR high	HR* high
	43	Functional quality pass of the device	E.45	HR high	HR high	HR* high	HR* high
	44	Test coverage of the manufacturing test		> 95 %	> 98 %	> 99 %	> 99 %
	45	Quality standards	E.46	HR low	HR medium	HR high	HR* high
	46	Quality management, for example according to ISO 9000		HR high	HR high	HR high	HR* high
	47	Burn-in test	E.40	R low	R medium	HR high	HR* high

Appropriate techniques/measures should be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. At least one of the alternate or equivalent techniques/measures should be applied.

NOTE The term (V)HDL denotes either the Very high speed integrated circuit Hardware Description Language (VHDL) or Verilog Hardware Description Language.

Table F.2 – Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD) (see 7.4.6.7)

Design phase	Ref	Technique/Measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Design entry	1	Structured description	E.3	HR high	HR high	HR* high	HR* high
	2	Design description in (V)HDL (see Note)	E.1	HR high	HR high	HR* high	HR* high
	3	Schematic entry	E.2	– high	– high	NR	NR
	4	Design description using boolean equations		R high	R high	NR	NR
	5a	For circuit descriptions that use boolean equations: manual inspection in designs with limited (low) complexity		HR high	HR high	HR* high	HR* high
	5b	For circuit descriptions that use boolean equations: simulation of state transitions in designs with higher complexity		HR high	HR high	HR* high	HR* high
	6	Application of a proven in use design environment	E.4	HR high	HR high	HR* high	HR* high
	7	Application of proven in use (V)HDL simulators (see Note)	E.4	HR high	HR high	HR* high	HR* high
	8	Functional test on module level (using for example (V)HDL test benches) (see Note)	E.6	HR high	HR high	HR* high	HR* high
	9	Restricted use of asynchronous constructs	E.9	HR high	HR high	HR* high	HR* high
	10	Design for testability (depending on the test coverage in percent)	E.11	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	11	Modularisation	E.12	R medium	R medium	HR high	HR high
	12	Coverage of the verification scenarios (test benches)	E.13	R medium	R medium	HR high	HR high
	13	Observation of coding guidelines	E.14	HR high	HR high	HR* high	HR* high
	14	Documentation of simulation results	E.17	HR low	HR medium	HR high	HR* high
	15a	Code inspection	E.18	R medium	R high	HR high	HR* high
	15b	Walk-through	E.19	R medium	R high	HR high	HR* high
	16a	Application of validated soft-cores	E.20	R medium	R high	HR high	HR* high
	16b	Validation of soft-cores	E.21	R medium	R high	HR* high	HR* high

Table F.2 *(continued)*

Design phase	Ref	Technique/Measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Synthesis	17	Internal consistency checks (see for example IEC 61508-7, E.4)		HR high	HR high	HR* high	HR* high
	18a	Simulation of the gate netlist, to check timing constraints	E.22	R medium	R medium	R high	R high
	18b	Static analysis of the propagation delay (STA)	E.23	R medium	R medium	R high	R high
	19a	Verification of the gate netlist against a reference model by simulation	E.24	R medium	R medium	HR high	HR high
	19b	Comparison of the gate netlist with the reference model (formal equivalence check)	E.25	R medium	R medium	HR high	HR high
	20	For PLD/CPLD in complex designs: check of the design by simulation		R medium	R medium	HR high	HR high
	21	Check of IC vendor requirements and constraints	E.26	HR high	HR high	HR* high	HR* high
	22	Documentation of synthesis constraints, results and tools	E.27	HR high	HR high	HR* high	HR* high
	23	Application of proven in use synthesis tools	E.28	HR high	HR high	HR* high	HR* high
	24	Application of proven in use libraries/CPLD technologies	E.29	HR high	HR high	HR* high	HR* high
	25	Script based procedure	E.30	R high	R high	HR high	HR* high
Placement, routing, layout generation	26a	Justification of proven in use for applied hard cores	E.34	HR high	HR high	HR* high	HR* high
	26b	Application of validated hard cores	E.35	HR high	HR high	HR* high	HR* high
	26c	Online testing of hard cores	E.36	HR high	HR high	HR* high	HR* high
	27a	Simulation of the gate netlist, to check timing constraints	E.22	HR high	HR high	HR* high	HR* high
	27b	Static analysis of the propagation delay (STA)	E.23	HR high	HR high	HR* high	HR* high
	28a	Verification of the gate netlist against a reference model by simulation	E.24	HR high	HR high	HR* high	HR* high
	28b	Comparison of the gate netlist with the reference model (formal equivalence check)	E.25	HR high	HR high	HR* high	HR* high
	29	Design rule check (DRC)	E.37	HR high	HR high	HR high	HR* high
	30	Application of a proven in use design environments, application of proven in use cell libraries	E.4	HR* high	HR* high	HR* high	HR* high
	31	Additional slack (>20 %) for process technologies in use for less than 3 years	E.39	HR high	HR high	HR* high	HR* high

Table F.2 *(continued)*

Design phase	Ref	Technique/Measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Manu-facturing	32	Application of a proven in use process technology		HR high	HR high	HR* high	HR* high
	33	Application of proven in use device-series	E.41	HR high	HR high	HR* high	HR* high
	34	Proven in use manufacturing process	E.42	HR low	HR medium	HR high	HR* high
	35	Quality control of the manufacturing process	E.43	HR high	HR high	HR high	HR* high
	36	Manufacturing quality pass of the device	E.44	R low	R medium	HR high	HR* high
	37	Functional quality pass of the device	E.45	HR high	HR high	HR* high	HR* high
	38	Quality standards	E.46	HR low	HR medium	HR high	HR* high
	39	Quality management, for example according to ISO 9000		HR high	HR high	HR high	HR* high
	40	Final verification and validation of the FPGA/PLD prototype in the system		HR high	HR high	HR* high	HR* high
	41	Final verification and validation during mass manufacturing, per-unit-check		R high	R high	HR* high	HR* high
	42	Burn-in test	E.40	R low	R low	R medium	HR* high

Appropriate techniques/measures should be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. At least one of the alternate or equivalent techniques/measures should be applied.

NOTE The term (V)HDL denotes either the Very high speed integrated circuit Hardware Description Language (VHDL) or Verilog Hardware Description Language.

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 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

[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 60601 (all parts), *Medical electrical equipment*

[7] IEC 61165, *Application of Markov techniques*

[8] IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

[9] IEC 61164, *Reliability growth – Statistical test and estimation methods*

[10] IEC 62308, *Equipment reliability – Reliability assessment methods*

[11] IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

[12] ISO 14224, *Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data for equipment*

[13] IEC 60050-191, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

[14] ISO 9000*, Quality management systems – Fundamentals and vocabulary*

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

[16] IEEE 352:1987, *IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 2: Exigences pour les systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité

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 61508-2 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 2000 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/549/FDIS	65A/573/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 le concept initial, 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,

– 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 2: Exigences pour les systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité

1 Domaine d'application

1.1 La présente partie de la série CEI 61508

a) est destinée à être utilisée uniquement après avoir assimilé sans ambiguïté la CEI 61508-1 qui fournit le cadre global permettant d'obtenir la sécurité fonctionnelle;

b) s'applique à tout système relatif à la sécurité tel que défini dans la CEI 61508-1, qui contient au moins un composant à base électrique, électronique ou électronique programmable;

c) s'applique à tous les éléments d'un système E/E/PE relatif à la sécurité (y compris les capteurs, les actionneurs et l'interface opérateur);

d) spécifie la manière d'affiner la spécification des exigences de sécurité des systèmes E/E/PE, développée conformément à la CEI 61508-1 (comprenant la spécification des exigences relatives aux fonctions de sécurité des systèmes E/E/PE et la spécification des exigences d'intégrité de sécurité de ces systèmes), dans le cadre de la spécification des exigences de conception des systèmes E/E/PE;

e) spécifie les exigences pour des activités qui doivent être appliquées pendant la conception et la fabrication des systèmes E/E/PE relatifs à la sécurité (ce qui signifie qu'elle établit le modèle du cycle de vie de sécurité des systèmes E/E/PE), à l'exception du logiciel qui est traité dans la CEI 61508-3 (voir Figures 2 à 4). Ces exigences comprennent l'application de techniques et de mesures qui sont classées en fonction du niveau d'intégrité de sécurité pour éviter et maîtriser les anomalies et défaillances;

f) spécifie les informations nécessaires à l'installation, à la mise en service et à la validation finale de la sécurité des systèmes E/E/PE relatifs à la sécurité;

g) ne s'applique pas à la phase d'exploitation et de maintenance des systèmes E/E/PE relatifs à la sécurité - celle-ci étant traitée dans la CEI 61508-1 - cependant, la CEI 61508-2 fournit des exigences relatives à la préparation des informations et procédures nécessaires à l'utilisateur pour l'exploitation et la maintenance des systèmes E/E/PE relatifs à la sécurité;

h) spécifie les exigences auxquelles doit satisfaire l'entité qui effectue une modification des systèmes E/E/PE relatifs à la sécurité;

NOTE 1 Cette partie de la CEI 61508 est principalement destinée aux fournisseurs et/ou aux services techniques internes des entreprises. Ceci est la raison pour laquelle elle comprend des exigences applicables en matière de modification.

NOTE 2 La Figure 4 montre la relation entre la CEI 61508-2 et la CEI 61508-3.

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

1.2 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.

1.3 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.

NOTE La sécurité fonctionnelle d'un système E/E/PE relatif à la sécurité ne peut être réalisée que lorsque toutes les exigences pertinentes sont satisfaites. En conséquence, il est important d'accorder une attention toute particulière aux exigences associées et de les référencer de façon appropriée.

1.4 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-4 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité. L'Annexe A de la CEI 61508-6 décrit l'application des CEI 61508-2 et 61508-3.

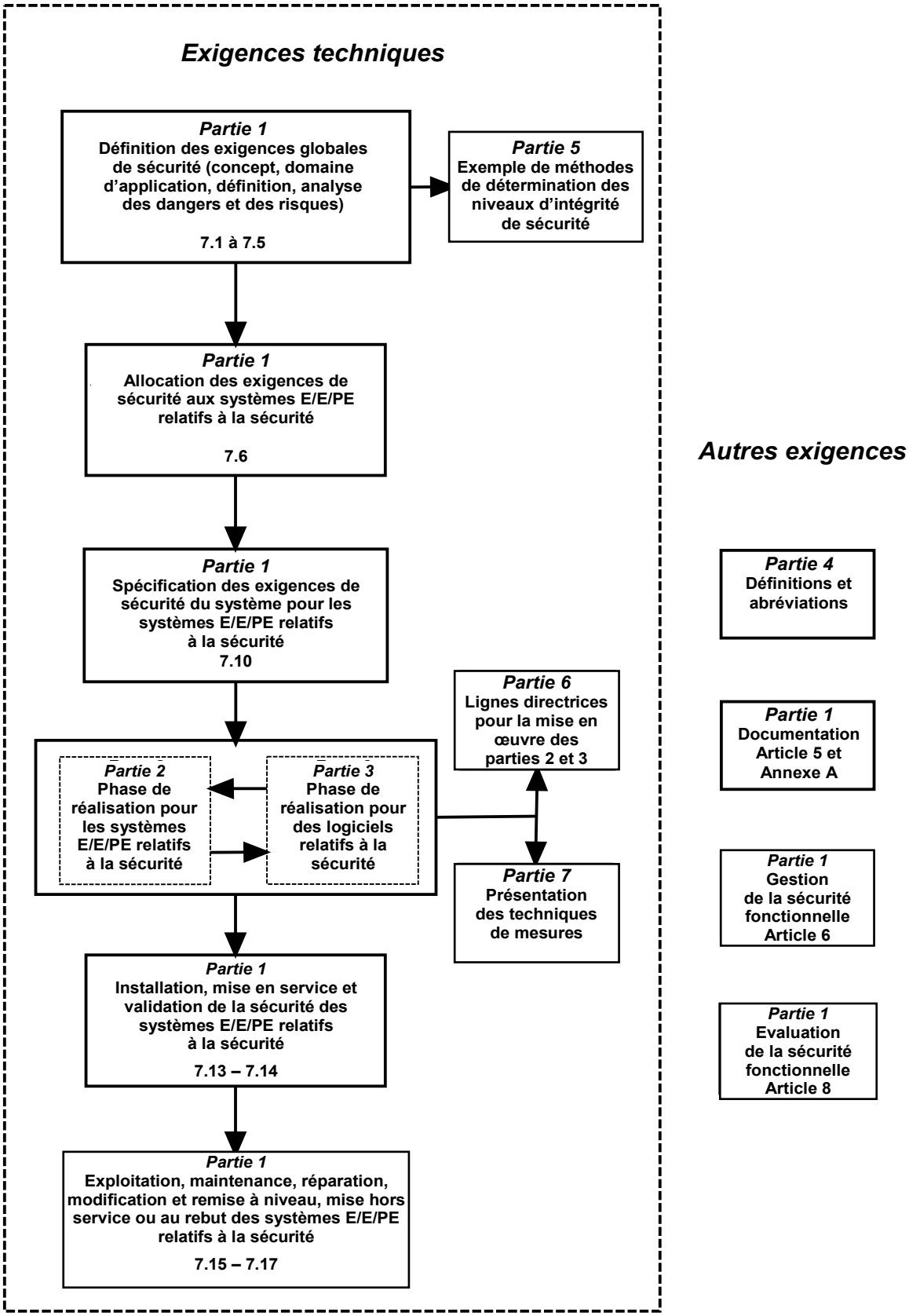


Figure 1 – Structure générale de la série CEI 61508

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 60947-5-1, *Appareillage à basse tension – Partie 5-1: Appareils et éléments de commutation pour circuits de commande – Appareils électromécaniques pour circuits de commande*

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)

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*

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

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*

CEI 61508-7 : 2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

CEI 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible en anglais seulement)

CEI 62280-1, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

CEI 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts*

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*

EN 50205, *Relais de tout ou rien à contacts guidés (liés)*

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

Les exigences concernant la conformité à la présente norme sont détaillées à l'Article 4 de la CEI 61508-1.

5 Documentation

Les exigences concernant la documentation sont détaillées à l'Article 5 de la CEI 61508-1.

6 Gestion de la sécurité fonctionnelle

Les exigences concernant la gestion de la sécurité fonctionnelle sont détaillées à l'Article 6 de la CEI 61508-1.

7 Exigences concernant le cycle de vie de sécurité des systèmes E/E/PE

7.1 Généralités

7.1.1 Objectifs et exigences – généralités

7.1.1.1 Le présent paragraphe établit les objectifs et les exigences pour les phases du cycle de vie de sécurité des systèmes E/E/PE.

NOTE La CEI 61508-1 donne les objectifs et les exigences du cycle de vie de sécurité global, ainsi qu'une introduction générale à la structure de la norme.

7.1.1.2 Pour toutes les phases du cycle de vie de sécurité des systèmes E/E/PE, le Tableau 1 indique

- les objectifs à atteindre;
- le domaine d'application de la phase;
- une référence au paragraphe qui contient les exigences;
- les données d'entrée requises de la phase;
- les résultats requis pour satisfaire aux exigences du paragraphe concerné.

7.1.2 Objectifs

7.1.2.1 Le premier objectif des exigences du présent paragraphe est de structurer de manière systématique les phases du cycle de vie de sécurité des systèmes E/E/PE qui doivent être prises en compte afin d'obtenir la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité.

7.1.2.2 Le second objectif des exigences du présent paragraphe est de recenser toutes les informations concernant la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité sur l'ensemble du cycle de vie de sécurité de ces systèmes.

7.1.3 Exigences

7.1.3.1 Le cycle de vie de sécurité des systèmes E/E/PE qui doit être utilisé pour la déclaration de conformité à la présente norme est celui spécifié à la Figure 2. Un modèle en V

détaillé du cycle de vie de développement ASIC pour la conception des circuits du même nom (voir CEI 61508-4, 3.2.15) est présenté à la Figure 3. Si un autre cycle de vie de sécurité des systèmes E/E/PE ou de développement d'un ASIC est utilisé, il doit être spécifié comme partie intégrante de la gestion des activités liées à la sécurité fonctionnelle (voir Article 6 de la CEI 61508-1), tous les objectifs et toutes les exigences de chaque paragraphe de la CEI 61508-2 devant par ailleurs être satisfaits.

NOTE 1 Les relations entre la CEI 61508-2 et la CEI 61508-3, ainsi que leur domaine d'application respectif, sont illustrés à la Figure 4

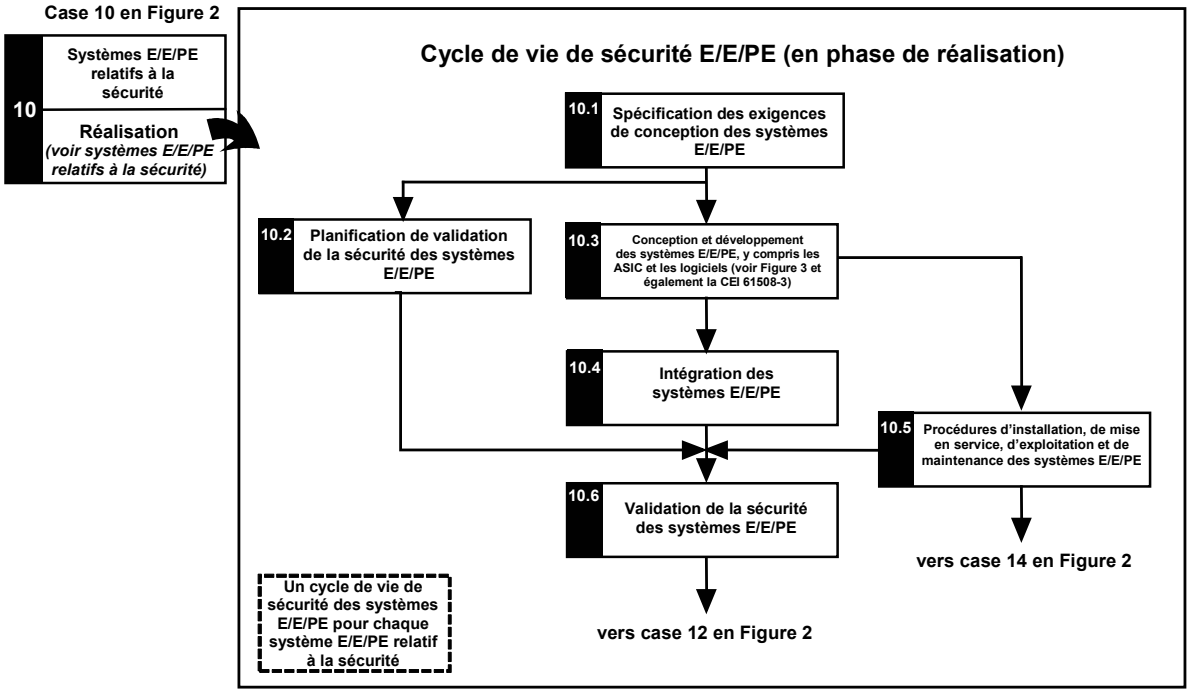
NOTE 2 Il existe des similitudes importantes entre les processus de conception des circuits intégrés (ASIC) et des logiciels. La CEI 61508-3 recommande le modèle en V pour la conception des logiciels de sécurité. Le modèle en V requiert un processus de conception à structure clairement établie et une structure logicielle modulaire, de manière à éviter ou maîtriser les anomalies systématiques. Le cycle de vie de développement des ASIC appliqué à la conception de ces derniers, et illustré à la Figure 3, suit ce modèle. Dans la première étape, les exigences relatives à la spécification des ASIC sont déduites des exigences relatives aux systèmes. L'architecture et la conception des ASIC, ainsi que le calcul du module suivent. Les résultats de chaque étape de la partie gauche du V constituent l'entrée de l'étape suivante, et sont également intégrés à l'étape précédente pour itération le cas échéant, jusqu'à la génération du code définitif. Ce code est vérifié par rapport à la conception correspondante par le biais d'une simulation après réalisation de la topologie, d'essais de module et d'intégration du module, ainsi que de la vérification des ASIC complets. Les résultats de toute étape peuvent nécessiter une révision de l'une quelconque des étapes précédentes. Enfin, l'ASIC est validé après son intégration dans le système E/E/PE relatif à la sécurité.

7.1.3.2 Les procédures de gestion de la sécurité fonctionnelle (voir Article 6 de la CEI 61508-1) doivent être exécutées parallèlement aux phases du cycle de vie de sécurité du système E/E/PE.

7.1.3.3 Chaque phase du cycle de vie de sécurité du système E/E/PE doit être divisée en activités élémentaires avec, pour chaque phase, la spécification du domaine d'application, des entrées et des sorties (voir Tableau 1).

7.1.3.4 A moins que cela ne soit justifié comme partie intégrante de la gestion des activités liées à la sécurité fonctionnelle (voir Article 6 de la CEI 61508-1), les résultats de chaque phase du cycle de vie de sécurité du système E/E/PE doivent être documentés (voir Article 5 de la CEI 61508-1).

7.1.3.5 Les résultats de chaque phase du cycle de vie de sécurité du système E/E/PE doivent satisfaire aux objectifs et exigences spécifiés pour chaque phase (voir 7.2 à 7.9).



NOTE 1 Voir également la CEI 61508-6; A.2 b).

NOTE 2 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 de la CEI 61508-1).

Figure 2 – Cycle de vie de sécurité du système E/E/PE (en phase de réalisation)

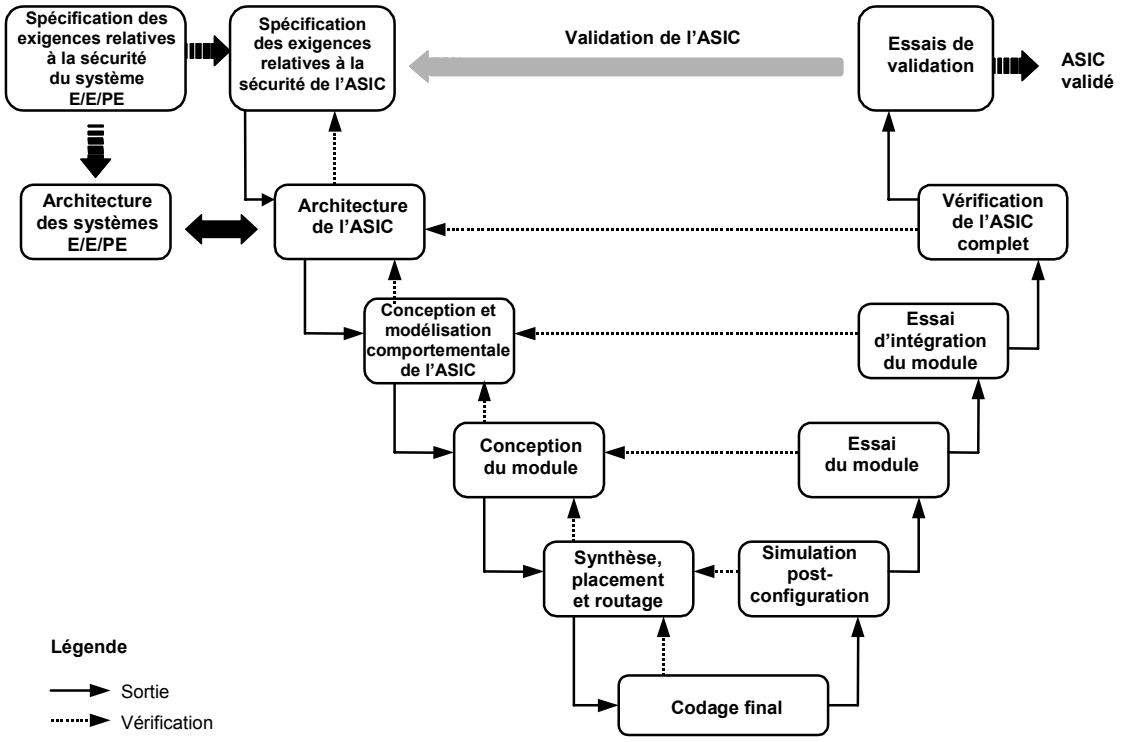


Figure 3 – Cycle de vie de développement d'un ASIC (modèle en V)

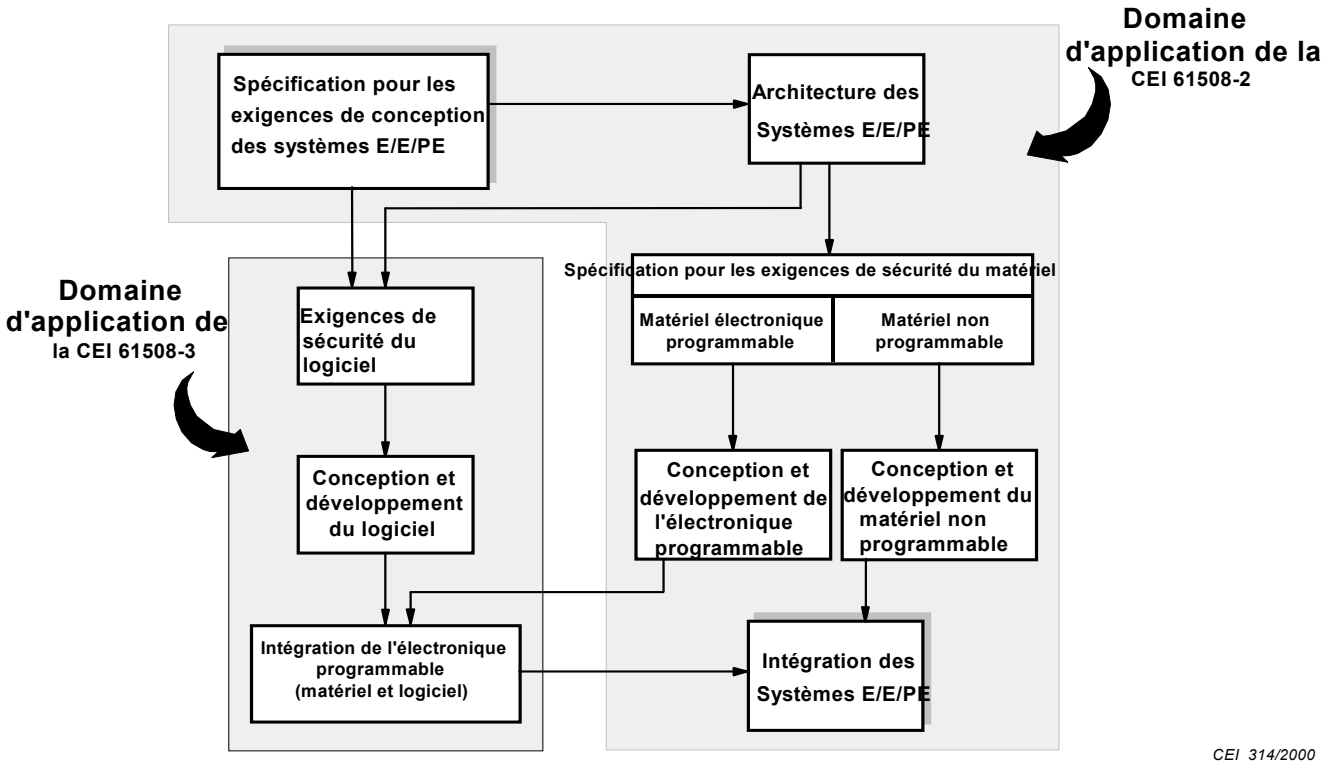


Figure 4 – Relation et domaine d'application pour la CEI 61508-2 et la CEI 61508-3

Tableau 1 – Présentation – Phase de réalisation du cycle de vie de sécurité du système E/E/PE

Phase ou activité du cycle de vie de sécurité		Objectifs	Domaine d'appli-cation	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	Titre					
10.1	Spécification des exigences de conception des systèmes E/E/PE	Spécifier les exigences de conception pour chaque système E/E/PE relatif à la sécurité, en termes des sous-systèmes et des éléments constitutifs (voir 7.10.2 de la CEI 61508-1)	Système E/E/PE relatif à la sécurité	7.2.2	Spécification des exigences de sécurité relatives aux systèmes E/E/PE (voir CEI 61508-1, 7.10)	Spécification des exigences de conception des systèmes E/E/PE, décrivant les équipements et les architectures de ces derniers
10.2	Planification de la validation de la sécurité des systèmes E/E/PE	Planifier la validation de la sécurité du système E/E/PE relatif à la sécurité	Système E/E/PE relatif à la sécurité	7.3.2	Spécifications des exigences de sécurité et de conception des systèmes E/E/PE relatifs à la sécurité	Plan de validation de la sécurité des systèmes E/E/PE relatifs à la sécurité
10.3	Conception et développement des systèmes E/E/PE, y compris les ASIC et les logiciels (Voir Figure 3 & également CEI 61508-3)	Concevoir et développer le système E/E/PE relatif à la sécurité (y compris les ASIC le cas échéant) afin de satisfaire à la spécification des exigences de conception du système (par rapport aux exigences relatives aux fonctions de sécurité et à l'intégrité de sécurité (voir 7.2))	Système E/E/PE relatif à la sécurité	7.4.2 à 7.4.11	Spécification des exigences de conception des systèmes E/E/PE	Conception des systèmes E/E/PE relatifs à la sécurité en conformité avec la spécification des exigences de conception de ces systèmes Plan pour l'essai d'intégration des systèmes E/E/PE Information architecturale des systèmes PE comme élément d'entrée de la spécification des exigences relatives au logiciel
10.4	Intégration des systèmes E/E/PE	Intégrer et soumettre à l'essai le système E/E/PE relatif à la sécurité	Système E/E/PE relatif à la sécurité	7.5.2	Conception des systèmes E/E/PE Plan pour l'essai d'intégration des systèmes E/E/PE Matériels et logiciels de l'électronique programmable	Systèmes E/E/PE relatifs à la sécurité totalement opérationnels en conformité avec la conception de ces systèmes Résultats des essais d'intégration des systèmes E/E/PE
10.5	Procédures d'installation, de mise en service, d'exploitation et de maintenance des systèmes E/E/PE	Développer des procédures permettant d'assurer que la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité est maintenue pendant l'exploitation et la maintenance	Système E/E/PE relatif à la sécurité EUC	7.6.2	Spécification des exigences de conception des systèmes E/E/PE Conception des systèmes E/E/PE	Procédures d'installation, de mise en service, d'exploitation et de maintenance pour chaque système E/E/PE individuel

Tableau 1 *(suite)*

Phase ou activité du cycle de vie de sécurité		Objectifs	Domaine d'appli-cation	Paragraphe contenant les exigences	Entrées	Sorties
Numéro de case de la Figure 2	Titre					
10.6	Validation de la sécurité des systèmes E/E/PE	Valider la conformité, à tous égards, des systèmes E/E/PE relatifs à la sécurité aux exigences de sécurité, en termes de fonctions de sécurité et d'intégrité de sécurité requises	Système E/E/PE relatif à la sécurité	7.7.2	Spécifications des exigences de sécurité et de conception des systèmes E/E/PE relatifs à la sécurité Plan de validation de la sécurité des systèmes E/E/PE relatifs à la sécurité	Systèmes E/E/PE relatifs à la sécurité soumis à une validation complète de la sécurité Résultats de la validation de la sécurité des systèmes E/E/PE
–	Modification des systèmes E/E/PE	Effectuer des corrections, des améliorations ou des adaptations au système E/E/PE relatif à la sécurité, afin d'assurer la réalisation et le maintien de l'intégrité de sécurité requise	Système E/E/PE relatif à la sécurité	7.8.2	Spécification des exigences de conception des systèmes E/E/PE	Résultats de la modification des systèmes E/E/PE
–	Vérification des systèmes E/E/PE	Soumettre à l'essai et évaluer les résultats d'une phase donnée pour assurer le caractère correct et la cohérence des résultats par rapport aux produits et normes fournis comme données pour cette phase	Système E/E/PE relatif à la sécurité	7.9.2	Comme décrit ci-dessus – dépend de la phase Plan de vérification des systèmes E/E/PE relatifs à la sécurité pour chaque phase	Comme décrit ci–dessus – dépend de la phase Résultats de la vérification des systèmes E/E/PE relatifs à la sécurité pour chaque phase
–	Evaluation de la sécurité fonctionnelle des systèmes E/E/PE	Enquêter et élaborer un jugement sur la sécurité fonctionnelle obtenue par le système E/E/PE relatif à la sécurité	Système E/E/PE relatif à la sécurité	8	Plan pour l'évaluation de la sécurité fonctionnelle des systèmes E/E/PE	Résultats de l'évaluation de la sécurité fonctionnelle des systèmes E/E/PE

7.2 Spécification des exigences de conception des systèmes E/E/PE

NOTE Cette phase correspond à la case 10.1 de la Figure 2.

7.2.1 Objectif

L'objectif des exigences du présent paragraphe est de spécifier les exigences de conception pour chaque système E/E/PE relatif à la sécurité, en termes des sous-systèmes et des éléments constitutifs.

NOTE La spécification des exigences de conception des systèmes E/E/PE est normalement déduite de la spécification des exigences de sécurité des systèmes E/E/PE, par une décomposition des fonctions de sécurité et une attribution des éléments constitutifs de la fonction de sécurité aux sous-systèmes (par exemple groupes de capteurs, unités logiques ou actionneurs). Les exigences relatives aux sous-systèmes peuvent être incluses dans la spécification des exigences de conception des systèmes E/E/PE ou peuvent être définies séparément et référencées sur la base de la spécification des exigences de conception de ces systèmes. Les sous-systèmes peuvent être également décomposés en éléments et architectures afin de satisfaire aux exigences de conception et développement définies en 7.4. Les exigences pour ces éléments peuvent être intégrées aux exigences relatives aux sous-systèmes ou peuvent être définies séparément et référencées sur la base des exigences relatives aux sous-systèmes.

7.2.2 Généralités

7.2.2.1 La spécification des exigences de conception des systèmes E/E/PE doit être déduite des exigences de sécurité de ces systèmes, spécifiées en 7.10 de la CEI 61508-1.

NOTE Il convient de prendre des précautions particulières lorsque des fonctions non relatives à la sécurité et des fonctions de sécurité sont mises en œuvre dans le même système E/E/PE relatif à la sécurité. Alors que cette disposition est admise dans la norme, elle peut donner lieu à une plus grande complexité et rendre plus difficile l'exécution des activités du cycle de vie de sécurité E/E/PE (par exemple, la conception, la validation, l'évaluation et le maintien de la sécurité fonctionnelle). Voir aussi 7.4.2.3.

7.2.2.2 La spécification des exigences de conception des systèmes E/E/PE doit être exprimée et structurée pour que ces dernières soient:

a) claires, précises, non ambiguës, vérifiables, aptes aux essais, actualisables et réalisables;

b) rédigées de manière à faciliter la compréhension des personnes susceptibles d'utiliser les informations à toute étape du cycle de vie de sécurité des systèmes E/E/PE; et

c) vérifiables par rapport à la spécification des exigences de sécurité relatives aux systèmes E/E/PE.

7.2.3 Spécification des exigences de conception des systèmes E/E/PE

7.2.3.1 La spécification des exigences de conception des systèmes E/E/PE doit contenir les exigences de conception relatives aux fonctions de sécurité (voir 7.2.3.2) ainsi que les exigences de conception relatives à l'intégrité de sécurité (voir 7.2.3.3).

7.2.3.2 La spécification des exigences de conception des systèmes E/E/PE doit contenir les détails de tous les matériels et logiciels nécessaires pour mettre en œuvre les fonctions de sécurité requises, avec la précision requise par la spécification des exigences relatives aux fonctions de sécurité de ces mêmes systèmes (voir 7.10.2.6 de la CEI 61508-1). La spécification doit inclure, pour chaque fonction de sécurité:

a) les exigences relatives aux sous-systèmes et le cas échéant, les exigences relatives à leurs éléments matériels et logiciels;

b) les exigences relatives à l'intégration des sous-systèmes et de leurs éléments matériels et logiciels afin de satisfaire à la spécification des exigences relatives aux fonctions de sécurité des systèmes E/E/PE;

c) la performance de vitesse qui permet de satisfaire aux exigences relatives au temps de réaction;

d) les exigences de précision et de stabilité relatives aux mesures et aux commandes;

e) les interfaces entre les systèmes E/E/PE relatifs à la sécurité et l'opérateur;

f) les interfaces entre les systèmes E/E/PE relatifs à la sécurité et les autres systèmes (à l'intérieur ou à l'extérieur de l'EUC);

g) tous les modes de comportement des systèmes E/E/PE relatifs à la sécurité, en particulier le comportement en cas de défaillance et la réponse requise (par exemple, alarmes, arrêt automatique, etc.) de ces systèmes;

h) l'importance de toutes les interactions entre matériel/logiciel et lorsque cela est pertinent, les contraintes exigées entre le matériel et le logiciel;

NOTE Lorsque ces interactions ne sont pas connues avant l'achèvement de la conception, seules les contraintes d'ordre général peuvent être déclarées.

i) les conditions aux limites et de contrainte pour les systèmes E/E/PE relatifs à la sécurité et leurs éléments associés, par exemple, contraintes temporelles (ou contraintes dues à la possibilité de défaillances de cause commune);

j) toutes exigences spécifiques liées aux procédures de démarrage et redémarrage des systèmes E/E/PE relatifs à la sécurité.

7.2.3.3 La spécification des exigences de conception des systèmes E/E/PE doit contenir les détails appropriés à la conception, qui permettent d'obtenir le niveau d'intégrité de sécurité et

l'objectif chiffré de défaillance requis pour la fonction de sécurité, tel qu'il est précisé par la spécification des exigences relatives à l'intégrité de sécurité de ces mêmes systèmes (voir 7.10.2.7 de la CEI 61508-1), y compris:

a) l'architecture de chaque sous-système requise pour répondre aux contraintes architecturales relatives à l'intégrité de sécurité du matériel (voir 7.4.4);

b) tous les paramètres pertinents de modélisation de la fiabilité, tels que la fréquence d'essai périodique requise de tous les éléments matériels nécessaires pour atteindre l'objectif chiffré de défaillance;

NOTE 1 Les informations concernant l'application spécifique ne peuvent pas être sous-estimées (voir 7.10.2.1 de la CEI 61508-1). Ceci est plus 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 destinée à l'application particulière. Par exemple, l'intervalle entre les opérations d'entretien et de maintenance qui peut raisonnablement être obtenue pour des articles produits en série utilisés par le public, est susceptible d'être supérieur à celui prévu avec une application davantage maîtrisée.

c) les actions entreprises en cas de détection d'une défaillance dangereuse par diagnostic;

d) les exigences, contraintes, fonctions et installations qui permettent d'effectuer l'essai périodique des matériels E/E/PE;

e) les aptitudes des équipements utilisés à supporter des conditions environnementales extrêmes (par exemple, température, humidité, contraintes mécaniques et électriques) spécifiées comme nécessaires 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 niveaux d'immunité électromagnétique requis (voir CEI/TS 61000-1-2: 2008);

NOTE 2 Les niveaux d'immunité requis peuvent varier pour différents éléments du système relatif à la sécurité, selon l'emplacement physique et les dispositions d'alimentation.

NOTE 3 Des recommandations figurent dans les normes de produits CEM. Il est toutefois important de considérer que des niveaux d'immunité plus élevés, ou des exigences supplémentaires relatives à l'immunité, que ceux/celles spécifié(e)s dans de telles normes peuvent être nécessaires dans des localisations particulières ou lorsque les équipements sont destinés à être utilisés dans des environnements électromagnétiques plus sévères ou différents.

g) les mesures d'assurance/contrôle qualité nécessaires pour la gestion de la sécurité (voir 6.2.5 de la CEI 61508-1);

7.2.3.4 La spécification des exigences de conception des systèmes E/E/PE doit être complétée en détail à mesure de l'évolution de la conception, et si nécessaire, actualisée après modification.

7.2.3.5 Pour éviter les erreurs au cours de l'élaboration de la spécification des exigences de conception des systèmes E/E/PE, un ensemble de techniques et de mesures appropriées conformément au Tableau B.1 doit être utilisé.

7.2.3.6 Les conséquences des exigences de conception des systèmes E/E/PE sur l'architecture doivent être prises en considération

NOTE Il convient que cette prise en considération recherche la simplicité de mise en œuvre permettant d'obtenir le niveau d'intégrité de sécurité requis (y compris les questions d'ordre architectural et la répartition de la fonctionnalité sur les données de configuration ou le système intégré).

7.3 Planification de la validation de la sécurité des systèmes E/E/PE

NOTE Cette phase correspond à la case 10.2 de la Figure 2. Elle est normalement réalisée parallèlement à la conception et au développement des systèmes E/E/PE (voir 7.4).

7.3.1 Objectif

L'objectif des exigences du présent paragraphe est de planifier la validation de la sécurité des systèmes E/E/PE relatifs à la sécurité.

7.3.2 Exigences

7.3.2.1 Une planification doit être réalisée afin de spécifier les étapes (tant en termes de procédure que de technique) qui doivent être utilisées pour démontrer que les systèmes E/E/PE relatifs à la sécurité sont conformes à la spécification des exigences de sécurité de ces systèmes (voir 7.10 de la CEI 61508-1) et à la spécification des exigences de conception de ces mêmes systèmes (voir 7.2).

7.3.2.2 La planification de la validation des systèmes E/E/PE relatifs à la sécurité doit tenir compte des éléments suivants:

a) l'ensemble des exigences définies dans la spécification des exigences de sécurité des systèmes E/E/PE, ainsi que dans la spécification des exigences de conception de ces systèmes;

b) les procédures à appliquer pour valider la mise en œuvre correcte de chaque fonction de sécurité ainsi que les critères de succès/échec pour la réalisation des essais;

c) les procédures à appliquer pour valider l'intégrité de sécurité requise pour chaque fonction de sécurité ainsi que les critères de succès/échec pour la réalisation des essais;

d) l'environnement nécessaire à la réalisation des essais, y compris l'ensemble des outils et équipements nécessaires (prévoir également les outils et équipements qu'il convient d'étalonner);

e) les procédures d'évaluation des essais (avec leurs justifications);

f) les procédures d'essai et les critères d'aptitude à appliquer pour valider les limites d'immunité électromagnétique spécifiées;

NOTE La CEI/TS 61000-1-2 donne des recommandations concernant la spécification des essais d'immunité électromagnétique pour les éléments constitutifs des systèmes relatifs à la sécurité.

g) les stratégies de résolution des défaillances lors de la validation.

7.4 Conception et développement des systèmes E/E/PE

NOTE Cette phase correspond à la case 10.3 de la Figure 2. Elle est normalement réalisée parallèlement à la planification de la validation de la sécurité des systèmes E/E/PE (voir 7.3).

7.4.1 Objectif

L'objectif des exigences du présent paragraphe est de concevoir et développer le système E/E/PE relatif à la sécurité (y compris les ASIC le cas échéant, voir CEI 61508-4, 3.2.15) afin de satisfaire à la spécification des exigences de conception du système E/E/PE (par rapport aux exigences relatives aux fonctions de sécurité et à l'intégrité de sécurité (voir 7.2).

7.4.2 Exigences générales

7.4.2.1 La conception du système E/E/PE relatif à la sécurité doit être réalisée conformément à la spécification des exigences de conception des systèmes E/E/PE (voir 7.2.3), en tenant compte de toutes les exigences de 7.2.3.

7.4.2.2 La conception du système E/E/PE relatif à la sécurité (y compris l'architecture matérielle et logicielle globale, les capteurs, les actionneurs, l'électronique programmable, les ASIC, le logiciel intégré, le logiciel d'application, les données, etc.), doit satisfaire à l'ensemble des exigences a) à e), comme suit:

a) les exigences d'intégrité de sécurité du matériel qui comprennent:
   - les contraintes architecturales relatives à l'intégrité de sécurité du matériel (voir 7.4.4); et
   - les exigences relatives à la quantification de l'effet des défaillances aléatoires (voir 7.4.5);

b) le cas échéant, les exigences d'architecture particulières relatives aux circuits intégrés à redondance sur la puce (voir Annexe E) à moins qu'il ne puisse être justifié que le même

niveau d'indépendance entre différents canaux est obtenu en appliquant un ensemble de mesures différent;

c) les exigences relatives à l'intégrité de sécurité systématique (capabilité systématique), pouvant être satisfaites en suivant l'un des parcours de conformité suivants:

   – Parcours 1_S: conformité aux exigences relatives à l'évitement des anomalies systématiques (voir 7.4.6 et CEI 61508-3), et aux exigences pour la maîtrise des anomalies systématiques (voir 7.4.7 et CEI 61508-3), ou

   – Parcours 2_S: conformité aux exigences attestant que les équipements sont éprouvés par une utilisation antérieure (voir 7.4.10), ou

   – Parcours 3_s (éléments logiciels préexistant uniquement): conformité aux exigences de la CEI 61508-3, 7.4.2.12;

   NOTE L'indice « S » dans les parcours ci-dessus, désigne l'intégrité de sécurité systématique pour différencier des parcours 1_H, et 2_H et pour l'intégrité de sécurité du matériel.

d) les exigences relatives au comportement du système lors de la détection d'une anomalie (voir 7.4.8);

e) les exigences relatives aux processus de communications de données (voir 7.4.11).

7.4.2.3 Lorsqu'un système E/E/PE relatif à la sécurité doit mettre en œuvre des fonctions relatives à la sécurité et des fonctions non relatives à la sécurité, tout le matériel et le logiciel doivent alors être traités comme des éléments relatifs à la sécurité, sauf s'il peut être démontré que la mise en œuvre des fonctions de sécurité et des fonctions non relatives à la sécurité est suffisamment indépendante (ce qui signifie que la défaillance des fonctions non relatives à la sécurité ne provoque pas de défaillance dangereuse des fonctions relatives à la sécurité.

NOTE 1 Une indépendance suffisante de la mise en œuvre est établie en démontrant que la probabilité de défaillances interdépendantes entre les parties non relatives à la sécurité et les parties relatives à la sécurité est suffisamment faible par rapport au niveau d'intégrité de sécurité le plus élevé associé aux fonctions de sécurité impliquées.

NOTE 2 Il convient de veiller plus particulièrement aux fonctions relatives à la sécurité et non relatives à la sécurité mises en œuvre dans le même système E/E/PE relatif à la sécurité. Alors que cette disposition est admise dans la norme, elle peut donner lieu à une plus grande complexité et rendre plus difficile l'exécution des activités du cycle de vie de sécurité E/E/PE (par exemple, la conception, la validation, l'évaluation et le maintien de la sécurité fonctionnelle).

7.4.2.4 Les exigences relatives aux matériels et aux logiciels doivent être déterminées par le niveau d'intégrité de sécurité de la fonction de sécurité ayant le niveau d'intégrité de sécurité le plus élevé, sauf s'il peut être démontré que la mise en œuvre de fonctions de sécurité des différents niveaux d'intégrité de sécurité est suffisamment indépendante.

NOTE 1 Une indépendance suffisante de la mise en œuvre est établie en démontrant que la probabilité de défaillances interdépendantes entre les parties utilisant des fonctions de sécurité de niveaux d'intégrité différents est suffisamment faible par rapport au niveau d'intégrité de sécurité le plus élevé associé aux fonctions de sécurité impliquées.

NOTE 2 Lorsque plusieurs fonctions de sécurité sont réalisées dans un système E/E/PE relatif à la sécurité, il est alors nécessaire de prendre en considération la possibilité d'une anomalie unique pouvant provoquer la défaillance de plusieurs fonctions de sécurité. Dans une telle situation, il peut être approprié de déterminer les exigences relatives aux matériels et aux logiciels sur la base d'un niveau d'intégrité de sécurité plus élevé que celui associé à l'une quelconque des fonctions de sécurité, selon le risque correspondant à ce type de défaillance.

7.4.2.5 Lorsque l'indépendance entre les fonctions de sécurité est nécessaire (voir 7.4.2.3 et 7.4.2.4), les aspects suivants doivent alors être documentés lors de la conception:

a) la méthode pour obtenir l'indépendance;

b) la justification de cette méthode.

EXEMPLE Traiter les modes de défaillance prévisibles, susceptibles de sous-estimer l'indépendance, et leurs taux de défaillance, en appliquant une analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) ou une analyse des défaillances dépendante.

7.4.2.6 Les exigences applicables au logiciel de sécurité (voir CEI 61508-3) doivent être mises à la disposition du développeur du système E/E/PE relatif à la sécurité.

7.4.2.7 Le développeur du système E/E/PE relatif à la sécurité doit examiner les exigences du logiciel et du matériel relatifs à la sécurité pour assurer qu'elles sont spécifiées de manière appropriée. Le développeur des systèmes E/E/PE doit notamment tenir compte des éléments suivants:

a) fonctions de sécurité;

b) exigences d'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité;

c) interfaces entre les équipements et l'opérateur.

7.4.2.8 La documentation de conception des systèmes E/E/PE relatifs à la sécurité doit spécifier les techniques et les mesures nécessaires au cours des phases du cycle de vie de sécurité de ces systèmes pour obtenir le niveau d'intégrité de sécurité.

7.4.2.9 La documentation de conception des systèmes E/E/PE relatifs à la sécurité doit justifier des techniques et mesures choisies pour constituer un ensemble intégré conforme au niveau d'intégrité de sécurité requis.

NOTE L'adoption d'une approche globale utilisant une homologation de type indépendante des systèmes E/E/PE relatifs à la sécurité (y compris les capteurs, actionneurs, etc.) pour le matériel et le logiciel, les essais de diagnostic et les outils de programmation et utilisant dans toute la mesure du possible des langages appropriés pour le logiciel, permet potentiellement de réduire la complexité technique de l'application des systèmes E/E/PE.

7.4.2.10 Lors des activités de conception et développement, l'importance (le cas échéant) de toutes les interactions entre le matériel et le logiciel doit être identifiée, évaluée et documentée.

7.4.2.11 La conception doit être basée sur une décomposition en sous-systèmes, chaque sous-système ayant une conception et un ensemble d'essais d'intégration spécifiés (voir 7.5.2).

NOTE 1 On peut considérer qu'un sous-système comprend un seul élément ou un groupe quelconque d'éléments. Voir la CEI 61508-4 pour les définitions. Un système E/E/PE relatif à la sécurité complet est constitué d'un certain nombre de sous-systèmes identifiables et distincts qui, lorsqu'ils sont réunis, réalisent la fonction de sécurité considérée. Un sous-système peut être constitué de plusieurs canaux (voir 7.4.9.3 et 7.4.9.4).

NOTE 2 Lorsque c'est possible, il convient d'utiliser des sous-systèmes existants et vérifiés pour la mise en œuvre. Cette indication n'est généralement valable que s'il est possible de mettre en correspondance, à près de 100 %, la fonctionnalité, la capacité et les caractéristiques de performance du sous-système ou élément existant avec la nouvelle exigence, ou bien si le sous-système ou l'élément vérifié est structuré de telle sorte que l'utilisateur soit capable de choisir uniquement les fonctions, les capacités ou les caractéristiques de performance requises pour l'application spécifique. Des fonctionnalités, des capacités ou des caractéristiques de performance excessives peuvent être préjudiciables à la sécurité du système, si le sous-système ou l'élément existant est d'une complexité trop grande, ou présente des caractéristiques non utilisées, et s'il n'est pas possible d'obtenir la protection nécessaire contre les fonctions non souhaitées.

7.4.2.12 Lorsque la conception initiale du système E/E/PE relatif à la sécurité est achevée, une analyse doit être effectuée pour déterminer si une défaillance raisonnablement prévisible de ce système peut provoquer une situation dangereuse ou solliciter toute autre mesure de maîtrise du risque. Si toute défaillance raisonnablement prévisible peut avoir l'un des ces effets, la première priorité doit alors consister à modifier la conception du système E/E/PE relatif à la sécurité de manière à éviter de tels modes de défaillance. Si cela n'est pas possible, des mesures doivent alors être prises pour réduire la probabilité d'occurrence de ces modes de défaillance à un niveau proportionné à l'objectif chiffré de défaillance. Ces mesures doivent être soumises aux exigences de la présente norme.

NOTE Le présent article a pour objectif d'identifier les modes de défaillance du système E/E/PE relatif à la sécurité qui sollicite d'autres mesures de maîtrise du risque. Il peut exister des situations dans lesquelles le taux de défaillance des modes de défaillance spécifiés ne peut pas être réduit et où une nouvelle fonction de sécurité est requise ou le SIL des autres fonctions de sécurité est réexaminé, compte tenu du taux de défaillance.

7.4.2.13 Il convient de tenir compte du déclassement par rapport à des caractéristiques assignées (voir CEI 61508-7) pour tous les éléments matériels. Toute justification pour utiliser des éléments matériels à leurs limites doit être documentée (voir CEI 61508-1, Article 5).

NOTE Lorsque le déclassement est approprié, un facteur de déclassement d'au moins deux-tiers est généralement utilisé.

7.4.2.14 Lorsque la conception d'un système E/E/PE relatif à la sécurité comprend un ou plusieurs ASIC visant à appliquer une fonction de sécurité, un cycle de vie lié au développement de ces circuits (voir 7.1.3.1) doit être utilisé.

7.4.3 Synthèse des éléments permettant d'obtenir la capabilité systématique requise

7.4.3.1 Dans les circonstances décrites dans cette section et afin de satisfaire aux exigences relatives à une intégrité de sécurité systématique, le système E/E/PE relatif à la sécurité désigné peut être réparti en éléments d'une capabilité systématique différente.

NOTE 1 La capabilité systématique d'un élément détermine la possibilité pour des anomalies systématiques de cet élément de générer une défaillance de la fonction de sécurité. Le concept de capabilité systématique d'un élément s'applique tant aux éléments matériels qu'aux éléments logiciels.

NOTE 2 Le paragraphe 7.2.6.7 de la CEI 61508-1 reconnaît la valeur d'indépendance et de diversité au niveau d'une fonction de sécurité, ainsi que les systèmes E/E/PE relatifs à la sécurité auxquels elle peut être attribuée. Ces concepts peuvent également être appliqués au niveau de conception détaillée lorsqu'un ensemble d'éléments mettant en œuvre une fonction de sécurité peut potentiellement atteindre des performances systématiques meilleures que celles obtenues avec les éléments pris individuellement.

7.4.3.2 Pour un élément de capabilité systématique SC N (N = 1, 2, 3), lorsqu'une anomalie systématique de cet élément ne génère pas de défaillance de la fonction de sécurité spécifiée, mais génère en revanche une défaillance uniquement en association avec une seconde anomalie systématique d'un autre élément de capabilité systématique SC N, la combinaison des deux éléments peut être considérée comme ayant une capabilité systématique de SC (N + 1), sous réserve de l'existence d'une indépendance suffisante entre les deux éléments (voir 7.4.3.4).

NOTE L'indépendance des éléments peut être évaluée uniquement lorsque l'application spécifique de ces derniers est connue par rapport aux fonctions de sécurité définies.

7.4.3.3 La capabilité systématique pouvant être déclarée pour une combinaison d'éléments dont la capabilité systématique SC N de chaque élément est égale à SC (N+1). Un élément SC N ne peut être utilisé de cette manière qu'une seule fois. La constitution d'une capabilité systématique SC (N+2) et au-delà par assemblages successifs d'ensembles d'éléments de capabilité systématique SC N n'est pas admise.

7.4.3.4 Une indépendance suffisante, dans la conception entre les éléments et dans l'application de ces derniers, doit être justifiée par une analyse des défaillances de cause commune afin de démontrer que la probabilité d'interférence entre les éléments, et entre ces derniers et l'environnement est suffisamment faible par rapport au niveau d'intégrité de sécurité de la fonction de sécurité considérée.

NOTE 1 Pour la capabilité systématique et en ce qui concerne la conception, la réalisation, l'exploitation et la maintenance du matériel, les méthodes possibles d'obtention d'une indépendance suffisante incluent:

– la diversité fonctionnelle; utilisation de différentes approches pour obtenir les mêmes résultats;
– techniques diverses: utilisation de différents types d'équipements pour obtenir les mêmes résultats;
– des parties/services communs: assurer qu'il n'existe pas de parties, services ou systèmes annexes communs (par exemple, sources d'alimentation en énergie) dont la défaillance peut conduire à un mode de défaillance dangereuse de tous les systèmes;
– des procédures communes; assurer qu'il n'existe pas de procédures communes d'exploitation, de maintenance ou d'essai.

NOTE 2 L'indépendance des moyens d'application signifie que les éléments n'affectent pas le comportement d'exécution de chacun d'entre eux de manière à générer une défaillance dangereuse.

NOTE 3 Pour l'indépendance des éléments logiciels, voir 7.4.2.8 et 7.4.2.9 de la CEI 61508-3.

7.4.4 Contraintes architecturales portant sur l'intégrité de sécurité du matériel

NOTE 1 Les équations, relatives aux contraintes portant sur l'intégrité de sécurité du matériel, sont spécifiées à l'Annexe C et les contraintes portant sur l'intégrité de sécurité sont synthétisées dans les Tableaux 2 et 3.

NOTE 2 L'Article A.2 de la CEI 61508-6 donne une vue d'ensemble des étapes nécessaires lors de la réalisation de l'intégrité de sécurité du matériel requise, et présente la manière suivant laquelle le présent paragraphe est en rapport avec d'autres exigences de la présente norme.

Dans le cadre de l'intégrité de sécurité du matériel, le niveau d'intégrité de sécurité le plus élevé pouvant être déclaré pour une fonction de sécurité est limité par les contraintes portant sur l'intégrité de sécurité du matériel imposées par l'application de l'un des deux parcours possibles (mise en œuvre au niveau du système ou du sous-système):

– Parcours 1_H basé sur les concepts de tolérance aux anomalies du matériel et de proportion de défaillances en sécurité; ou

– Parcours 2_H basé sur le retour d'exploitation par l'utilisateur final et concernant les données de fiabilité des composants des niveaux de confiance plus élevés et une tolérance aux anomalies du matériel (HFT)[1] pour les niveaux d'intégrité de sécurité spécifiés.

Les normes d'application basées sur la série CEI 61508 peuvent indiquer le parcours préférentiel (c'est-à-dire le parcours 1_H ou le parcours 2_H).

NOTE 3 L'indice « H » dans les parcours ci-dessus, désigne l'intégrité de sécurité du matériel pour les différencier des parcours 1_S , 2_S et 3_S, pour l'intégrité de sécurité systématique.

7.4.4.1 Exigences générales

7.4.4.1.1 Concernant les exigences relatives à la tolérance aux anomalies du matériel

a) une tolérance aux anomalies du matériel N signifie que N+1 correspond au nombre minimal d'anomalies susceptibles de provoquer la perte de la fonction de sécurité (pour plus de clarification, voir Note 1 et Tableaux 2 et 3). Lors de la détermination de la tolérance aux anomalies du matériel, aucune autre mesure pouvant contrôler les effets des anomalies, tels que les diagnostics, ne doit être prise en compte; et

b) lorsqu'une anomalie donne directement lieu à l'apparition d'une ou de plusieurs anomalies consécutives, toutes ces anomalies sont considérées comme une anomalie unique;

c) lors de la détermination de la tolérance aux anomalies du matériel, certaines anomalies peuvent être exclues à condition que leur probabilité d'occurrence soit très faible par rapport aux exigences d'intégrité de sécurité du sous-système. De telles exclusions d'anomalies doivent être justifiées et documentées (voir la Note 2).

NOTE 1 Les contraintes portant sur l'intégrité de sécurité du matériel ont été incluses afin d'obtenir une architecture suffisamment robuste tout en tenant compte du niveau de complexité de l'élément et du sous-système (voir 7.4.4.1.1 et 7.4.4.1.2). Le niveau d'intégrité de sécurité maximal admissible pour la fonction de sécurité appliquée par le système E/E/PE relatif à la sécurité, obtenu par l'application de ces exigences, est le niveau maximum qu'il est permis de déclarer pour la fonction de sécurité, même si, dans certains cas, les calculs de fiabilité montrent qu'un niveau d'intégrité de sécurité supérieur peut être obtenu. Il convient également de noter que même si la tolérance aux anomalies du matériel est obtenue pour tous les sous-systèmes, un calcul de fiabilité est toujours nécessaire pour démontrer que l'objectif chiffré de défaillance spécifié a été réalisé, cet élément pouvant par ailleurs nécessiter un accroissement de la tolérance aux anomalies du matériel pour satisfaire aux exigences de conception.

NOTE 2 Les exigences relatives à la tolérance aux anomalies du matériel s'appliquent à l'architecture du sous-système utilisée dans des conditions de fonctionnement normales. Il est admis d'assouplir les exigences relatives à la tolérance aux anomalies du matériel lorsque le système E/E/PE relatif à la sécurité est en cours de réparation en ligne. Cependant, il convient que les paramètres clés relatifs à tout assouplissement aient été préalablement évalués (par exemple, en comparant la durée moyenne de rétablissement à la probabilité d'une sollicitation).

NOTE 3 Certaines anomalies peuvent être exclues étant donné que, si un élément a à l'évidence une très faible probabilité de défaillance en raison de propriétés inhérentes à sa conception et à sa construction (par exemple, la fuite d'un actionneur mécanique), alors il n'est pas normalement considéré comme nécessaire de contraindre (sur

[1] HFT = *Hardware Fault Tolerant*.

la base de la tolérance aux anomalies du matériel) l'intégrité de sécurité de toute fonction de sécurité qui utilise cet élément.

NOTE 4 Le choix du parcours est dépendant de l'application et du secteur, et il convient de tenir compte des points suivants lors de ce choix:

– une défaillance en sécurité d'une fonction peut générer un nouveau danger ou constituer une cause supplémentaire de génération d'un danger existant;

– la redondance peut ne pas être réalisable pour toutes les fonctions,

– une réparation n'est pas toujours possible ou rapide (par exemple, non réalisable dans un délai négligeable par rapport à l'intervalle d'essai périodique).

NOTE 5 Les exigences d'architecture particulières relatives aux circuits intégrés à redondance sur la puce sont fournies à l'Annexe E.

7.4.4.1.2 Un élément peut être considéré comme du type A si, pour les composants nécessaires à la réalisation de la fonction de sécurité

a) les modes de défaillance de tous les composants qui le constituent sont bien définis; et

b) le comportement de l'élément dans des conditions d'anomalie peut être entièrement déterminé; et

c) il existe des données de défaillance suffisamment fiables pour démontrer que les taux de défaillance déclarés relatifs à des défaillances dangereuses détectées et non détectées sont satisfaits (voir 7.4.9.3 à 7.4.9.5).

7.4.4.1.3 Un élément doit être considéré comme du type B si, pour les composants nécessaires à la réalisation de la fonction de sécurité,

a) le mode de défaillance d'au moins un des composants qui le constituent n'est pas bien défini; ou

b) le comportement de l'élément dans des conditions d'anomalie ne peut être entièrement déterminé; ou

c) il n'existe aucune donnée de défaillance suffisamment fiable pour appuyer les déclarations relatives aux taux de défaillance relatifs à des défaillances dangereuses détectées et non détectées (voir 7.4.9.3 à 7.4.9.5).

NOTE Cela signifie que si au moins un des composants d'un élément proprement dit satisfait aux conditions applicables à un élément de type B, alors cet élément est considéré comme étant du type B plutôt que du type A.

7.4.4.1.4 Pour estimer la proportion de défaillances en sécurité d'un élément, destiné à être utilisé dans un sous-système ayant une tolérance aux anomalies du matériel nulle, et qui met en œuvre une fonction de sécurité en totalité ou en partie, et fonctionnant en mode sollicitation élevée ou en mode continu, le diagnostic est crédible uniquement si:

– la somme de l'intervalle entre les essais de diagnostic et du temps nécessaire à l'exécution de l'action spécifiée pour obtenir ou maintenir un état de sécurité est inférieure au temps de sécurité du processus; ou,

– en mode de fonctionnement à sollicitation élevée, le rapport du taux d'essais de diagnostic sur la fréquence de sollicitation est supérieur ou égal à 100.

7.4.4.1.5 Pour estimer la proportion de défaillances en sécurité d'un élément

– ayant une tolérance aux anomalies du matériel supérieure à zéro, et qui met en œuvre une fonction de sécurité en totalité ou en partie, et fonctionnant en mode sollicitation élevée ou en mode continu; ou

– qui applique en totalité ou en partie une fonction de sécurité, fonctionnant en mode faible sollicitation,

le diagnostic doit être crédible uniquement si la somme de l'intervalle entre les essais de diagnostic et du temps nécessaire à l'exécution de la réparation d'une défaillance détectée, est inférieure à la durée moyenne de panne (MTTR) utilisée dans le calcul pour déterminer l'intégrité de sécurité obtenue pour la fonction de sécurité concernée.

7.4.4.2 Parcours 1_H

7.4.4.2.1 Pour déterminer le niveau d'intégrité de sécurité maximal pouvant être déclaré par rapport à une fonction de sécurité spécifiée, la procédure suivante doit être suivie:

1) Définir les sous-systèmes qui constituent le système E/E/PE relatif à la sécurité.
2) Pour chaque sous-système, déterminer la proportion de défaillances en sécurité pour tous les éléments de ce sous-système séparément (c'est-à-dire sur la base d'un élément individuel ayant une tolérance aux anomalies du matériel nulle). Dans le cas de configurations à éléments redondants, la proportion de défaillances en sécurité peut être calculée en prenant en compte le diagnostic supplémentaire pouvant exister (par exemple, par comparaison des éléments redondants).
3) Pour chaque élément, utiliser la proportion de défaillances en sécurité obtenue et la tolérance aux anomalies du matériel nulle pour déterminer le niveau d'intégrité de sécurité maximal pouvant être déclaré sur la base de la colonne 2 du Tableau 2 (pour les éléments de type A) et de la colonne 2 du Tableau 3 (pour les élément de type B).
4) Utiliser la méthode décrite en 7.4.4.2.3 et 7.4.4.2.4 pour déterminer le niveau d'intégrité de sécurité maximal pouvant être déclaré pour le sous-système.
5) Le niveau d'intégrité de sécurité maximal pouvant être déclaré pour un système E/E/PE relatif à la sécurité doit être déterminé par le sous-système ayant atteint le niveau d'intégrité de sécurité le plus faible.

7.4.4.2.2 Pour une application aux sous-systèmes comprenant des éléments conformes aux exigences spécifiques détaillées ci-dessous et comme alternative à l'application des exigences spécifiées en 7.4.4.2.1 2) à 7.4.4.2.1 4), les indications suivantes sont applicables:

1) le sous-système comprend deux éléments ou plus; et
2) les éléments sont du même type; et
3) tous les éléments ont obtenu des proportions de défaillances en sécurité comprises dans la même plage (voir Note 1 ci-dessous) spécifiées dans les Tableaux 2 ou 3; la procédure suivante peut alors être suivie,
   a) déterminer la proportion de défaillances en sécurité de tous les éléments individuels. Dans le cas de configurations à éléments redondants, la proportion de défaillances en sécurité peut être calculée en prenant en compte le diagnostic supplémentaire pouvant exister (par exemple, par comparaison des éléments redondants);
   b) déterminer la tolérance aux anomalies du matériel du sous-système;
   c) déterminer le niveau d'intégrité de sécurité maximal pouvant être déclaré pour le sous-système, si les éléments sont du type A décrit dans le Tableau 2;
   d) déterminer le niveau d'intégrité de sécurité maximal pouvant être déclaré pour le sous-système, si les éléments sont du type B décrit dans le Tableau 3.

NOTE 1 La plage indiquée en 3) ci-dessus fait référence aux Tableaux 2 et 3 dans lesquels la proportion de défaillances en sécurité est classée dans l'une des quatre plages mentionnées (c'est-à-dire (<60 %); (60 % à <90 %); (90 % à <99 %) et (≥99 %)). Toutes les SFF devraient se situer dans la même plage (par exemple, toutes dans la plage (90 % à <99 %).

EXEMPLE 1 Pour déterminer le niveau d'intégrité de sécurité maximal effectivement obtenu pour la fonction de sécurité spécifiée par un sous-système ayant une tolérance aux anomalies du matériel de 1, où des éléments parallèles mettent en œuvre une fonction de sécurité applicable à chaque élément, la méthode suivante peut être adoptée sous réserve que le sous-système satisfasse aux exigences de 7.4.4.2.2. Dans cet exemple, tous les éléments sont du type B et les proportions de défaillances en sécurité des éléments se situent dans la plage (90 % à < 99 %).

L'étude du Tableau 3 permet d'observer que, pour une tolérance aux anomalies du matériel égale à 1, les proportions de défaillances en sécurité des deux éléments se situant par ailleurs dans la plage (90 % à <99 %), le niveau d'intégrité de sécurité maximal admissible pour la fonction de sécurité spécifiée est SIL 3.

EXEMPLE 2 Pour déterminer la tolérance aux anomalies du matériel requise pour un sous-système, pour la fonction de sécurité spécifiée, où des éléments parallèles mettent en œuvre une fonction de sécurité applicable à chaque élément, la méthode suivante peut être adoptée sous réserve que le sous-système satisfasse aux exigences de 7.4.4.2.2. Dans cet exemple, tous les éléments sont du type A et les proportions de défaillances en

sécurité des éléments se situent dans la plage (60 % à <90 %). Le niveau d'intégrité de sécurité de la fonction de sécurité est SIL 3.

L'étude du Tableau 2 permet d'observer que, pour satisfaire à l'exigence relative au SIL 3, la tolérance aux anomalies du matériel requise doit être égale à 1. Cela signifie que deux éléments parallèles se révèlent nécessaires.

Tableau 2 – Niveau d'intégrité de sécurité maximal admissible pour une fonction de sécurité exécutée par un élément ou sous-système relatif à la sécurité de type A

Proportion de défaillances en sécurité d'un élément	Tolérance aux anomalies du matériel		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 Ce Tableau, associé à 7.4.4.2.1 et 7.4.4.2.2 permet de déterminer le niveau d'intégrité de sécurité maximal pouvant être déclaré pour un sous-système: compte tenu de la tolérance aux anomalies du sous-système et de la SFF des éléments utilisés.

i. Pour une application générale à tout sous-système, voir 7.4.4.2.1.

ii. Pour une application aux sous-systèmes comprenant des éléments conformes aux exigences spécifiques de 7.4.4.2.2. Pour déclarer qu'un sous-système satisfait à un SIL spécifié directement à partir de ce tableau, il est nécessaire de satisfaire à toutes les exigences mentionnées en 7.4.4.2.2.

NOTE 2 Le tableau, associé à 7.4.4.2.1 et 7.4.4.2.2, peut également être utilisé:

i. Pour déterminer les exigences de tolérance aux anomalies du matériel pour un sous-système, compte tenu du SIL requis de la fonction de sécurité et des SFF des éléments à utiliser.

ii. Pour déterminer les exigences relatives aux SFF applicables aux éléments, compte tenu du SIL requis de la fonction de sécurité et de la tolérance aux anomalies du matériel du sous-système.

NOTE 3 Les exigences spécifiées en 7.4.4.2.3 et 7.4.4.2.4 sont basées sur les données spécifiées dans ce tableau et le Tableau 3.

NOTE 4 Voir l'Annexe C pour les détails concernant la méthode de calcul de la proportion de défaillances en sécurité.

Tableau 3 – Niveau d'intégrité de sécurité maximal admissible pour une fonction de sécurité exécutée par un élément ou sous-système relatif à la sécurité de type B

Proportion de défaillances en sécurité d'un élément	Tolérance aux anomalies du matériel		
	0	1	2
<60 %	Non toléré	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 Ce Tableau, associé à 7.4.4.2.1 et 7.4.4.2.2 permet de déterminer le niveau d'intégrité de sécurité maximal pouvant être déclaré pour un sous-système compte tenu de la tolérance aux anomalies du sous-système et de la SFF des éléments utilisés.

i. Pour une application générale à tout sous-système, voir 7.4.4.2.1.

ii. Pour une application aux sous-systèmes comprenant des éléments conformes aux exigences spécifiques de 7.4.4.2.2. Pour déclarer qu'un sous-système satisfait à un SIL spécifié directement à partir de ce tableau, il est nécessaire de satisfaire à toutes les exigences mentionnées en 7.4.4.2.2.

NOTE 2 Le tableau, associé à 7.4.4.2.1 et 7.4.4.2.2, peut également être utilisé:

i. Pour déterminer les exigences de tolérance aux anomalies du matériel pour un sous-système, compte tenu du SIL requis de la fonction de sécurité et des SFF des éléments à utiliser.

ii. Pour déterminer les exigences relatives aux SFF applicables aux éléments, compte tenu du SIL requis de la fonction de sécurité et de la tolérance aux anomalies du matériel du sous-système.

NOTE 3 Les exigences spécifiées en 7.4.4.2.3 et 7.4.4.2.4 sont basées sur les données spécifiées dans ce tableau et le Tableau 2.

NOTE 4 Voir l'Annexe C pour les détails concernant la méthode de calcul de la proportion de défaillances en sécurité.

NOTE 5 En appliquant 7.4.4.2.1 pour la combinaison des éléments de type B, avec une tolérance aux anomalies du matériel de 1, et où les deux éléments ont une proportion de défaillances en sécurité inférieure à 60 %, le niveau d'intégrité de sécurité maximal admissible pour une fonction de sécurité exécutée par la combinaison est SIL 1.

7.4.4.2.3 Dans un sous-système E/E/PE relatif à la sécurité où un grand nombre de fonctions de sécurité applicables à un élément est mis en œuvre par une combinaison d'éléments en série (comme illustré à la Figure 5), le niveau d'intégrité de sécurité maximal qui peut être déclaré pour la fonction de sécurité considérée, doit être déterminé par l'élément qui a obtenu le niveau d'intégrité de sécurité le plus faible pour la proportion de défaillances en sécurité obtenue, et ce, pour une tolérance aux anomalies du matériel égale à zéro. Pour une illustration de la méthode, soit une architecture comme indiqué à la Figure 5 et voir l'exemple ci-dessous.

EXEMPLE (voir Figure 5): Soit une architecture où un certain nombre de fonctions de sécurité applicables à un élément sont exécutées par un sous-système comprenant un canal unique d'éléments 1, 2 et 3 et où les éléments satisfont aux exigences des Tableaux 2 et 3 de la manière suivante:

– L'élément 1 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 1;

– L'élément 2 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 2;

– L'élément 3 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 1;

– Les deux éléments 1 et 3 limitent le SIL maximal, pouvant être déclaré, simplement au SIL 1, pour la tolérance aux anomalies du matériel et la proportion de défaillances en sécurité obtenues.

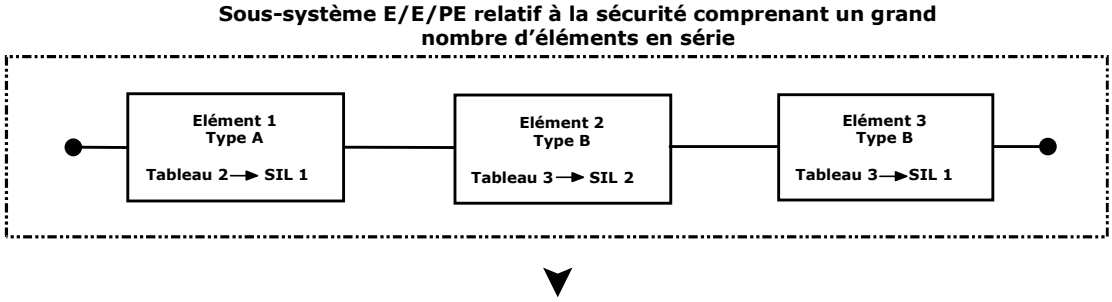


Figure 5 – Détermination du SIL maximal pour l'architecture spécifiée (sous-système E/E/PE relatif à la sécurité comprenant un grand nombre d'éléments en série, voir 7.4.4.2.3)

7.4.4.2.4 Dans un sous-système E/E/PE relatif à la sécurité où une fonction de sécurité applicable à un élément est mise en œuvre par plusieurs canaux (combinaison d'éléments parallèles) ayant une tolérance aux anomalies du matériel de N, le niveau d'intégrité de sécurité maximal qui peut être déclaré pour la fonction de sécurité considérée, doit être déterminé par:

a) le regroupement de la combinaison d'éléments en série pour chaque canal, puis la détermination du niveau d'intégrité de sécurité maximal pouvant être déclaré pour la fonction de sécurité considérée pour chaque canal (voir 7.4.4.2.3); et

b) le choix du canal ayant le niveau d'intégrité de sécurité le plus élevé obtenu pour la fonction de sécurité considérée, puis en ajoutant N niveaux d'intégrité de sécurité afin de déterminer le niveau d'intégrité de sécurité maximal pour la combinaison totale du sous-système.

Pour une illustration de la méthode, soit une architecture comme indiqué à la Figure 6 et voir l'exemple ci-dessous.

NOTE 1 N est la tolérance aux anomalies du matériel de la combinaison d'éléments parallèles (voir 7.4.4.1.1).

NOTE 2 Voir l'exemple ci-dessous concernant l'application du présent paragraphe.

EXEMPLE Il est admis d'effectuer le regroupement et l'analyse de ces combinaisons de diverses manières. Supposons, pour illustrer une méthode possible, une architecture dans laquelle une fonction de sécurité particulière est exécutée par deux sous-systèmes, X et Y, où le sous-système X comprend les éléments 1, 2, 3 et 4 et où le sous-système Y comprend le seul élément 5, comme illustré à la Figure 6. L'utilisation de canaux parallèles dans le sous-système X permet d'assurer que les éléments 1 et 2 mettent en œuvre la partie de la fonction de sécurité requise du sous-système X, indépendamment des éléments 3 et 4, et inversement. La fonction de sécurité est exécutée:

– dans le cas d'une anomalie dans l'élément 1 ou l'élément 2 (dans la mesure où la combinaison des éléments 3 et 4 est capable d'exécuter la partie requise de la fonction de sécurité); ou

– dans le cas d'une anomalie dans l'élément 3 ou l'élément 4 (dans la mesure où la combinaison des éléments 1 et 2 est capable d'exécuter la partie requise de la fonction de sécurité).

La détermination du niveau d'intégrité de sécurité maximal qui peut être déclaré, pour la fonction de sécurité considérée, est détaillée dans les étapes suivantes.

Pour le sous-système X et par rapport à la fonction de sécurité spécifiée considérée, chaque élément satisfait aux exigences des Tableaux 2 et 3 comme suit:

– L'élément 1 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 3;

– L'élément 2 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 2;

– L'élément 3 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 2;

– L'élément 4 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 1.

Les éléments sont combinés pour obtenir un niveau d'intégrité de sécurité du matériel maximal pour la fonction de sécurité considérée et pour le sous-système X comme suit:

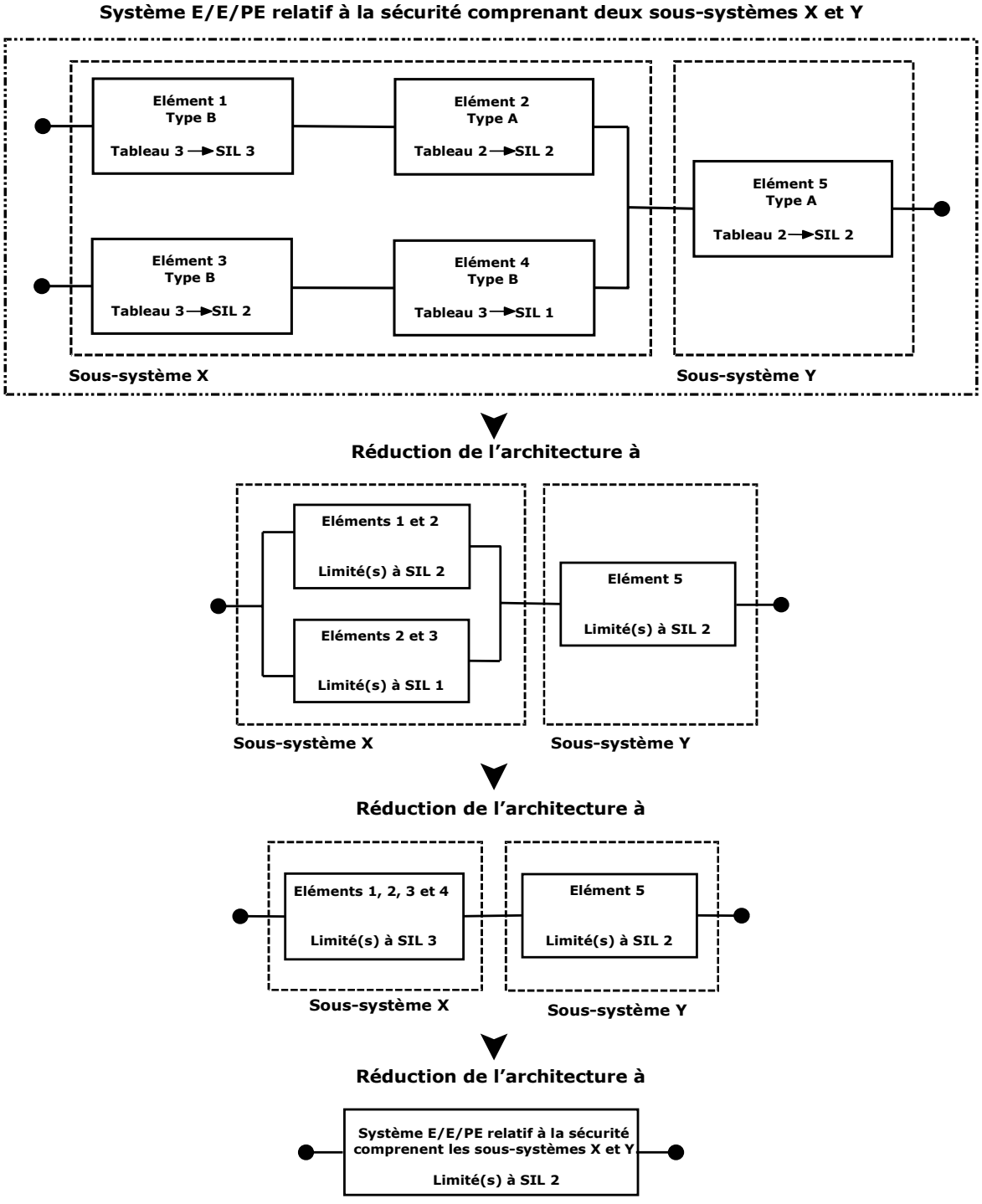
a) Combinaison des éléments 1 et 2: La tolérance aux anomalies du matériel et la proportion de défaillances en sécurité obtenues par la combinaison des éléments 1 et 2 (chacun étant séparément conforme aux exigences de SIL 3 et SIL 2 respectivement) satisfont aux exigences de SIL 2 (déterminé par l'élément 2; voir 7.4.4.2.3);

b) Combinaison des éléments 3 et 4: La tolérance aux anomalies du matériel et la proportion de défaillances en sécurité obtenues par la combinaison des éléments 3 et 4 (chacun étant séparément conforme aux exigences de SIL 2 et SIL 1 respectivement) satisfont aux exigences de SIL 1 (déterminé par l'élément 4, voir 7.4.4.2.3);

c) Association complémentaire de la combinaison des éléments 1 et 2 et de la combinaison des éléments 3 et 4: le niveau d'intégrité de sécurité maximal qui peut être déclaré pour la fonction de sécurité considérée est déterminé en choisissant le canal ayant le niveau d'intégrité de sécurité le plus élevé effectivement obtenu, puis en ajoutant N niveaux d'intégrité de sécurité pour déterminer le niveau d'intégrité de sécurité maximal pour la combinaison totale des éléments. Dans ce cas, le sous-système comporte deux canaux parallèles ayant une tolérance aux anomalies du matériel de 1. Le canal ayant le niveau d'intégrité de sécurité le plus élevé, pour la fonction de sécurité considérée, était celui comportant les éléments 1 et 2 ayant satisfait aux exigences applicables au SIL2. Par conséquent, le niveau d'intégrité de sécurité maximal du sous-système pour une tolérance aux anomalies du matériel de 1 est (SIL2 + 1) = SIL3 (voir 7.4.4.2.4).

Pour le sous-système Y, l'élément 5 satisfait aux exigences, pour une tolérance aux anomalies du matériel nulle et, pour une proportion de défaillances en sécurité spécifique, pour le SIL 2.

Pour le système E/E/PE relatif à la sécurité complet (comprenant deux sous-systèmes X et Y ayant satisfait aux exigences, pour la fonction de sécurité considérée, des SIL 3 et SIL 2 respectivement), le niveau d'intégrité de sécurité maximal qui peut être déclaré pour un système E/E/PE relatif à la sécurité est déterminé par le sous-système ayant obtenu le niveau d'intégrité de sécurité le plus bas (7.4.4.2.1 5)). Par conséquent, pour cet exemple, le niveau d'intégrité de sécurité maximal, pouvant être déclaré pour le système E/E/PE relatif à la sécurité, pour la fonction de sécurité considérée, est SIL2.



Système E/E/PE relatif à la sécurité satisfaisant aux contraintes architecturales, pour la fonction de sécurité, limité au SIL 2

NOTE 1 Les éléments 1 et 2 mettent en œuvre la partie de la fonction de sécurité requise du sous-système X indépendamment des éléments 3 et 4, et inversement.

NOTE 2 Les sous-systèmes qui mettent en œuvre la fonction de sécurité sont répartis dans l'ensemble du système E/E/PE relatif à la sécurité en termes de classement entre les capteurs et les actionneurs.

Figure 6 – Détermination du SIL maximal pour l'architecture spécifiée (sous-système E/E/PE relatif à la sécurité comprenant deux sous-systèmes X & Y, voir 7.4.4.2.4)

7.4.4.3 Parcours 2_H

7.4.4.3.1 La tolérance minimale aux anomalies du matériel pour chaque sous-système d'un système E/E/PE relatif à la sécurité appliquant une fonction de sécurité d'un niveau d'intégrité de sécurité spécifié doit être la suivante:

NOTE Dans les articles suivants, la fonction de sécurité, sauf spécification contraire, peut être exécutée en mode faible sollicitation, en mode sollicitation élevée ou en mode continu.

a) une tolérance aux anomalies du matériel de 2 pour une fonction de sécurité spécifiée de SIL 4, sauf si les conditions définies en 7.4.4.3.2 s'appliquent.

b) une tolérance aux anomalies du matériel de 1 pour une fonction de sécurité spécifiée de SIL 3, sauf si les conditions définies en 7.4.4.3.2 s'appliquent.

c) une tolérance aux anomalies du matériel de 1 pour une fonction de sécurité spécifiée de SIL 2, exécutée en mode sollicitation élevée ou en mode continu, sauf si les conditions définies en 7.4.4.3.2 s'appliquent.

d) une tolérance aux anomalies du matériel de 0 pour une fonction de sécurité spécifiée de SIL 2 exécutée en mode faible sollicitation.

e) une tolérance aux anomalies du matériel de 0 pour une fonction de sécurité spécifiée de SIL 1.

7.4.4.3.2 Pour les éléments de type A uniquement, s'il est déterminé que le respect des exigences HFT spécifiées en 7.4.4.3.1 pour une situation dans laquelle une HFT supérieure à 0 est requise, génèrerait des défaillances supplémentaires et entraînerait une réduction de la sécurité globale de l'EUC, alors une architecture alternative plus sûre avec une HFT réduite peut être appliquée. Dans ce cas, cette application doit être justifiée et documentée. La justification doit attester du fait que:

a) la conformité avec les exigences HFT spécifiées en 7.4.4.3.1 génèrerait des défaillances supplémentaires et entraînerait une réduction de la sécurité globale de l'EUC; et

b) si la HFT est réduite à zéro, les modes de défaillance identifiés dans l'élément qui applique la fonction de sécurité, peuvent être exclus dans la mesure où le(s) taux de défaillance dangereuse du (des) mode(s) de défaillance identifié(s) associé(s) est/sont très faible(s) par rapport à l'objectif chiffré de défaillance pour la fonction de sécurité considérée (voir 7.4.4.1.1 c)). C'est-à-dire, qu'il convient que la somme des fréquences de défaillances dangereuses de tous les éléments de série, pour laquelle l'exclusion des anomalies est déclarée, ne dépasse pas 1 % de l'objectif chiffré de défaillance. Par ailleurs, l'applicabilité des exclusions des anomalies doit être justifiée compte tenu des anomalies systématiques éventuelles

NOTE La tolérance aux anomalies constitue la solution préférentielle pour obtenir l'assurance requise qu'une architecture robuste a été réalisée. Lorsque le paragraphe 7.4.4.3.2 s'applique, la justification a pour objet de démontrer que l'architecture alternative proposée prévoit une solution équivalente ou meilleure. Ceci peut dépendre du domaine technique et/ou de l'application. Des exemples comprennent: une alternative (par exemple, redondance analytique, substitution des données obtenues avec un capteur défaillant par les résultats d'un calcul physique effectué avec les données obtenues avec d'autres capteurs), utilisation d'éléments plus fiables de la même technologie (si disponibles), changement pour une technologie plus fiable, réduction de l'impact des défaillances de cause commune par l'emploi d'une technologie diversifiée, augmentation des marges de conception, restriction des conditions environnementales (par exemple pour les composants électroniques), réduction de l'incertitude de la fiabilité par regroupement d'un plus grand nombre de retours d'exploitations ou de jugements d'experts.

7.4.4.3.3 Si le parcours 2_H est choisi, alors les données de fiabilité utilisées pour quantifier l'effet des défaillances aléatoires du matériel (voir 7.4.5) doivent être:

a) basées sur les retours d'exploitations concernant les équipements utilisés dans une application et un environnement similaires; et

b) basées sur les données recueillies conformément aux normes internationales (par exemple, CEI 60300-3-2 ou ISO 14224); et

c) évaluées selon:

   i) la quantité de retours d'informations d'exploitation; et,

ii) les jugements d'experts, et si nécessaire,

iii) la réalisation d'essais spécifiques;

de manière à estimer la moyenne et le niveau d'incertitude (par exemple, l'intervalle de confiance à 90 % ou la loi de probabilité (voir Note 2) de chaque paramètre de fiabilité (par exemple, taux de défaillance) utilisé dans les calculs.

NOTE 1 Les utilisateurs finaux sont incités à organiser des recueils de données relatives à la fiabilité des composants, tel que décrit dans les normes publiées.

NOTE 2 L'intervalle de confiance à 90 % d'un taux de défaillance λ est l'intervalle $[\lambda_{5\ \%},\ \lambda_{95\ \%}]$ auquel la probabilité d'appartenance de sa valeur réelle est de 90 %. λ a une probabilité de 5 % d'être supérieur à $\lambda_{5\ \%}$ et inférieur à $\lambda_{95\ \%}$. Sur une base purement statistique, la moyenne du taux de défaillance peut être estimée en utilisant « l'estimation du maximum de vraisemblance » et les limites de confiance ($\lambda_{5\ \%}$, $\lambda_{95\ \%}$) peuvent être calculées à l'aide de la fonction χ^2. La précision dépend du temps d'observation cumulé et du nombre de défaillances constatées. La méthode bayésienne peut être utilisée pour traiter les observations statistiques, les jugements d'experts et les résultats d'essais spécifiques. Cette méthode peut être utilisée avec les fonctions de répartition probabilistes appropriées pour une simulation de Monte Carlo ultérieure.

Si le parcours 2_H est choisi, alors les incertitudes relatives aux données de fiabilité doivent être traitées pour pouvoir calculer l'objectif chiffré de défaillance (c'est-à-dire PFD_{avg} ou PFH) et le système doit être amélioré jusqu'à ce que la certitude de la réalisation d'un objectif chiffré de défaillance soit supérieure à 90 %.

7.4.4.3.4 Tous les éléments de type B utilisés avec le parcours 2_H doivent avoir, au minimum, une couverture de diagnostic d'au moins 60 %.

7.4.5 Exigences relatives à la quantification de l'effet de défaillances aléatoires du matériel

NOTE L'Article A.2 de la CEI 61508-6 donne une vue d'ensemble des étapes nécessaires lors de la réalisation de l'intégrité de sécurité du matériel requise, et présente la manière suivant laquelle le présent paragraphe est en rapport avec d'autres exigences de la présente norme.

7.4.5.1 Pour chaque fonction de sécurité, l'intégrité de sécurité obtenue du système E/E/PE relatif à la sécurité, due aux défaillances aléatoires du matériel (y compris les erreurs intermittentes) et aux défaillances aléatoires des processus de communication de données doit être estimée conformément à 7.4.5.2 et à 7.4.11, et doit être inférieure ou égale à l'objectif chiffré de défaillance défini dans la spécification des exigences de sécurité du système E/E/PE relatif à la sécurité (voir CEI 61508-1, 7.10).

NOTE Afin de démontrer que cela a été obtenu, il est nécessaire d'effectuer une prédiction de fiabilité pour la fonction de sécurité correspondante, en utilisant la technique appropriée (voir 7.4.5.2), et de comparer le résultat à l'objectif chiffré de défaillance de la fonction de sécurité considérée (voir CEI 61508-1).

7.4.5.2 L'estimation de la mesure de défaillance réalisée pour chaque fonction de sécurité, tel que requis par 7.4.5.1, doit tenir compte:

a) de l'architecture du système E/E/PE relatif à la sécurité, pour ce qui concerne ses sous-systèmes, dans la mesure où elle se rapporte à chacune des fonctions de sécurité considérées;

NOTE 1 Ceci implique de décider quels sont les modes de défaillance des éléments des sous-systèmes qui sont en configuration série (c'est-à-dire, que toute défaillance provoque la défaillance de la fonction de sécurité correspondante à exécuter) et quels sont les modes de défaillance qui sont en configuration parallèle (c'est-à-dire que des défaillances simultanées sont nécessaires pour provoquer la défaillance de la fonction de sécurité considérée).

b) de l'architecture de chaque sous-système du système E/E/PE relatif à la sécurité, en ce qui concerne ses éléments, dans la mesure où elle se rapporte à chacune des fonctions de sécurité considérées;

c) du taux de défaillance estimé de chaque sous-système et de ses éléments, dans tous les modes qui provoqueraient une défaillance dangereuse du système E/E/PE relatif à la sécurité, les défaillances étant celles détectées par des essais de diagnostic (voir 7.4.9.4 à 7.4.9.5). Il convient de fournir la justification des taux de défaillance en tenant compte de la source des données et de sa précision ou tolérance. Ceci peut inclure la prise en

compte et la comparaison des données d'un grand nombre de sources, ainsi que le choix des taux de défaillance de systèmes très proches de celui considéré. Les taux de défaillance utilisés pour quantifier l'effet des défaillances aléatoires du matériel et calculer la proportion de défaillances en sécurité ou la couverture de diagnostic doivent tenir compte des conditions de fonctionnement spécifiées.

NOTE 2 Pour prendre en compte les conditions de fonctionnement, il est généralement nécessaire d'ajuster les taux de défaillance à partir de bases de données, par exemple, en raison d'une charge de contact ou de la température.

d) de la sensibilité du système E/E/PE relatif à la sécurité et de ses sous-systèmes aux défaillances de cause commune (voir Notes 3 et 4). Les hypothèses formulées doivent être justifiées.

NOTE 3 Les défaillances dues aux effets de cause commune peuvent résulter d'effets autres que les défaillances réelles des éléments matériels (par exemple, perturbation électromagnétique, erreurs de décodage, etc.). Toutefois, de telles défaillances sont prises en compte, pour les besoins de la présente norme, dans la quantification de l'effet des défaillances aléatoires du matériel. L'échelonnement des essais des éléments réduit la probabilité d'une défaillance de cause commune.

NOTE 4 Dans le cas où les défaillances de cause commune sont identifiées entre les systèmes E/E/PE relatifs à la sécurité et les causes de sollicitation ou d'autres couches de protection, il doit être confirmé que cet élément a été pris en compte dans la détermination des exigences relatives au niveau d'intégrité de sécurité et à l'objectif chiffré de défaillance. Pour les méthodes de détermination des facteurs de cause commune, voir la CEI 61508-6, Annexe D.

e) de la couverture de diagnostic des essais de diagnostic (déterminée conformément à l'Annexe C), de l'intervalle entre les essais de diagnostic associé et du taux de défaillance dangereuse non révélée du diagnostic, dû aux défaillances aléatoires du matériel de chaque sous-système. Le cas échéant, seuls les essais de diagnostic qui satisfont aux exigences de 7.4.5.3 doivent être pris en considération. Les MTTR et MRT (voir 3.6.21 et 3.6.22 de la CEI 61508-4) doivent être pris en considération dans le modèle de fiabilité.

NOTE 5 En déterminant l'intervalle entre les essais de diagnostic, les intervalles entre chacun des essais qui contribuent à la couverture de diagnostic doivent être pris en compte.

f) des intervalles de temps auxquels des essais périodiques sont effectués pour révéler les anomalies dangereuses;

g) s'il est probable que l'essai périodique soit efficace à 100 %;

NOTE 6 Un essai périodique incorrect génère une fonction de sécurité non rétablie à l'état « de conditions de fonctionnement aussi bonnes qu'une nouvelle fonction », ce qui augmente par conséquent la probabilité de défaillance. Il convient de justifier les hypothèses formulées. Il convient, plus particulièrement, d'inclure la période de renouvellement des éléments ou l'effet sur la réduction du risque au cours du cycle de vie de la fonction de sécurité. Il est nécessaire de prendre en compte la durée des essais si l'entité est soumise à l'essai hors ligne pendant les essais effectifs.

h) des temps de réparation correspondant aux défaillances détectées;

NOTE 7 Le temps de réparation (MRT) constitue une partie de la durée moyenne de panne (MTTR) (voir 3.6.22 et 3.6.21 de la CEI 61508-4), qui comprend également le temps consacré à la détection d'une défaillance et toute période pendant laquelle la réparation n'est pas possible (voir Annexe B de la CEI 61508-6 qui donne un exemple de la manière suivant laquelle la durée moyenne de panne et le temps de réparation peuvent être utilisés pour calculer la probabilité d'une défaillance). La réparation peut être considérée instantanée uniquement lors de l'arrêt de l'EUC ou lorsque ce dernier est en état de sécurité pendant la réparation. Dans les situations où la réparation ne peut être effectuée que lorsque l'EUC est à l'arrêt et en état de sécurité, il est particulièrement important de tenir dûment compte de la période pendant laquelle aucune réparation n'est possible, particulièrement lorsque cette période est relativement importante. Il convient de tenir compte de tous les facteurs pertinents relatifs aux réparations.

i) de l'effet d'une erreur humaine aléatoire si une personne doit prendre des mesures pour obtenir la fonction de sécurité.

NOTE 8 Il convient de tenir compte de la nature aléatoire de l'erreur humaine dans les cas où une personne est informée de l'existence d'une condition dangereuse et doit prendre des mesures. Il convient également d'intégrer la probabilité de l'erreur humaine dans le calcul global.

j) du fait qu'un certain nombre de méthodes de modélisation sont disponibles et qu'il appartient à l'analyste de déterminer la méthode la plus appropriée, et ce, en fonction des circonstances. Les méthodes disponibles incluent l'analyse cause-conséquence (B.6.6.2 de la CEI 61508-7), l'analyse par arbre de panne (B.6.6.5 de la CEI 61508-7), les modèles de Markov (Annexe B de la CEI 61508-6 et B.6.6.6 de la CEI 61508-7), les diagrammes

de fiabilité (Annexe B de la CEI 61508-6 et B.6.6.7 de la CEI 61508-7) et les réseaux de Pétri (Annexe B de la CEI 61508-6 et B.2.3.3 de la CEI 61508-7).

NOTE 9 L'Annexe B de la CEI 61508-6 décrit une approche simplifiée qui peut être utilisée pour estimer la probabilité moyenne de non fonctionnement en cas de sollicitation d'une fonction de sécurité due à des défaillances aléatoires du matériel, afin de déterminer qu'une architecture satisfait à l'objectif chiffré de défaillance requis.

NOTE 10 L'Article A.2 de la CEI 61508-6 donne une vue d'ensemble des étapes nécessaires lors de la réalisation de l'intégrité de sécurité du matériel requise, et présente la manière suivant laquelle le présent paragraphe est en rapport avec d'autres exigences de la présente norme.

NOTE 11 Il est nécessaire de quantifier séparément, pour chaque fonction de sécurité, la fiabilité des systèmes E/E/PE relatifs à la sécurité, dans la mesure où différents modes de défaillance des éléments s'appliquent et où l'architecture des systèmes E/E/PE relatifs à la sécurité (en termes de redondance) peut également varier.

7.4.5.3 Lors de la quantification de l'effet des défaillances aléatoires du matériel d'un sous-système, avec une tolérance aux anomalies nulle et l'application partielle ou totale d'une fonction de sécurité, fonctionnant en mode sollicitation élevée ou en mode continu, le diagnostic doit être crédible uniquement si:

– la somme de l'intervalle entre les essais de diagnostic et du temps nécessaire à l'exécution de l'action spécifiée pour obtenir ou maintenir un état de sécurité est inférieure au temps de sécurité du processus; ou

– en mode de fonctionnement à sollicitation élevée, le rapport du taux des essais de diagnostic sur la fréquence de sollicitation est supérieur ou égal à 100.

7.4.5.4 L'intervalle entre les essais de diagnostic de tout sous-système:

– avec une tolérance aux anomalies supérieure à zéro et l'application partielle ou totale d'une fonction de sécurité, fonctionnant en mode sollicitation élevée ou en mode continu; ou

– qui applique en totalité ou en partie une fonction de sécurité, fonctionnant en mode faible sollicitation,

doit être tel que la somme de l'intervalle entre les essais de diagnostic et du temps nécessaire à l'exécution de la réparation d'une défaillance détectée, est inférieure à la durée moyenne de rétablissement (MTTR) utilisée dans le calcul pour déterminer l'intégrité de sécurité obtenue pour la fonction de sécurité concernée.

7.4.5.5 Si, pour une conception particulière, l'exigence d'intégrité de sécurité de la fonction de sécurité considérée n'est pas obtenue, alors:

a) déterminer les éléments, sous-systèmes et/ou paramètres contribuant le plus au taux de défaillance calculé de la fonction;

b) évaluer l'effet des mesures possibles d'amélioration sur les éléments, sous-systèmes ou paramètres critiques identifiés (par exemple, composants plus fiables, défenses supplémentaires contre les défaillances de mode commun, couverture de diagnostic accrue, redondance accrue, intervalle entre les essais périodiques réduit, étalement des essais, etc.);

c) choisir et mettre en œuvre les améliorations applicables;

d) répéter les étapes nécessaires pour déterminer la nouvelle probabilité de défaillance aléatoire du matériel.

7.4.6 Exigences pour l'évitement des anomalies systématiques

NOTE Voir 7.4.2.2 c) pour les détails lorsque les exigences du présent paragraphe s'appliquent.

7.4.6.1 Un ensemble approprié de techniques et de mesures doit être conçu et utilisé pour éviter l'introduction d'anomalies pendant la conception et le développement des matériels et logiciel du système E/E/PE relatif à la sécurité (voir Tableau B.2 et CEI 61508-3).

NOTE La présente norme ne comporte aucune exigence spécifique relative à l'évitement des anomalies systématiques lors de la conception des circuits intégrés électroniques de série, tels que les microprocesseurs usuels. Ceci est dû au fait que la probabilité d'occurrence des anomalies avec ce type de dispositifs est réduite au minimum par le biais de procédures de développement contraignantes, d'essais sévères et d'une large expérience d'utilisation avec un retour d'information important de la part des utilisateurs. Pour les circuits intégrés électroniques ne pouvant être justifiés sur cette base (par exemple, nouveaux dispositifs ou ASIC), les exigences relatives aux ASIC (voir 7.4.6.7 et Annexe F informative) s'appliquent si ces derniers doivent être utilisés dans un système E/E/PE relatif à la sécurité. En cas de doute (concernant la large expérience d'utilisation avec un retour d'information important de la part des utilisateurs), il convient de tenir compte des exigences relatives à « l'expérience pratique » spécifiées au Tableau B.6, avec une efficacité « faible » pour SIL 1 et SIL 2, une efficacité "moyenne" pour SIL 3 et une efficacité "élevée" pour SIL 4.

7.4.6.2 Conformément au niveau d'intégrité de sécurité requis, la méthode de conception choisie doit inclure des dispositions qui facilitent:

a) la transparence, la modularité et les autres caractéristiques permettant de maîtriser la complexité;

b) une expression claire et précise
   - de la fonctionnalité;
   - des interfaces entre les sous-systèmes et les éléments;
   - de la séquence et des informations temporelles,
   - de la simultanéité et de la synchronisation;

c) une documentation claire et précise ainsi que la communication d'informations;

d) la vérification et la validation.

7.4.6.3 Les exigences de maintenance, destinées à assurer le maintien de la conformité aux exigences d'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité, doivent être formalisées pendant l'étape de conception.

7.4.6.4 Le cas échéant, des outils d'essai automatiques et des outils de développement intégrés doivent être utilisés.

7.4.6.5 Pendant la conception, des essais d'intégration des systèmes E/E/PE doivent être planifiés. La documentation du programme d'essai doit comprendre

a) les types d'essais à réaliser ainsi que les procédures à suivre;

b) l'environnement, les outils, la configuration et les programmes d'essai;

c) les critères de succès/échec.

7.4.6.6 Pendant la conception, les activités qui peuvent être réalisées dans les locaux du développeur doivent être différenciées de celles qui nécessitent un accès au site de l'utilisateur.

7.4.6.7 Un ensemble approprié de techniques et de mesures essentielles doit être utilisé pour éviter l'introduction d'anomalies pendant la conception et le développement des ASIC.

NOTE Les techniques et mesures qui soutiennent la réalisation des propriétés pertinentes sont fournies à l'Annexe F informative. Le cycle de vie de développement des ASIC associé est illustré à la Figure 3.

7.4.7 Exigences pour la maîtrise des anomalies systématiques

NOTE Voir 7.4.2.2 c) pour les détails lorsque les exigences du présent paragraphe s'appliquent.

7.4.7.1 Afin de maîtriser les anomalies systématiques, la conception des systèmes E/E/PE doit avoir des caractéristiques telles que les systèmes E/E/PE relatifs à la sécurité soient tolérants:

a) aux anomalies de conception résiduelles du matériel, sauf si l'éventualité d'anomalies de conception du matériel peut être exclue (voir Tableau A.15);

b) aux contraintes environnementales, y compris les perturbations électromagnétiques (voir Tableau A.16);

c) aux erreurs imputables à l'opérateur de l'EUC (voir Tableau A.17);

d) aux anomalies de conception résiduelles du logiciel (voir 7.4.3 de la CEI 61508-3 ainsi que le tableau correspondant);

e) aux erreurs et autres effets provenant de tout processus de communication de données (voir 7.4.11).

7.4.7.2 La maintenabilité et la testabilité doivent être prises en compte lors des activités de conception et de développement afin de faciliter la mise en œuvre de ces propriétés dans les systèmes E/E/PE relatifs à la sécurité définitifs.

7.4.7.3 La conception des systèmes E/E/PE relatifs à la sécurité doit tenir compte des aptitudes et des limites humaines et doit convenir aux actions attribuées aux opérateurs et au personnel chargé de la maintenance. Les exigences de conception doivent être fondées sur de bonnes pratiques en termes de facteur humain et doivent s'adapter au niveau probable de formation ou de sensibilisation des opérateurs comme, par exemple, dans le cas de systèmes E/E/PE relatifs à la sécurité de série, où l'opérateur n'est pas un professionnel.

NOTE 1 Il convient que l'objectif de la conception soit d'éviter ou d'éliminer, dans toute la mesure du possible, les erreurs humaines critiques prévisibles imputables aux opérateurs ou au personnel de maintenance, ou que l'action nécessite une confirmation secondaire avant finalisation.

NOTE 2 Il est admis que certaines erreurs dues aux opérateurs ou au personnel de maintenance ne soient pas récupérables par des systèmes E/E/PE relatifs à la sécurité, par exemple si elles ne sont pas détectables ou récupérables de manière réaliste si ce n'est par inspection directe, telles que certaines défaillances mécaniques de l'EUC.

7.4.8 Exigences relatives au comportement du système, lors de la détection d'une anomalie

NOTE Les exigences du présent paragraphe s'appliquent aux fonctions de sécurité spécifiées mises en œuvre par un système E/E/PE relatif à la sécurité unique lorsque la fonction de sécurité globale n'a pas été allouée à des dispositifs externes de réduction de risque.

7.4.8.1 La détection d'une anomalie dangereuse (par les essais de diagnostic, les essais périodiques ou tout autre moyen) dans tout sous-système qui a une tolérance aux anomalies du matériel supérieure à zéro, doit déclencher soit:

a) une action spécifiée pour obtenir ou maintenir un état de sécurité (voir Note); ou

b) l'isolement de la partie du sous-système présentant l'anomalie afin de permettre la poursuite en sécurité de l'exploitation de l'EUC, pendant que la partie présentant une défaillance est réparée. Si la réparation n'est pas accomplie pendant la durée moyenne de réparation (MRT), voir 3.6.22 de la CEI 61508-4, prise comme hypothèse dans le calcul de la probabilité de défaillance aléatoire du matériel (voir 7.4.5.2), alors une action spécifiée doit être entreprise afin d'obtenir ou de maintenir un état de sécurité (voir Note).

NOTE L'action spécifiée requise pour obtenir ou maintenir un état de sécurité est définie dans les exigences de sécurité relatives aux systèmes E/E/PE (voir CEI 61508-1, 7.10). Elle peut consister, par exemple, en l'arrêt de sécurité de l'EUC, ou de la partie de ce dernier qui repose, pour la sécurité fonctionnelle, sur le sous-système présentant l'anomalie.

7.4.8.2 La détection d'une anomalie dangereuse (par les essais de diagnostic, les essais périodiques ou tout autre moyen) dans tout sous-système qui a une tolérance aux anomalies du matériel nulle, doit, dans le cas où ce sous-système est utilisé uniquement par une (des) fonction(s) de sécurité exploitée(s) en mode faible sollicitation, déclencher soit:

a) une action spécifiée pour obtenir ou maintenir un état de sécurité; ou

b) la réparation du sous-système présentant une défaillance, pendant la durée moyenne de réparation (MRT), voir 3.6.22 de la CEI 61508-4, prise comme hypothèse dans le calcul de la probabilité de défaillance aléatoire du matériel (voir 7.4.5.2). Pendant ce délai, la sécurité continue de l'EUC doit être assurée par des mesures et contraintes supplémentaires. L'intégrité de sécurité procurée par ces mesures et contraintes doit être

au moins égale à l'intégrité de sécurité procurée par le système E/E/PE relatif à la sécurité en l'absence de toute anomalie. Les mesures et contraintes supplémentaires doivent être spécifiées dans les procédures d'exploitation et de maintenance des systèmes E/E/PE (voir 7.6).

NOTE L'action spécifiée requise pour obtenir ou maintenir un état de sécurité est définie dans la spécification des exigences de sécurité relatives aux systèmes E/E/PE (voir 7.10 de la CEI 61508-1). Elle peut consister, par exemple, en l'arrêt de sécurité de l'EUC, ou de la partie de ce dernier qui repose, pour la sécurité fonctionnelle, sur le sous-système présentant l'anomalie.

7.4.8.3 La détection d'une anomalie dangereuse (par les essais de diagnostic, les essais périodiques ou tout autre moyen) dans tout sous-système qui a une tolérance aux anomalies du matériel nulle, doit, dans le cas où un sous-système met en œuvre une (des) fonction(s) de sécurité exploitée(s) en mode sollicitation élevée ou continu, déclencher une action spécifiée pour obtenir ou maintenir un état de sécurité (voir Note).

NOTE L'action spécifiée requise pour obtenir ou maintenir un état de sécurité est définie dans la spécification des exigences de sécurité relatives aux systèmes E/E/PE (voir 7.10 de la CEI 61508-1). Elle peut consister, par exemple, en l'arrêt de sécurité de l'EUC, ou de la partie de ce dernier qui repose, pour la sécurité fonctionnelle, sur le sous-système présentant l'anomalie.

7.4.9 Exigences relatives à la mise en œuvre du système E/E/PE

7.4.9.1 Le système E/E/PE relatif à la sécurité doit être mis en œuvre selon la spécification des exigences de conception des systèmes E/E/PE (7.2.3).

7.4.9.2 Tous les sous-systèmes et leurs éléments qui sont utilisés par une ou plusieurs fonctions de sécurité doivent être identifiés et documentés en tant que sous-systèmes et éléments relatifs à la sécurité.

7.4.9.3 Les informations suivantes doivent être disponibles pour chaque sous-système relatif à la sécurité et chaque élément selon le cas (voir également 7.4.9.4):

NOTE Il est nécessaire que le fournisseur d'un sous-système ou d'un élément, déclaré comme conforme à la CEI 61508, mette ces informations à disposition du concepteur d'un système relatif à la sécurité (ou un autre sous-système ou élément) dans le manuel de sécurité d'article conforme, voir Annexe D.

a) une spécification fonctionnelle du sous-système et de ses éléments le cas échéant;

b) toutes instructions ou contraintes relatives à l'application du sous-système et de ses éléments, qu'il convient d'observer afin d'éviter des défaillances systématiques du sous-système;

c) la capabilité systématique de chaque élément (voir 7.4.2.2 c));

d) l'identification de la configuration matérielle et/ou logicielle de l'élément afin de permettre la gestion de configuration du système E/E/PE relatif à la sécurité, conformément à 6.2.1 de la CEI 61508-1;

e) la preuve documentaire qu'il a été vérifié que le sous-système et ses éléments satisfont aux exigences fonctionnelles spécifiées et aux capabilités systématiques conformément à la spécification des exigences de conception des systèmes E/E/PE (voir 7.2.3).

7.4.9.4 Les informations suivantes doivent être disponibles pour chaque élément relatif à la sécurité susceptible de présenter une défaillance aléatoire du matériel (voir également 7.4.9.3 et 7.4.9.5):

NOTE 1 Il est nécessaire que le fournisseur d'un élément, déclaré comme conforme à la série CEI 61508, mette ces informations à disposition du concepteur d'un système relatif à la sécurité dans le manuel de sécurité des éléments, voir Annexe D.

a) les modes de défaillance de l'élément (en termes du comportement de ses sorties), dus aux défaillances aléatoires du matériel, qui entraînent une défaillance de la fonction de sécurité et qui ne sont pas détectés par les essais de diagnostic internes à l'élément, ou qui ne sont pas détectables par un diagnostic externe à l'élément (voir 7.4.9.5);

b) pour chaque mode de défaillance défini en a), un taux de défaillance estimé compte tenu des conditions de fonctionnement spécifiées;

c) les modes de défaillance de l'élément (en termes du comportement de ses sorties), dus aux défaillances aléatoires du matériel, qui entraînent une défaillance de la fonction de sécurité et qui sont détectés par les essais de diagnostic internes à l'élément, ou qui sont détectables par un diagnostic externe à l'élément (voir 7.4.9.5);

d) pour chaque mode de défaillance défini en c), un taux de défaillance estimé compte tenu des conditions de fonctionnement spécifiées;

e) toutes limitations concernant l'environnement de l'élément qu'il convient d'observer afin de maintenir la validité des taux de défaillance estimés dus à des défaillances aléatoires du matériel;

f) toutes limitations concernant la durée de vie de l'élément qu'il convient de ne pas dépasser afin de maintenir la validité des taux de défaillance estimés dus à des défaillances aléatoires du matériel;

g) tout essai périodique et/ou toutes exigences de maintenance;

h) pour chaque mode de défaillance défini en c) qui est détecté par un diagnostic interne à l'élément, la couverture de diagnostic calculée conformément à l'Annexe C (voir Note 2);

i) pour chaque mode de défaillance défini en c) qui est détecté par un diagnostic interne à l'élément, l'intervalle entre les essais de diagnostic (voir Note 2);

NOTE 2 La couverture de diagnostic et l'intervalle entre les essais de diagnostic sont nécessaires pour affirmer le bénéfice de l'action des essais de diagnostic exécutés sur l'élément interne au modèle d'intégrité de sécurité du matériel du système E/E/PE relatif à la sécurité (voir 7.4.5.2, 7.4.5.3 et 7.4.5.4).

j) le taux de défaillance du diagnostic, dû aux défaillances aléatoires du matériel;

k) les informations supplémentaires (par exemple, les temps de réparation) qui sont nécessaires pour pouvoir déduire le temps moyen de dépannage (MRT), voir 3.6.22 de la CEI 61508-4, à la suite de la détection d'une anomalie par le diagnostic;

l) toutes les informations nécessaires pour permettre de déduire la proportion de défaillances en sécurité (SFF) de l'élément telle qu'appliquée au système E/E/PE relatif à la sécurité, déterminée conformément à l'Annexe C, y compris le classement comme type A ou type B selon 7.4.4;

m) la tolérance aux anomalies du matériel, pour l'élément.

7.4.9.5 Les taux de défaillance estimés, dus à des défaillances aléatoires du matériel, pour les éléments (voir 7.4.9.4 a) et c)), peuvent être déterminés soit:

a) par une analyse des modes de défaillance et des effets de la conception utilisant les données de taux de défaillance des éléments provenant d'une source industrielle reconnue; ou

b) par expérience d'une utilisation antérieure de l'élément dans un environnement similaire (voir 7.4.10).

NOTE 1 Il convient que toutes les données utilisées relatives aux taux de défaillance aient un niveau de confiance d'au moins 70 %. La détermination statistique du niveau de confiance est définie dans la référence [9] de la Bibliographie. Pour un terme équivalent: « niveau de signification », se reporter à la référence [10].

NOTE 2 Si des données relatives aux défaillances spécifiques au site d'utilisation sont disponibles, il est alors préférable de les utiliser. Si tel n'est pas le cas, il peut alors être nécessaire d'utiliser des données génériques.

NOTE 3 Bien qu'un taux de défaillance constant soit pris comme hypothèse par la plupart des estimations statistiques, cela s'applique uniquement si la durée de vie utile des éléments n'est pas dépassée. Au delà de leur durée de vie utile (c'est-à-dire lorsque la probabilité de défaillance s'accroît de manière significative en fonction du temps), les résultats de la plupart des méthodes de calcul probabilistes sont par conséquent sans intérêt. Il convient ainsi que toute estimation probabiliste inclue une spécification de la durée de vie utile des éléments. La durée de vie utile dépend fortement de l'élément lui–même et de ses conditions d'utilisation – la température en particulier (par exemple, les condensateurs électrolytiques peuvent y être très sensibles). L'expérience a montré que la durée de vie utile se situe souvent dans une plage comprise entre 8 et 12 ans. Elle peut toutefois être significativement moindre si les éléments sont utilisés dans des conditions proches des limites de leur spécification. Les éléments ayant des durées de vie utile plus longues ont tendance à être considérablement plus chers.

7.4.9.6 Les fournisseurs doivent prévoir un manuel de sécurité d'article conforme, conformément à l'Annexe D, pour chaque article conforme qu'ils proposent et pour lequel ils déclarent la conformité à la série CEI 61508.

7.4.9.7 Le fournisseur doit documenter une justification de toutes les informations contenues dans chaque manuel de sécurité d'article conforme.

NOTE 1 Il est essentiel que les performances de sécurité déclarées d'un élément soient soutenues par un nombre de preuves suffisant. Les déclarations non soutenues par des preuves ne permettent pas d'établir le caractère approprié et l'intégrité de la fonction de sécurité à laquelle l'élément contribue.

NOTE 2 La disponibilité des preuves peut faire l'objet de restrictions d'ordre commercial ou juridique. Ces restrictions ne relèvent pas du domaine d'application de la présente norme. Si ces restrictions impliquent qu'il n'y a aucune relation entre l'évaluation de la sécurité fonctionnelle et les preuves existantes, alors l'élément ne convient pas à une utilisation avec les systèmes E/E/PE relatifs à la sécurité.

7.4.10 Exigences relatives aux éléments éprouvés par une utilisation antérieure

NOTE Voir 7.4.2.2 c) pour les détails lorsque les exigences du présent paragraphe s'appliquent.

7.4.10.1 Un élément doit être considéré comme éprouvé par une utilisation antérieure uniquement lorsque sa fonctionnalité est clairement limitée et spécifiée et lorsqu'un nombre de preuves documentaires appropriées suffisant existe pour démontrer que la probabilité d'occurrence de toutes anomalies systématiques dangereuses est suffisamment faible pour pouvoir obtenir les niveaux d'intégrité de sécurité requis des fonctions de sécurité qui utilisent l'élément. Les preuves doivent être basées sur l'analyse d'une expérience opérationnelle d'une configuration spécifique de l'élément, ainsi que sur une analyse et des essais de pertinence.

NOTE L'analyse et les essais de pertinence se concentrent sur la démonstration des performances des éléments dans le cadre de l'application prévue. Il convient de tenir compte des résultats des analyses et des essais existants. Ceci comprend le comportement fonctionnel, la précision, le comportement dans le cas d'une anomalie, la réaction dans le temps, la réaction à une surcharge, la facilité d'utilisation (par exemple, prévention de toute erreur humaine) et la maintenabilité.

7.4.10.2 Les preuves documentaires requises par 7.4.10.1 doivent démontrer que:

a) les conditions d'utilisation précédentes (voir Note 1) de l'élément spécifique sont les mêmes, ou suffisamment proches, de celles de l'élément dans le système E/E/PE relatif à la sécurité;

NOTE 1 Les conditions d'utilisation (profil d'exploitation) comprennent tous les facteurs qui peuvent déclencher les anomalies systématiques dans le matériel et le logiciel de l'élément. Par exemple, l'environnement, les modes d'utilisation, les fonctions accomplies, la configuration, les interfaces avec d'autres systèmes, le système d'exploitation, le compilateur, les facteurs humains. Des conditions rigoureuses pour la similarité du profil d'exploitation sont décrites dans la CEI 61784-3.

b) le taux de défaillance dangereuse n'a pas été dépassé au cours d'une exploitation précédente.

NOTE 2 Voir la CEI 61508-7, Annexe D, pour des recommandations sur l'utilisation d'une approche probabiliste afin de déterminer l'intégrité de sécurité pour logiciels pré-développés sur la base de l'expérience opérationnelle.

NOTE 3 La collecte des preuves relatives aux éléments éprouvés par une utilisation antérieure nécessite la mise en place d'un système efficace de signalement des défaillances

7.4.10.3 Lorsqu'il existe une différence entre les conditions d'utilisation antérieures et celles que rencontre le système E/E/PE relatif à la sécurité, une analyse d'impact sur les différences constatées doit alors être effectuée sur la base d'une combinaison de méthodes analytiques appropriées et d'essais, afin de déterminer que la probabilité de toute anomalie systématique dangereuse est suffisamment faible pour que le(s) niveau(x) d'intégrité de sécurité requis de la (des) fonction(s) de sécurité qui utilise(nt) cet élément soit (soient) obtenu(s).

7.4.10.4 Une justification de la sécurité éprouvée par une utilisation antérieure doit être documentée, en utilisant les informations disponibles de 7.4.10.2, en indiquant que l'élément soutient la fonction de sécurité requise avec l'intégrité de sécurité systématique nécessaire. La documentation doit comprendre:

a) l'analyse et les essais de pertinence de l'élément pour l'application prévue;

b) la démonstration de l'équivalence entre l'exploitation prévue et l'expérience opérationnelle précédente, y compris l'analyse d'impact sur les différences;

c) les preuves statistiques.

7.4.10.5 Les facteurs suivants doivent être pris en compte en déterminant si les exigences ci-dessus (7.4.10.1 à 7.4.10.4) sont ou non satisfaites, tant en termes de couverture que de degré de détail des informations disponibles (voir également 4.1 de la CEI 61508-1):

a) la complexité de l'élément;

b) la capabilité systématique de l'élément requise;

c) l'aspect novateur de la conception.

7.4.10.6 Des preuves satisfaisantes doivent permettre d'attester que les fonctions existantes de l'élément qui ne sont pas couvertes par la démonstration de validation en utilisation ne peuvent pas altérer l'intégrité de sécurité des fonctions de l'élément effectivement utilisées.

NOTE Cette exigence peut être réalisée en s'assurant de la désactivation physique ou électrique des fonctions, ou de l'exclusion de la configuration opérationnelle du logiciel de mise en œuvre de ces fonctions, ou par d'autres formes d'arguments et de preuves.

7.4.10.7 Toute modification future d'un élément éprouvé par une utilisation antérieure doit satisfaire aux exigences de 7.8 et de la CEI 61508-3.

7.4.11 Exigences supplémentaires relatives aux communications de données

7.4.11.1 Lorsque la communication de données est utilisée dans la mise en œuvre d'une fonction de sécurité, la mesure de défaillance (telle que la probabilité d'occurrence d'une défaillance non détectée) du processus de communication doit alors être estimée en tenant compte des erreurs de transmission, des répétitions, des suppressions, des insertions, des modifications de la séquence, de la corruption, du retard et de l'usurpation. Cette mesure de défaillance doit être prise en compte lors de l'estimation de la mesure de défaillance de la fonction de sécurité, due à des défaillances aléatoires (voir 7.4.5).

NOTE Le terme « usurpation » signifie que le contenu exact d'un message n'est pas correctement identifié. Par exemple, un message provenant d'un élément qui n'est pas de sécurité est identifié incorrectement comme un message provenant d'un élément de sécurité.

7.4.11.2 Les techniques et mesures nécessaires à la réalisation de la mesure de défaillance requise (telle que la probabilité d'occurrence d'une défaillance non détectée) du processus de communication (voir 7.4.11.1) doivent être appliquées selon les exigences de la présente norme et de la CEI 61508-3. Cela permet l'utilisation de deux approches possibles:

– le canal de communication complet doit être conçu, mis en œuvre et validé conformément à la série CEI 61508 et à la CEI 61784-3 ou à la série CEI 62280. Ce canal est communément appelé « canal blanc » (voir Figure 7 a); ou

– les parties du canal de communication ne sont pas conçues ou validées conformément à la série CEI 61508. Ce canal est communément appelé « canal noir » (voir Figure 7 b). Dans ce cas, les mesures nécessaires pour établir les caractéristiques de défaillance du processus de communication doivent être appliquées aux sous-systèmes ou éléments E/E/PE relatifs à la sécurité qui constituent une interface avec le canal de communication, conformément à la série CEI 61784-3 ou la CEI 62280 le cas échéant.

NOTE La référence [12] dans la Bibliographie contient les détails de certains profils de communication pour la sécurité fonctionnelle.

Figure 7 (a) Canal blanc

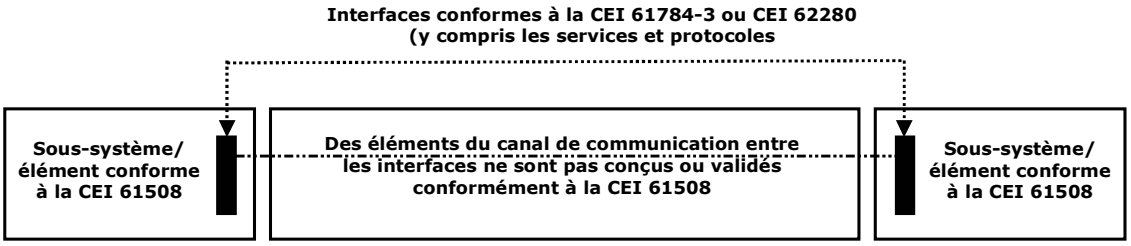


Figure 7 (b) Canal noir

Figure 7 – Architectures pour la communication des données

7.5 Intégration des systèmes E/E/PE

NOTE Cette phase correspond à la case 10.4 de la Figure 2.

7.5.1 Objectif

L'objectif des exigences du présent paragraphe est d'intégrer et de soumettre à l'essai le système E/E/PE relatif à la sécurité.

7.5.2 Exigences

7.5.2.1 Le système E/E/PE relatif à la sécurité doit être intégré conformément à la conception du système E/E/PE spécifiée et doit être soumis à l'essai selon les essais d'intégration du système E/E/PE spécifiés (voir 7.4.2.11).

7.5.2.2 Dans le cadre de l'intégration de tous les modules dans le système E/E/PE relatif à la sécurité, ce système doit être soumis à l'essai comme spécifié (voir 7.4). Ces essais doivent démontrer que tous les modules interagissent de manière correcte pour remplir leur fonction prévue et sont conçus de manière à ne pas exécuter de fonctions non prévues.

NOTE 1 Ceci n'implique pas de soumettre aux essais toutes les combinaisons d'entrée. Il peut être suffisant de soumettre aux essais toutes les classes d'équivalence (voir B.5.2 de la CEI 61508-7). Il est admis que le nombre de cas d'essais peut être réduit à un niveau acceptable par une analyse statique (voir B.6.4 de la CEI 61508-7), une analyse dynamique (voir B.6.5 de la CEI 61508-7) ou une analyse des défaillances (voir B.6.6 de la CEI 61508-7). Les exigences peuvent être plus facilement satisfaites si le développement du système E/E/PE relatif à la sécurité est obtenu conformément aux méthodes donnant lieu à une conception structurée (voir B.3.2 de la CEI 61508-7) ou à des méthodes semi-formelles (voir B.2.3 de la CEI 61508-7).

NOTE 2 Lorsque le développement est effectué selon les méthodes formelles (voir B.2.2 de la CEI 61508-7) ou en utilisant des preuves ou des déclarations formelles (voir C.5.12 et C.3.3 de la CEI 61508-7), il est admis que le domaine d'application de ces essais soit réduit.

NOTE 3 Il est également admis d'utiliser des preuves statistiques (voir B.5.3 de la CEI 61508-7).

7.5.2.3 L'intégration du logiciel de sécurité dans le système E/E/PE relatif à la sécurité doit être réalisée selon 7.5 de la CEI 61508-3.

7.5.2.4 La documentation appropriée des essais d'intégration du système E/E/PE relatif à la sécurité doit être produite, en indiquant les résultats des essais et en précisant la conformité ou non aux objectifs et critères spécifiés pendant la phase de conception et de

développement. En cas de défaillance, les raisons de cette dernière et les actions correctives doivent être documentées.

7.5.2.5 Pendant les essais d'intégration, les modifications ou les changements effectués sur le système E/E/PE relatif à la sécurité doivent faire l'objet d'une analyse d'impact qui doit identifier tous les sous-systèmes et éléments concernés ainsi que les activités de nouvelle vérification nécessaires.

7.5.2.6 Les essais d'intégration du système E/E/PE doivent consigner par écrit les informations suivantes:

a) la version de la spécification d'essai utilisée;

b) les critères d'acceptation des essais d'intégration;

c) la version du système E/E/PE relatif à la sécurité soumis aux essais;

d) les outils et les équipements utilisés ainsi que les données d'étalonnage;

e) les résultats de chaque essai;

f) toute divergence entre les résultats prévus et les résultats réels;

g) l'analyse effectuée ainsi que les décisions prises quant à la poursuite de l'essai ou l'émission d'une demande de modification, dans le cas où des divergences apparaissent.

7.5.2.7 Pour éviter les anomalies au cours de l'intégration du système E/E/PE, un ensemble approprié de techniques et de mesures, conforme au Tableau B.3, doit être utilisé.

7.6 Procédures d'exploitation et de maintenance des systèmes E/E/PE

NOTE Cette phase correspond à la case 10.5 de la Figure 2.

7.6.1 Objectif

L'objectif des exigences du présent paragraphe est de développer des procédures permettant d'assurer que la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité est maintenue pendant l'exploitation et la maintenance.

7.6.2 Exigences

7.6.2.1 Les procédures d'exploitation et de maintenance des systèmes E/E/PE doivent être rédigées. Elles doivent spécifier les informations suivantes:

a) les actions périodiques qu'il est nécessaire d'exécuter afin de maintenir la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité «telle qu'elle a été conçue», y compris le remplacement systématique des éléments dont la durée de vie est prédéfinie, par exemple, les ventilateurs de refroidissement, les accumulateurs; etc.

b) les actions et contraintes qui sont nécessaires (par exemple, pendant l'installation, le démarrage, le fonctionnement normal, les essais individuels de série, les perturbations prévisibles, les anomalies ou défaillances, ainsi que l'arrêt) pour éviter un état de non-sécurité et/ou réduire les conséquences d'un événement dangereux;

c) la documentation qu'il est nécessaire de maintenir en cas de défaillance du système ainsi que les fréquences de sollicitation sur le système E/E/PE relatif à la sécurité;

d) la documentation qu'il est nécessaire de maintenir, montrant les résultats des audits et des essais effectués sur le système E/E/PE relatif à la sécurité;

e) les procédures de maintenance à suivre lorsque des anomalies ou défaillances se produisent dans le système E/E/PE relatif à la sécurité, y compris:

   – les procédures de diagnostic et de réparation des anomalies;

   – les procédures de revalidation;

   – les exigences relatives au compte-rendu de maintenance;

– les procédures de revalidation si les équipements d'origine ne sont plus disponibles ou ont été remplacés par de nouvelles versions.

f) les procédures de compte rendu d'exécution de la maintenance doivent être spécifiées. Notamment:

– les procédures de compte rendu de défaillances;

– les procédures d'analyse de défaillances;

g) les outils nécessaires à la maintenance et à la revalidation ainsi que les procédures de maintenance des outils et des équipements.

NOTE 1 Il peut être avantageux, tant pour des raisons de sécurité que d'économie, d'intégrer les procédures d'exploitation et de maintenance des systèmes E/E/PE aux procédures globales d'exploitation et de maintenance de l'EUC.

NOTE 2 Il convient que les procédures d'exploitation et de maintenance des systèmes E/E/PE incluent les procédures de modification du logiciel (voir CEI 61508-3, 7.8).

7.6.2.2 Les procédures d'exploitation et de maintenance des systèmes E/E/PE relatifs à la sécurité doivent être constamment mises à niveau sur la base de données telles que (1) les résultats des audits de sécurité fonctionnelle et (2) les essais effectués sur le système E/E/PE relatif à la sécurité.

7.6.2.3 Les actions de maintenance périodique requises pour maintenir la sécurité fonctionnelle requise (telle que conçue) du système E/E/PE relatif à la sécurité doivent être déterminées par une méthode systématique. Cette méthode doit déterminer les défaillances non révélées de tous les éléments relatifs à la sécurité (des capteurs aux éléments finaux) qui pourraient entraîner une réduction de l'intégrité de sécurité obtenue. Les méthodes appropriées comprennent:

– l'examen des arbres de panne;

– l'analyse des modes de défaillance et de leurs effets.

NOTE 1 La prise en compte des facteurs humains constitue un élément clé pour la détermination des actions requises et de la (les) interface(s) appropriée(s) avec le système E/E/PE relatif à la sécurité.

NOTE 2 Des essais périodiques sont effectués selon la fréquence nécessaire pour atteindre l'objectif chiffré de défaillance.

NOTE 3 La fréquence des essais périodiques, l'intervalle entre les essais de diagnostic et la durée de réparation qui en découle dépendent de plusieurs facteurs (voir Annexe B de la CEI 61508-6), y compris:

– l'objectif chiffré de défaillance associé au niveau d'intégrité de sécurité;

– l'architecture;

– la couverture de diagnostic des essais de diagnostic; et

– la fréquence de sollicitation prévue.

NOTE 4 La fréquence des essais périodiques et l'intervalle entre les essais de diagnostic sont susceptibles d'influencer fortement la réalisation de l'intégrité de sécurité du matériel. L'un des principaux justificatifs de l'analyse de fiabilité du matériel (voir 7.4.5.2) est d'assurer que les fréquences des deux types d'essais conviennent à l'intégrité de sécurité cible du matériel.

NOTE 5 Il convient de respecter les exigences de maintenance du fabricant et de ne pas se fier uniquement aux méthodes de maintenance basée sur la fiabilité jusqu'à ce qu'elles puissent être pleinement justifiées (par exemple, par une analyse de fiabilité qui démontre que les objectifs chiffrés de défaillance des systèmes E/E/PE relatifs à la sécurité sont satisfaits).

7.6.2.4 L'impact potentiel des procédures d'exploitation et de maintenance des systèmes E/E/PE sur l'EUC doit être évalué.

7.6.2.5 Pour l'évitement des anomalies et des défaillances au cours des procédures d'exploitation et de maintenance des systèmes E/E/PE, un ensemble approprié de techniques et de mesures, conforme au Tableau B.4, doit être utilisé.

7.7 Validation de la sécurité des systèmes E/E/PE

NOTE Cette phase correspond à la case 10.6 de la Figure 2.

7.7.1 Objectif

L'objectif des exigences du présent paragraphe est de valider la conformité, à tous égards, des systèmes E/E/PE relatifs à la sécurité aux exigences de sécurité, en termes de fonctions de sécurité et d'intégrité de sécurité requises (voir 7.2 susmentionné et 7.10 de la CEI 61508-1).

7.7.2 Exigences

7.7.2.1 La validation de la sécurité des systèmes E/E/PE doit être effectuée conformément à un plan préétabli (voir également 7.7 de la CEI 61508-3).

NOTE 1 Sur le cycle de vie de sécurité des systèmes E/E/PE, la validation de sécurité de ces systèmes est illustrée avant l'installation; cependant, dans certains cas, cette validation ne peut être effectuée qu'après installation (par exemple, lorsque le développement du logiciel applicatif n'est finalisé qu'après installation).

NOTE 2 La validation d'un système électronique programmable relatif à la sécurité comprend la validation du matériel et du logiciel. Les exigences de validation du logiciel sont contenues dans la CEI 61508-3.

7.7.2.2 Tous les équipements de mesure pour les essais utilisés pour la validation doivent être étalonnés par rapport à un étalon lié à un étalon national, si ce dernier existe, ou selon une procédure reconnue. Le fonctionnement correct de tous les équipements d'essai doit être vérifié.

7.7.2.3 La mise en œuvre appropriée de chaque fonction de sécurité spécifiée dans les exigences de sécurité des systèmes E/E/PE (voir 7.10 de la CEI 61508-1), les exigences de conception de ces systèmes (voir 7.2) et toutes les procédures d'exploitation et de maintenance de ces mêmes systèmes doivent être validées par un essai et/ou une analyse. Si l'indépendance ou le découplage approprié(e) entre des éléments ou des sous-systèmes individuels ne peut être démontré(e) par une analyse, les combinaisons associées du comportement fonctionnel doivent être soumises à l'essai.

NOTE Le nombre de combinaisons d'essais nécessaires pouvant devenir très important, une restructuration du système peut alors être requise.

7.7.2.4 La documentation appropriée relative aux essais de validation de sécurité des systèmes E/E/PE doit être élaborée et doit indiquer pour chaque fonction de sécurité:

a) la version du plan de validation de sécurité des systèmes E/E/PE utilisée;

b) la fonction de sécurité soumise à essai (ou à analyse), ainsi que la référence spécifique à l'exigence spécifiée lors de la planification de la validation de sécurité des systèmes E/E/PE;

c) les outils et les équipements utilisés, ainsi que les données d'étalonnage;

d) les résultats de chaque essai;

e) les divergences entre les résultats prévus et les résultats réels.

NOTE Il n'est pas nécessaire de fournir une documentation séparée pour chaque fonction de sécurité; cependant, les informations requises au titre des alinéas a) à e) doivent s'appliquer à chaque fonction de sécurité et lorsque pour une fonction de sécurité donnée, ces informations sont différentes, la relation doit être indiquée.

7.7.2.5 Lorsque des divergences apparaissent (c'est-à-dire lorsque les résultats réels s'écartent des résultats prévus au-delà des tolérances indiquées), les résultats des essais de validation de sécurité des systèmes E/E/PE doivent être consignés par écrit, y compris:

a) l'analyse effectuée; et

b) la décision prise quant à la poursuite de l'essai ou l'émission d'une demande de modification et retour à une étape antérieure de l'essai de validation.

7.7.2.6 Le fournisseur ou le développeur doit mettre les résultats des essais de validation de sécurité des systèmes E/E/PE à disposition du développeur de l'EUC et du système de commande de ce dernier, de manière à leur permettre de satisfaire aux exigences pour la validation de sécurité globale définie dans la CEI 61508-1.

7.7.2.7 Pour éviter les anomalies au cours de la validation de sécurité des systèmes E/E/PE, un ensemble approprié de techniques et de mesures, conforme au Tableau B.5, doit être utilisé.

7.8 Modification des systèmes E/E/PE

7.8.1 Objectif

L'objectif des exigences du présent paragraphe est d'effectuer des corrections, améliorations ou adaptations apportées au système E/E/PE relatif à la sécurité, afin d'assurer que l'intégrité de sécurité requise est obtenue et maintenue.

7.8.2 Exigences

7.8.2.1 Une documentation appropriée doit être établie et maintenue pour chaque activité de modification des systèmes E/E/PE. La documentation doit comprendre:

a) la spécification détaillée de la modification ou du changement;

b) une analyse de l'impact de l'activité de modification sur le système dans son ensemble, y compris le matériel, le logiciel (voir la CEI 61508-3), l'interaction humaine, l'environnement, ainsi que les interactions potentielles;

c) toutes les approbations relatives aux modifications;

d) l'avancement des modifications;

e) les cas d'essais pour les sous-systèmes et les éléments, y compris les données de revalidation;

f) l'historique de la gestion de configuration des systèmes E/E/PE;

g) les écarts par rapport à l'exploitation et aux conditions normales;

h) les modifications qu'il est nécessaire d'apporter aux procédures du système;

i) les modifications qu'il est nécessaire d'apporter à la documentation.

7.8.2.2 Les fabricants ou les fournisseurs de système qui déclarent une conformité avec tout ou partie de la présente norme doivent maintenir un système permettant de lancer des modifications à la suite d'une détection d'anomalies dans le matériel ou le logiciel, et d'informer les utilisateurs du besoin de modification dans le cas d'une anomalie affectant la sécurité.

7.8.2.3 Les modifications doivent être effectuées en utilisant au moins le même niveau d'expertise, d'outils automatisés (voir 7.4.4.2 de la CEI 61508-3), de planification et de gestion que le développement initial des systèmes E/E/PE relatifs à la sécurité.

7.8.2.4 Après modification, les systèmes E/E/PE relatifs à la sécurité doivent être revérifiés et revalidés.

NOTE Voir également 7.16.2.6 de la CEI 61508-1.

7.9 Vérification des systèmes E/E/PE

7.9.1 Objectif

L'objectif des exigences du présent paragraphe est de soumettre à l'essai et d'évaluer les résultats d'une phase donnée pour assurer le caractère correct et la cohérence des systèmes par rapport aux produits et normes fournis en données pour cette phase.

NOTE Pour des raisons pratiques, toutes les activités de vérification ont été regroupées en 7.9, mais sont en fait entreprises pour chaque phase correspondante.

7.9.2 Exigences

7.9.2.1 La vérification des systèmes E/E/PE relatifs à la sécurité doit être planifiée en même temps que le développement (voir 7.4), pour chaque phase du cycle de vie de sécurité de ces systèmes et doit être documentée.

7.9.2.2 La planification de la vérification des systèmes E/E/PE doit faire référence à tous les critères, techniques et outils à utiliser au cours de la vérification pour cette phase.

7.9.2.3 La planification de la vérification des systèmes E/E/PE doit spécifier les activités à entreprendre pour assurer le caractère correct et la cohérence des systèmes par rapport aux produits et normes fournis en données pour cette phase.

7.9.2.4 La planification de la vérification des systèmes E/E/PE doit tenir compte des éléments suivants:

a) le choix des stratégies et techniques de vérification;

b) le choix et l'utilisation des équipements d'essai;

c) le choix et la documentation des activités de vérification;

d) l'évaluation des résultats de vérification obtenus directement à partir des équipements de vérification et à partir des essais.

7.9.2.5 Au cours de chaque phase de conception et de développement, il doit être démontré que les exigences fonctionnelles et les exigences d'intégrité de sécurité sont satisfaites.

7.9.2.6 Le résultat de chaque activité de vérification doit être consigné par écrit et indiquer que les systèmes E/E/PE relatifs à la sécurité ont passé avec succès la vérification, ou les raisons de l'échec constaté. Les éléments suivants doivent être pris en compte:

a) les articles qui ne sont pas conformes à une ou plusieurs exigences pertinentes du cycle de vie de sécurité des systèmes E/E/PE (voir 7.2);

b) les articles qui ne sont pas conformes à une ou plusieurs normes de conception applicables (voir 7.4);

c) les articles qui ne sont pas conformes à une ou plusieurs exigences de gestion de sécurité applicables (voir Article 6).

7.9.2.7 Pour la vérification des exigences de conception des systèmes E/E/PE, une fois ces dernières établies (voir 7.2) et avant d'entamer la phase suivante (conception et développement), la vérification doit:

a) déterminer si les exigences de conception des systèmes E/E/PE permettent de satisfaire à la spécification des exigences de sécurité de ces systèmes (voir 7.10 de la CEI 61508-1) pour la sécurité, la fonctionnalité, et aux autres exigences spécifiées au cours de la planification de la sécurité; et

b) vérifier les incompatibilités entre:

   – les exigences de sécurité relatives aux systèmes E/E/PE (voir 7.10 de la CEI 61508-1);

   – les exigences de conception relatives aux systèmes E/E/PE (voir 7.2);

   – les essais effectués sur les systèmes E/E/PE (voir 7.4); et

   – la documentation de l'utilisateur et toute autre documentation relative aux systèmes.

7.9.2.8 Pour la vérification de la conception et du développement des systèmes E/E/PE, après achèvement de la conception et du développement de ces systèmes (voir 7.4) et avant d'entamer la phase suivante (intégration), la vérification doit:

a) déterminer si les essais effectués sur les systèmes E/E/PE conviennent à la conception et au développement de ces systèmes;

b) déterminer la cohérence et l'exhaustivité (jusqu'au niveau du module inclus) de la conception et du développement des systèmes E/E/PE par rapport aux exigences de sécurité de ces systèmes (voir 7.10 de la CEI 61508-1); et

c) vérifier les incompatibilités entre:

   – les exigences de sécurité relatives aux systèmes E/E/PE (voir 7.10 de la CEI 61508-1);

   – les exigences de conception relatives aux systèmes E/E/PE (voir 7.2);

   – la conception et le développement des systèmes E/E/PE (voir 7.4); et

   – les essais effectués sur les systèmes E/E/PE (voir 7.4).

NOTE 1 Le Tableau B.5 recommande des techniques de validation de la sécurité, d'analyse des défaillances et d'essai qui sont également applicables à la vérification.

NOTE 2 La vérification de la réalisation de la couverture de diagnostic tient compte du Tableau A.1, qui donne les anomalies et défaillances qui doivent être détectées.

7.9.2.9 Pour la vérification de l'intégration des systèmes E/E/PE, l'intégration des systèmes E/E/PE relatifs à la sécurité doit être vérifiée pour assurer que les exigences de 7.5 ont été satisfaites.

7.9.2.10 Les cas d'essai ainsi que leurs résultats doivent être consignés par écrit.

8 Evaluation de la sécurité fonctionnelle

Les exigences relatives à l'évaluation de la sécurité fonctionnelle sont telles que détaillées à l'Article 8 de la CEI 61508-1.

Annexe A
(normative)

Techniques et mesures applicables aux systèmes E/E/PE relatifs à la sécurité – maîtrise des défaillances en exploitation

A.1 Généralités

La présente annexe doit être utilisée conjointement à 7.4. Elle limite la couverture de diagnostic maximale qu'il est admis de déclarer pour les techniques et les mesures pertinentes. Pour chaque niveau d'intégrité de sécurité, l'annexe recommande des techniques et des mesures pour maîtriser les défaillances aléatoires, systématiques, environnementales et opérationnelles du matériel. L'Annexe B de la CEI 61508-6 et l'Annexe A de la CEI 61508-7 fournissent plus d'informations concernant les architectures et les mesures correspondantes.

Il n'est pas possible d'énumérer chaque cause physique particulière de défaillance dans un matériel complexe et ce, pour deux raisons principales:

– le rapport cause/effet entre les anomalies et les défaillances est souvent difficile à déterminer;

– le caractère des défaillances devient plus systématique et moins aléatoire lorsque des matériels et des logiciels complexes sont utilisés.

En fonction du moment de leur apparition, les défaillances des systèmes E/E/PE relatifs à la sécurité peuvent être classées en différentes catégories:

– des défaillances dues à des anomalies apparaissant **avant ou pendant l'installation du système** (par exemple, les anomalies logicielles comprennent des anomalies de spécification et de programme, les anomalies matérielles comprennent des anomalies de fabrication et une sélection d'éléments incorrecte); et

– des défaillances dues à des anomalies ou à des erreurs humaines apparaissant **après installation du système** (par exemple, des défaillances aléatoires du matériel ou des défaillances dues à une utilisation incorrecte).

Pour éviter ou maîtriser ces défaillances, lorsqu'elles apparaissent, un grand nombre de mesures est en général nécessaire. La structure des exigences spécifiées dans les Annexes A et B résulte de la division des mesures en mesures d'**évitement de défaillances** pendant les différentes phases du cycle de vie de sécurité des systèmes E/E/PE (Annexe B) et en mesures **de maîtrise des défaillances** au cours de l'exploitation (la présente Annexe). Les mesures permettant de maîtriser les défaillances sont des caractéristiques intégrées des systèmes E/E/PE relatifs à la sécurité.

La couverture de diagnostic et la proportion de défaillances en sécurité sont déterminées sur la base du Tableau A.1 et conformément aux procédures détaillées à l'Annexe C. Les Tableaux A.2 à A.14 appuient les exigences du Tableau A.1 en recommandant des techniques et des mesures d'essais de diagnostic ainsi que des niveaux maximum de couverture de diagnostic qui peuvent être obtenus en appliquant ces techniques et mesures. Ces tableaux ne se substituent pas aux exigences de l'Annexe C. Les Tableaux A.2 à A.14 ne sont pas exhaustifs. D'autres mesures et techniques peuvent être utilisées, à condition de produire la preuve permettant d'appuyer la couverture de diagnostic déclarée. Si une couverture de diagnostic élevée est déclarée, il convient alors, au minimum, qu'au moins une technique permettant une couverture de diagnostic élevée soit appliquée, à partir de chacun de ces tableaux.

De la même manière, les Tableaux A.15 à A.17 recommandent des techniques et des mesures pour chaque niveau d'intégrité de sécurité pour maîtriser des défaillances systématiques. Le Tableau A.15 recommande des mesures globales pour maîtriser des

défaillances systématiques (voir également la CEI 61508-3), le Tableau A.16 recommande des mesures pour maîtriser des défaillances environnementales et le Tableau A.17 recommande pour sa part des mesures pour maîtriser des défaillances opérationnelles. La plupart de ces mesures de maîtrise peuvent être classées en fonction du Tableau A.18.

Toutes les techniques et mesures définies dans ces tableaux sont décrites en Annexe A de la CEI 61508-7. Les techniques et mesures logicielles requises pour chaque niveau d'intégrité de sécurité sont fournies dans la CEI 61508-3. Les recommandations permettant de déterminer l'architecture d'un système E/E/PE relatif à la sécurité sont fournies en Annexe B de la CEI 61508-6.

Le fait de se conformer aux recommandations de la présente annexe ne garantit pas en soi l'intégrité de sécurité requise. Il est important de tenir compte des éléments suivants:

– la cohérence des techniques et mesures choisies ainsi que leur degré de complémentarité; et
– les techniques et les mesures qui sont les mieux adaptées aux problèmes spécifiques rencontrés au cours du développement de chaque système E/E/PE relatif à la sécurité particulier.

A.2 Intégrité de sécurité du matériel

Le Tableau A.1 fournit des exigences relatives aux anomalies ou aux défaillances qui doivent être détectées par les techniques et mesures de maîtrise des défaillances du matériel afin d'obtenir la couverture de diagnostic pertinente (voir également l'Annexe C). Les Tableaux A.2 à A.14 appuient les exigences du Tableau A.1 en recommandant des techniques et des mesures d'essais de diagnostic ainsi que des niveaux maximum de couverture de diagnostic qui peuvent être obtenus en appliquant ces techniques et mesures. Il est admis que ces essais soient appliqués de manière permanente ou périodique. Les tableaux ne se substituent à aucune des exigences de 7.4. Les Tableaux A.2 à A.14 ne sont pas exhaustifs. D'autres mesures et techniques peuvent être utilisées, à condition de produire la preuve permettant d'appuyer la couverture de diagnostic déclarée.

NOTE 1 La présentation générale des techniques et mesures associées à ces tableaux est fournie à l'Annexe A de la CEI 61508-7. Le paragraphe applicable est référencé dans la deuxième colonne des Tableaux A.2 à A.14.

NOTE 2 Les qualificatifs « faible », « moyen » et « élevé » de la couverture de diagnostic sont quantifiés à 60 %, 90 % et 99 % respectivement.

Tableau A.1 – Anomalies ou défaillances à supposer lors de la quantification de l'effet des défaillances aléatoires du matériel ou à prendre en compte pour déduire la proportion de défaillances en sécurité

Composant	Voir tableau (x)	Exigences relatives à la couverture de diagnostic déclarée		
		Faible (60 %)	**Moyenne (90 %)**	**Elevée (99 %)**
Dispositifs électromécaniques	A.2	Défauts d'excitation ou de désexcitation	Défauts d'excitation ou de désexcitation	Défauts d'excitation ou de désexcitation
		Contacts soudés	Contacts soudés identifiés	Contacts soudés identifiés. Pas de guidage positif des contacts (cette défaillance n'est pas prise en compte pour les relais construits et soumis à l'essai conformément à l'EN 50205, ou équivalent)
				Pas d'ouverture positive (cette défaillance n'est pas prise en compte pour les interrupteurs de position construits et soumis à l'essai conformément à la CEI 60947-5-1, ou équivalent)
Matériel discret	A.3, A.7, A.9			
E/S numérique		Blocage (voir Note 1)	Modèle DC (voir Note 2)	Modèle DC dérive et oscillation
E/S analogique		Blocage	Modèle DC dérive et oscillation	Modèle DC dérive et oscillation
Alimentation		Blocage	Modèle DC dérive et oscillation	Modèle DC dérive et oscillation
Bus	A.3			
Généralités	A.7	Blocage des adresses	Hors délai	Hors délai
Unité de gestion mémoire (MMU)	A.8	Blocage des données ou des adresses	Décodage d'adresse erroné	Décodage d'adresse erroné
			Changement d'adresses dû à des erreurs intermittentes dans les registres MMU (voir Notes 3 et 4)	Changement d'adresses dû à des erreurs intermittentes dans les registres MMU
Accès direct en mémoire (DMA)		Pas d'accès ou accès en continu	Modèle DC pour les données et les adresses	Toutes anomalies affectant les données en mémoire
			Modification d'information due à des erreurs intermittentes dans les registres DMA	Temps d'accès erroné
			Temps d'accès erroné	
Arbitrage bus (voir Note 5)		Blocage des signaux d'arbitrage	Pas d'arbitrage ou arbitrage en continu	Pas d'arbitrage, arbitrage en continu ou arbitrage erroné
Unité de traitement centrale (CPU)	A.4A.10			
Registre, RAM interne		Blocage des données et adresses	Modèle DC pour les données et les adresses	Modèle DC pour les données et les adresses
			Modification d'information due à des erreurs intermittentes	Chevauchement dynamique pour les cellules mémoire
				Modification d'information due à des erreurs intermittentes
				Pas d'adressage, adressage erroné ou multiple
Codage et exécution y compris le registre de pointeur		Codage erroné ou pas d'exécution	Codage erroné ou pas d'exécution	Aucune hypothèse de défaillance définie
Calcul d'adresse		Blocage	Modèle DC	Aucune hypothèse de défaillance définie
			Changement d'adresses dû à des erreurs intermittentes	
Compteur programme, pointeur de pile		Blocage	Modèle DC	Modèle DC
			Changement d'adresses dû à des erreurs intermittentes	Changement d'adresses dû à des erreurs intermittentes

Tableau A.1 *(suite)*

Composant	Voir tableau (x)	Exigences relatives à la couverture de diagnostic déclarée		
		Faible (60 %)	**Moyenne (90 %)**	**Elevée (99 %)**
Gestion des interruptions	A.4			
Interruption		Pas d'interruption ou interruption en continu (voir Note 6)	Pas d'interruption ou interruption en continu Chevauchement des interruptions	Pas d'interruption ou interruption en continu Chevauchement des interruptions
Ré-initialisation des circuits		Blocage Pas d'initialisation des composants individuels pour la réinitialisation de l'état	Modèle DC Dérive et oscillation Pas d'initialisation des composants individuels pour la réinitialisation de l'état	Modèle DC Dérive et oscillation Pas d'initialisation des composants individuels pour la réinitialisation de l'état
Mémoire invariable	A.5	Blocage des données et adresses	Modèle DC pour les données et les adresses	Toutes anomalies affectant les données en mémoire
Mémoire variable	A.6	Blocage des données et adresses	Modèle DC pour les données et les adresses Modification d'information due à des erreurs intermittentes	Modèle DC pour les données et les adresses Chevauchement dynamique pour les cellules mémoire Modification d'information due à des erreurs intermittentes Pas d'adressage, adressage erroné ou multiple
Horloge (quartz, oscillateur, PLL)	A.11	Sous- ou sur-harmonique Gigue périodique	Fréquence incorrecte Gigue périodique	Fréquence incorrecte Gigue périodique
Communication et mémoire de masse	A.12	Données ou adresses erronées Pas de transmission	Toutes anomalies affectant les données en mémoire Données ou adresses erronées Temps de transmission erroné Séquence de transmission erronée	Toutes anomalies affectant les données en mémoire Données ou adresses erronées Temps de transmission erroné Séquence de transmission erronée
Capteurs	A.13	Blocage	Modèle DC Dérive et oscillation	Modèle DC Dérive et oscillation
Eléments finaux	A.14	Blocage	Modèle DC Dérive et oscillation	Modèle DC Dérive et oscillation

NOTE 1 «Blocage» est une catégorie d'anomalie qui peut être décrite avec «0» ou «1» continu ou «actif» aux broches d'un élément.

NOTE 2 «Modèle DC» inclut les modes de défaillance suivants: blocage, blocage ouvert, sorties ouvertes ou haute impédance ainsi que les courts-circuits entre les lignes de signaux. Pour les circuits intégrés, le court-circuit qui se produit entre deux connecteurs (broches) est pris en compte.

NOTE 3 Le taux d'erreurs intermittentes (SER) pour les semi-conducteurs à faible énergie correspond à plus d'un ordre de grandeur supérieur (50x.500x) au taux d'erreurs récurrentes (dommage permanent au dispositif).

NOTE 4 Les sources d'erreurs intermittentes sont les suivantes: particules alpha d'une désintégration de paquets, neutrons, bruit EMI externe et diaphonie interne. Seules des mesures d'intégrité de sécurité appliquées pendant le temps d'exécution peuvent maîtriser l'effet des erreurs intermittentes. Les mesures d'intégrité de sécurité efficaces pour les défaillances aléatoires du matériel peuvent ne pas se révéler efficaces pour les erreurs intermittentes.

EXEMPLE: Les essais RAM, tels que « walk-path », « galpat », etc. ne sont pas efficaces, tandis que les techniques de surveillance utilisant la parité et le code CCE avec lecture récurrente des cellules de mémoire ou les techniques utilisant la redondance (et la comparaison ou le vote) peuvent l'être.

NOTE 5 L'arbitrage bus est le mécanisme qui permet de décider du dispositif qui maîtrise le bus.

NOTE 6 Pas d'interruption signifie qu'aucune interruption n'a lieu lorsqu'il convient qu'il y en ait une ou plusieurs. Des interruptions en continu signifient que des interruptions continues ont lieu lorsqu'il convient qu'il n'y en ait pas.

NOTE 7 Pour les ASIC, ce tableau et les Tableaux A.2 à A.18 s'appliquent le cas échéant.

Tableau A.2 – Composants électriques

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Détection des défaillances par surveillance en ligne	A.1.1	Faible (mode faible sollicitation) Moyen (mode sollicitation élevée ou mode continu)	Dépend de la couverture de diagnostic de la détection de défaillance
Surveillance des contacts de relais	A.1.2	Elevée	Il convient de tenir compte du taux de commutation relais pour la quantification de l'effet des défaillances aléatoires
Comparateur	A.1.3	Elevée	Elevé si les modes de défaillance ont une orientation de sécurité prédominante
Vote majoritaire	A.1.4	Elevée	Dépend de la qualité du vote
NOTE 1 Ce tableaux ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.3 – Composants électroniques

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Détection des défaillances par surveillance en ligne	A.1.1	Faible (mode faible sollicitation) Moyen (mode sollicitation élevée ou mode continu)	Dépend de la couverture de diagnostic de la détection de défaillance
Comparateur	A.1.3	Elevée	Elevé si les modes de défaillance ont une orientation de sécurité prédominante
Vote majoritaire	A.1.4	Elevée	Dépend de la qualité du vote
Essais par un matériel redondant	A.2.1	Moyenne	Dépend de la couverture de diagnostic de la détection de défaillance
Principes dynamiques	A.2.2	Moyenne	Dépend de la couverture de diagnostic de la détection de défaillance
Port d'accès d'essai normalisé et architecture d'essai du type «registre à décalage périphérique	A.2.3	Elevée	Dépend de la couverture de diagnostic de la détection de défaillance
Redondance surveillée	A.2.5	Elevée	Dépend du degré de redondance et de la surveillance
Matériel avec contrôle automatique	A.2.6	Elevée	Dépend de la couverture de diagnostic des essais
Surveillance du signal analogique	A.2.7	Faible	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.4 – Unités de traitement

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Comparateur	A.1.3	Elevée	Dépend de la qualité de la comparaison
Vote majoritaire	A.1.4	Elevée	Dépend de la qualité du vote
Autotest logiciel: nombre limité de patterns (un canal)	A.3.1	Faible	
Autotest logiciel: walking bit (un canal)	A.3.2	Moyenne	
Autotest pris en charge par le matériel (un canal)	A.3.3	Moyenne	
Traitement codé (un canal)	A.3.4	Elevée	
Comparaison réciproque par logiciel	A.3.5	Elevée	Dépend de la qualité de la comparaison
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C.			
NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic.			
NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			
NOTE 4 Dans la mesure où un grand nombre d'anomalies d'unités de traitement entraînent une modification du contrôle de flux, les mesures et techniques de diagnostic énumérées dans le Tableau A.10 peuvent également être prises en compte pour les anomalies des unités de traitement. Ces mesures et techniques de diagnostic couvrent uniquement le flux de contrôle et non le flux des données.			

Tableau A.5 – Plages de mémoire invariable

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Redondance multi-bits à sauvegarde de mot	A.4.1	Moyenne	L'efficacité de la redondance multi-bits à sauvegarde de mot dépend de l'inclusion de l'adresse dans la redondance à bits multiples, et repose sur la mesure respective de détection des anomalies de cause commune multi-bits, par exemple adressage multiple (choix de rangs multiples, activation des commutateurs de lignes à bits locaux à globaux), problèmes d'alimentation (par exemple, défauts de pompe de chargement), remplacement des rangées et colonnes de production, mesure du rendement de production pour masquer les anomalies de production), etc.
Somme de contrôle modifiée	A.4.2	Faible	
Signature d'un seul mot (8 bits)	A.4.3	Moyenne	L'efficacité de la signature dépend de sa largeur, comparativement à la longueur du bloc d'informations à protéger
Signature d'un mot double (16 bits)	A.4.4	Elevée	L'efficacité de la signature dépend de sa largeur, comparativement à la longueur du bloc d'informations à protéger
Réplication de bloc	A.4.5	Elevée	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.6 – Plages de mémoire variable

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Essai RAM «échiquier» ou «défilement	A.5.1	Faible	
Essai RAM «walk-path»	A.5.2	Moyenne	
Essai RAM «Galpat» ou «Galpat» transparent	A.5.3	Elevée	
Essai RAM «Abraham»	A.5.4	Elevée	
Bit de parité de la RAM	A.5.5	Faible	
Surveillance de la RAM avec un code de Hamming modifié ou détection de la défaillance des données par des codes de détection d'erreur (EDC)	A.5.6	Moyenne	L'efficacité de la surveillance de la RAM avec un code de Hamming modifié ou une détection de la défaillance des données par des codes de détection d'erreur (EDC) dépend de l'inclusion de l'adresse dans le code de Hamming et repose sur la mesure respective de détection des anomalies de cause commune multi-bits, par exemple adressage multiple (choix de rangs multiples, activation des commutateurs de lignes à bits locaux à globaux), remplacement des rangées et colonnes de production (mesure du rendement de production pour masquer les anomalies de production), etc.
Double RAM avec comparaison matérielle ou logicielle et essai de lecture/écriture	A.5.7	Elevée	

NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C.

NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic.

NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.

NOTE 4 Pour une RAM qui est écrite/lue seulement à fréquence faible (par exemple, lors de la configuration), les mesures A.4.1 à A.4.4 de la CEI 61508-7 sont efficaces si elles sont effectuées après chaque accès de lecture/écriture.

Tableau A.7 – Unités E/S et interface (communication externe)

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Détection des défaillances par surveillance en ligne	A.1.1	Faible (mode faible sollicitation) Moyenne (mode sollicitation élevée ou mode continu)	Dépend de la couverture de diagnostic de la détection de défaillance
Trame d'essai	A.6.1	Elevée	
Protection par code	A.6.2	Elevée	
Sortie parallèle multicanal	A.6.3	Elevée	Uniquement si le flux de données change pendant l'intervalle d'essai de diagnostic
Sorties surveillées	A.6.4	Elevée	Uniquement si le flux de données change pendant l'intervalle d'essai de diagnostic
Comparaison/vote sur les entrées (1oo2, 2oo3 ou redondance meilleure)	A.6.5	Elevée	Uniquement si le flux de données change pendant l'intervalle d'essai de diagnostic
Transmission de signaux complémentaires	A.11.4	Elevée	Par exemple transmission de signaux inversés
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.8 – Chemins de données (communication interne)

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Redondance matérielle sur un bit	A.7.1	Faible	Dans le cas d'un chemin de données de type commutateur crossbar à plans multiples, l'efficacité donnée peut être supposée uniquement si les lignes d'adresse et de contrôle sont couvertes par les mesures de sécurité.
Redondance matérielle sur plusieurs bits	A.7.2	Moyenne	Dans le cas d'un chemin de données de type commutateur crossbar à plans multiples, l'efficacité donnée peut être supposée uniquement si les lignes d'adresse et de contrôle sont couvertes par les mesures de sécurité.
Redondance matérielle complète	A.7.3	Elevée	
Inspection utilisant des trames d'essai	A.7.4	Elevée	
Redondance de transmission	A.7.5	Elevée	Efficace contre les anomalies transitoires uniquement
Redondance d'informations	A.7.6	Elevée	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.9 – Alimentation

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Protection contre les surtensions avec arrêt de sécurité ou commutation sur la seconde unité d'alimentation	A.8.1	Faible	
Surveillance de la tension (secondaire) avec arrêt de sécurité ou commutation sur la seconde unité d'alimentation	A.8.2	Elevée	
Mise hors tension avec arrêt de sécurité ou commutation sur la seconde unité d'alimentation	A.8.3	Elevée	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.10 – Séquence du programme (chien de garde)

Technique/Mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
«Chien de garde» avec base de temps séparée sans fenêtre temporelle	A.9.1	Faible	
«Chien de garde» avec base de temps séparée et fenêtre temporelle	A.9.2	Moyenne	
Surveillance logique de la séquence du programme	A.9.3	Moyenne	Dépend de la qualité de la surveillance
Combinaison de surveillance temporelle et logique des séquences du programme	A.9.4	Elevée	
Surveillance temporelle avec contrôle en ligne	A.9.5	Moyenne	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.11 – Horloge

Technique/mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
«Chien de garde» avec base de temps séparée sans fenêtre temporelle	A.9.1	Faible	
«Chien de garde» avec base de temps séparée et fenêtre temporelle	A.9.2	Elevée	Dépend de la restriction de temps pour la fenêtre temporelle
Surveillance logique de la séquence du programme	A.9.3	Moyenne	Efficace uniquement contre les défaillances de l'horloge si des événements temporels externes influencent le flux de programme logique
Surveillance temporelle et logique	A.9.4	Elevée	
Surveillance temporelle avec contrôle en ligne	A.9.5	Moyenne	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.12 – Communication et mémoire de masse

Technique/mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Echange d'informations entre le système E/E/PE relatif à la sécurité et le procédé	A.6	Voir Tableau A.7	Voir unités E/S et interface
Echange d'informations entre systèmes E/E/PE relatifs à la sécurité	A.7	Voir Tableau A.8	Voir chemins de données/bus
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.13 – Capteurs

Technique/mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Détection des défaillances par surveillance en ligne	A.1.1	Faible (mode de faible sollicitation) Moyenne (mode de sollicitation élevée ou mode continu)	Dépend de la couverture de diagnostic de la détection de défaillance
Surveillance du signal analogique	A.2.7	Faible	
Trame d'essai	A.6.1	Elevée	
Comparaison/vote majoritaire sur les entrées (1oo2, 2oo3 ou redondance meilleure)	A.6.5	Elevée	Uniquement si le flux de données change pendant l'intervalle d'essai de diagnostic
Capteur de référence	A.12.1	Elevée	Dépend de la couverture de diagnostic de la détection de défaillance
Commutateur à action directe	A.12.2	Elevée	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

Tableau A.14 – Eléments finaux (actionneurs)

Technique/mesure de diagnostic	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Détection des défaillances par surveillance en ligne	A.1.1	Faible (mode faible sollicitation) Moyenne (mode sollicitation élevée ou mode continu)	Dépend de la couverture de diagnostic de la détection de défaillance
Surveillance des contacts de relais	A.1.2	Elevée	Il convient de tenir compte du taux de commutation relais pour la quantification de l'effet des défaillances aléatoires
Trame d'essai	A.6.1	Elevée	
Surveillance	A.13.1	Elevée	Dépend de la couverture de diagnostic de la détection de défaillance
Surveillance croisée de plusieurs actionneurs	A.13.2	Elevée	
NOTE 1 Ce tableau ne remplace aucune des exigences de l'Annexe C. NOTE 2 Les exigences de l'Annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le Tableau A.1.			

A.3 Intégrité de sécurité systématique

Les tableaux ci-dessous donnent des recommandations relatives aux techniques et mesures destinées à:

– maîtriser les défaillances dues à la conception du matériel (Tableau A.15);

– maîtriser les défaillances dues aux contraintes ou influences environnementales (voir Tableau A.16); et

– maîtriser les défaillances observées en cours d'exploitation (Tableau A.17).

Les Tableaux A.15 à A.17 donnent des recommandations et spécifient des exigences par niveau d'intégrité de sécurité en indiquant, en premier lieu, l'importance de la technique ou de la mesure et, en second lieu, l'efficacité requise si cette technique ou mesure est utilisée. L'importance est décrite de la manière suivante:

– M: la technique ou mesure est requise (obligatoire) pour ce niveau d'intégrité de sécurité;
– HR: la technique ou mesure est vivement recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure n'est pas utilisée, les motifs sous-jacents doivent alors être décrits de manière détaillée;
– R: la technique ou mesure est recommandée pour ce niveau d'intégrité de sécurité;
– -: la technique ou mesure ne porte aucune recommandation pour ou contre son utilisation;
– NR: la technique ou mesure n'est absolument pas recommandée pour ce niveau d'intégrité de sécurité; si cette technique ou mesure est utilisée, les motifs sous-jacents doivent alors être décrits de manière détaillée.

L'efficacité requise est décrite de la manière suivante:

– Faible: si elle est utilisée, la technique ou mesure doit être appliquée dans la mesure nécessaire pour garantir au moins une faible efficacité contre les défaillances systématiques;
– Moyenne: si elle est utilisée, la technique ou mesure doit être appliquée dans la mesure nécessaire pour garantir au moins une efficacité moyenne contre les défaillances systématiques;
– Elevée: si elle est utilisée, la technique ou mesure doit être appliquée dans la mesure nécessaire pour garantir une efficacité élevée contre les défaillances systématiques.

Le Tableau A.18 donne des instructions relatives aux niveaux d'efficacité pour la plupart des techniques et mesures.

Si une mesure n'est pas obligatoire, elle peut, en principe, être remplacée par d'autres mesures (soit prises séparément, soit en combinaison); ceci est régi par l'ombrage (de la zone correspondante) comme expliqué dans le tableau.

Toutes les techniques et mesures fournies ici sont des caractéristiques intégrées des systèmes E/E/PE relatifs à la sécurité qui peuvent aider à la maîtrise des défaillances en ligne. Des procédures ainsi que des techniques et des mesures organisationnelles sont nécessaires pendant le cycle de vie de sécurité des systèmes E/E/PE pour éviter l'introduction d'anomalies, et des techniques de validation sont nécessaires pour vérifier, au moyen d'essais, le comportement des systèmes E/E/PE relatifs à la sécurité contre des influences externes attendues et démontrer que les caractéristiques intégrées conviennent à l'application spécifique (voir Annexe B).

L'Annexe D de la CEI 61508-6 fournit des informations sur les défaillances de cause commune.

NOTE La plupart des mesures décrites dans les Tableaux A.15 à A.17 peuvent être utilisées avec une efficacité variable comme l'indique le Tableau A.18 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

Tableau A.15 – Techniques et mesures pour maîtriser les défaillances systématiques dues à la conception du matériel

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Surveillance de la séquence du programme	A.9	HR faible	HR faible	HR moyenne	HR élevée
	Détection des défaillances par surveillance en ligne (voir Note 4)	A.1.1	R faible	R faible	R moyenne	R élevée
	Essai par un matériel redondant	A.2.1	R faible	R faible	R moyenne	R élevée
	Port d'accès d'essai normalisé et architecture d'essai du type «registre à décalage périphérique (Scan Path) »	A.2.3	R faible	R faible	R moyenne	R élevée
	Protection par code	A.6.2	R faible	R faible	R moyenne	R élevée
	Diversité du matériel	B.1.4	- faible	– faible	R moyenne	R élevée

Au moins une des techniques du groupe ombré, ou une des techniques spécifiées dans le Tableau A.3 de la CEI 61508-3, est requise.

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède immédiatement ce tableau.

NOTE 2 Les mesures peuvent être utilisées pour faire varier l'efficacité conformément au Tableau A.18 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans les Annexes A, B et C de la CEI 61508-7. Le paragraphe applicable est référencé dans la deuxième colonne.

NOTE 4 Pour les systèmes E/E/PE relatifs à la sécurité utilisés dans un mode de fonctionnement à faible sollicitation (par exemple, systèmes d'arrêt d'urgence), la couverture de diagnostic obtenue à partir de la détection de défaillance par surveillance en ligne est généralement faible ou inexistante.

Tableau A.16 – Techniques et mesures pour maîtriser les défaillances systématiques dues aux contraintes ou influences environnementales

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Mesures contre les chutes de tension, les variations de tension, les surtensions, les sous-tensions et autres phénomènes tels que la variation de la fréquence d'alimentation courant alternatif pouvant générer une défaillance dangereuse	A.8	M faible	M moyenne	M moyenne	M élevée
	Séparation entre les lignes d'alimentation électriques et les lignes de données (voir la Note 4)	A.11.1	M	M	M	M
	Augmentation de l'immunité aux interférences	A.11.3	M faible	M faible	M moyenne	M élevée
	Mesures contre l'environnement physique (par exemple température, humidité, eau, vibrations, poussière, substances corrosives)	A.14	M faible	M élevée	M élevée	M élevée
	Surveillance de la séquence du programme	A.9	HR faible	HR faible	HR moyenne	HR élevée
	Mesures contre les surchauffes	A.10	HR faible	HR faible	HR moyenne	HR élevée
	Séparation spatiale des lignes multiples	A.11.2	HR faible	HR faible	HR moyenne	HR élevée
	Principe du courant de repos (lorsqu'une maîtrise continue n'est pas nécessaire pour obtenir ou maintenir un état de sécurité de l'EUC)	A.1.5	R	R	R	R
	Mesures de détection des interruptions de courant et des courts-circuits dans les lignes de signaux		R	R	R	R
	Détection des défaillances par surveillance en ligne (voir Note 5)	A.1.1	R faible	R faible	R moyenne	R élevée
	Essai par un matériel redondant	A.2.1	R faible	R faible	R moyenne	R élevée
	Protection par code	A.6.2	R faible	R faible	R moyenne	R élevée
	Transmission de signaux complémentaires	A.11.4	R faible	R faible	R moyenne	R élevée
	Diversité du matériel (voir Note 6)	B.1.4	– faible	– faible	– Moyenne	R élevée
	Architecture du logiciel	**7.4.3 de la CEI 61508-3**	Voir Tableaux A.2 et C.2 de la CEI 61508-3			

Ce tableau est divisé en trois groupes, comme indiqué par l'ombrage de la barre latérale. Toutes les techniques marquées «R» dans les groupes ombrés de couleur grise et noire peuvent être remplacées par d'autres techniques dans ce même groupe, mais au moins une des techniques du groupe grisé et au moins une des techniques du groupe ombré en noir est requise.

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède immédiatement le Tableau A.15.

NOTE 2 La plupart des mesures décrites dans ce tableau peuvent être utilisées pour faire varier l'efficacité conformément au Tableau A.18 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans les Annexes A et B de la CEI 61508-7. Le paragraphe applicable est référencé dans la deuxième colonne.

NOTE 4 La séparation entre les lignes d'alimentation électrique et les lignes de données n'est pas nécessaire en cas de transport optique des informations ou pour les lignes d'alimentation électrique de faible puissance qui sont conçues pour alimenter les éléments du système E/E/PE et véhiculer de l'information à partir de ou vers ces éléments.

NOTE 5 Pour les systèmes E/E/PE relatifs à la sécurité utilisés dans un mode de fonctionnement à faible sollicitation (par exemple, systèmes d'arrêt d'urgence), la couverture de diagnostic obtenue à partir de la détection de défaillance par surveillance en ligne est généralement faible ou inexistante.

NOTE 6 La diversité du matériel n'est pas requise s'il a été démontré, par validation et par une large expérience opérationnelle, que le matériel est suffisamment exempt d'anomalies de conception et protégé contre les défaillances de cause commune pour satisfaire aux objectifs chiffrés de défaillance.

Tableau A.17 – Techniques et mesures pour maîtriser les défaillances systématiques en exploitation

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Protection contre les modifications	B.4.8	M faible	M moyenne	M élevée	M élevée
	Détection des défaillances par surveillance en ligne (voir Note 4)	A.1.1	R faible	R faible	R moyenne	R élevée
	Accusé de réception des entrées	B.4.9	R faible	R faible	R moyenne	R élevée
	Programmation par assertion des défaillances	C.3.3	Voir Tableaux A.2 et C.2 de la CEI 61508-3			

Au moins une des techniques du groupe ombré est requise.

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède immédiatement le Tableau A.15.

NOTE 2 Deux des mesures décrites dans ce tableau peuvent être utilisées pour faire varier l'efficacité conformément au Tableau A.18 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans les Annexes A, B et C de la CEI 61508-7. Le paragraphe applicable est référencé dans la deuxième colonne.

NOTE 4 Pour les systèmes E/E/PE relatifs à la sécurité utilisés dans un mode de fonctionnement à faible sollicitation (par exemple, systèmes d'arrêt d'urgence), la couverture de diagnostic obtenue à partir de la détection de défaillance par surveillance en ligne est généralement faible ou inexistante.

Tableau A.18 – Efficacité des techniques et mesures pour la maîtrise des défaillances systématiques

Technique/mesure	Voir CEI 61508-7	Faible efficacité	Efficacité élevée
Détection des défaillances par surveillance en ligne (voir Note)	A.1.1	Des signaux de déclenchement de l'EUC et de son système de commande sont utilisés pour contrôler le fonctionnement correct des systèmes E/E/PE relatifs à la sécurité (uniquement comportement temporel avec une limite de temps supérieure)	Les systèmes E/E/PE relatifs à la sécurité sont réenclenchés par des signaux temporels et logiques en provenance de l'EUC et de son système de commande (fenêtre temporelle pour fonction de chien de garde temporelle)
Essais par un matériel redondant (voir note)	A.2.1	Du matériel supplémentaire est utilisé pour soumettre à l'essai les signaux de déclenchement des systèmes E/E/PE relatifs à la sécurité (uniquement comportement temporel avec une limite de temps supérieure); ce matériel commute un élément final secondaire	Le matériel supplémentaire est réenclenché par des signaux temporels et logiques en provenance des systèmes E/E/PE relatifs à la sécurité (fenêtre temporelle pour chien de garde temporel); dispositif de vote majoritaire entre plusieurs canaux
Port d'accès d'essai normalisé et architecture d'essai du type «registre à décalage périphérique (Scan Path) »	A.2.3	Essais de la logique à semi-conducteurs utilisée pendant l'essai périodique par le biais d'essais du type «registre à décalage périphérique (Scan Path)» définis	Essai de diagnostic de la logique à semi-conducteurs, conformément à la spécification fonctionnelle des systèmes E/E/PE relatifs à la sécurité; toutes les fonctions de tous les circuits intégrés sont contrôlées
Protection par code	A.6.2	Détection des défaillances par redondance temporelle de la transmission de signaux	Détection des défaillances par redondance temporelle et redondance des informations de transmission de signaux
Mesures contre l'interruption de tension, les variations de tension, la surtension et les sous-tensions	A.8	Protection contre les surtensions avec arrêt de sécurité ou commutation sur la seconde unité d'alimentation	Réglage de la tension (secondaire) avec arrêt de sécurité ou commutation sur la seconde unité d'alimentation; ou mise hors tension avec arrêt de sécurité ou commutation sur la seconde unité d'alimentation
Surveillance de la séquence du programme	A.9	Surveillance temporelle ou logique de la séquence du programme	Surveillance temporelle et logique de la séquence du programme en de très nombreux points de contrôle de ce dernier
Mesures contre les surchauffes	A.10	Détection de la surchauffe	Actionnement de l'arrêt de sécurité par l'intermédiaire d'un fusible thermique; ou plusieurs niveaux de détection de la surchauffe et d'alarmes; ou connexion du refroidissement par air forcé et indication d'état
Augmentation de l'immunité aux interférences (voir Note)	A.11.3	Filtre antibruit au niveau de l'alimentation et au niveau des entrées et sorties critiques; blindage si nécessaire	Filtres contre des perturbations électromagnétiques normalement inattendues; blindage
Mesures contre l'environnement physique	A.14	Pratique généralement acceptée pour l'application considérée	Techniques référencées dans les normes pour une application particulière
Diversité du matériel	B.1.4	Deux ou plusieurs éléments réalisant la même fonction mais différents de conception	Deux ou plusieurs éléments réalisant des fonctions différentes
Protection contre les modifications	B.4.8	La modification nécessite des outils spécifiques	La modification nécessite l'utilisation d'un verrou à clé ou d'un outil dédié avec mot de passe

Technique/mesure	Voir CEI 61508-7	Faible efficacité	Efficacité élevée
Accusé de réception des entrées	B.4.9	Contrôle par retour des actions de saisie vers l'opérateur	Vérification des règles strictes applicables à la saisie des données par l'opérateur, rejet des saisies incorrectes
NOTE Dans le cas des techniques référencées A.1.1, A.2.1, A.11.3 et A.14, il est supposé, pour une efficacité élevée de la technique ou de la mesure, que les approches de faible efficacité sont également utilisées.			

Annexe B
(normative)

Techniques et mesures applicables aux systèmes E/E/PE relatifs à la sécurité – évitement des défaillances systématiques lors des différentes phases du cycle de vie

Les Tableaux B.1 à B.5 de la présente annexe recommandent, pour chaque niveau d'intégrité de sécurité, des techniques et des mesures destinées à éviter les défaillances dans les systèmes E/E/PE relatifs à la sécurité. L'Annexe B de la CEI 61508-7 fournit des informations supplémentaires concernant les techniques et mesures applicables. Les exigences relatives aux mesures de maîtrise des défaillances en cours d'exploitation sont fournies à l'Annexe A de la CEI 61508-7.

Il n'est pas possible d'énumérer chaque cause particulière de défaillances systématiques, apparaissant au cours du cycle de vie de sécurité ou chaque remède applicable, et ce, pour deux raisons principales:

– l'effet d'une anomalie systématique dépend de la phase du cycle de vie au cours de laquelle elle a été introduite; et
– l'efficacité de toute mesure unique permettant d'éviter des défaillances systématiques dépend de l'application.

Il est par conséquent impossible d'effectuer une analyse quantitative d'évitement des défaillances systématiques.

Les défaillances des systèmes E/E/PE relatifs à la sécurité peuvent être classées en fonction de la phase du cycle de vie au cours de laquelle une anomalie causale est introduite de la manière suivante:

– des défaillances dues à des anomalies apparaissant *avant ou pendant l'installation du système* (par exemple, les anomalies logicielles comprennent des anomalies de spécification et de programme, les anomalies matérielles comprennent des anomalies de fabrication et une sélection d'éléments incorrecte); et
– des défaillances dues à des anomalies apparaissant *après installation du système* (par exemple, des défaillances aléatoires du matériel ou des défaillances dues à une utilisation incorrecte).

Pour éviter ou maîtriser ces défaillances, lorsqu'elles apparaissent, un grand nombre de mesures est en général nécessaire. La structure des exigences spécifiées dans les Annexes A et B résulte de la division des mesures en mesures *d'évitement de défaillances* pendant les différentes phases du cycle de vie de sécurité des systèmes E/E/PE (la présente annexe) et en mesures de *maîtrise des défaillances* au cours de l'exploitation (Annexe A). Les mesures destinées à maîtriser les défaillances sont des caractéristiques intégrées des systèmes E/E/PE relatifs à la sécurité tandis que les mesures destinées à éviter les défaillances sont mises en œuvre pendant le cycle de vie de sécurité.

Les Tableaux B.1 à B.5 formulent des recommandations et spécifient des exigences par niveau d'intégrité de sécurité en indiquant, en premier lieu, l'importance de la technique ou de la mesure et en second lieu, l'efficacité requise si cette technique ou mesure est utilisée. L'importance est décrite de la manière suivante:

– M: la technique ou mesure est requise (obligatoire) pour ce niveau d'intégrité de sécurité;
– HR: la technique ou mesure est vivement recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure n'est pas utilisée, les motifs sous-jacents doivent alors être décrits de manière détaillée;
– R: la technique ou mesure est recommandée pour ce niveau d'intégrité de sécurité;

– -: la technique ou mesure ne porte aucune recommandation pour ou contre son utilisation;

– NR: la technique ou mesure n'est absolument pas recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure est utilisée, les motifs sous-jacents doivent alors être décrits de manière détaillée.

L'efficacité requise est décrite de la manière suivante:

– Faible: si elle est utilisée, la technique ou mesure doit être appliquée dans la mesure nécessaire pour garantir au moins une faible efficacité contre les défaillances systématiques;

– Moyenne: si elle est utilisée, la technique ou mesure doit être appliquée dans la mesure nécessaire pour garantir au moins une efficacité moyenne contre les défaillances systématiques;

– Elevée: la technique ou mesure doit être appliquée dans la mesure nécessaire pour garantir une efficacité élevée contre les défaillances systématiques.

NOTE La plupart des mesures décrites dans les Tableaux B.1 à B.5 peuvent être utilisées avec une efficacité variable comme l'indique le Tableau B.6, qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

Si une mesure n'est pas obligatoire, elle peut, en principe, être remplacée par d'autres mesures (soit prises séparément, soit en combinaison); ceci est régi par l'ombrage (de la zone correspondante) comme expliqué dans chaque tableau.

Le fait de se conformer aux recommandations de la présente annexe ne garantit pas en soi l'intégrité de sécurité requise. Il est important de tenir compte des éléments suivants:

– la cohérence des techniques et mesures choisies ainsi que la manière dont elles se complètent;

– les techniques et mesures qui conviennent à chaque phase du cycle de vie de développement; et

– les techniques et les mesures qui sont les mieux adaptées aux problèmes spécifiques rencontrés au cours du développement de chaque système E/E/PE relatif à la sécurité différent.

Tableau B.1 – Techniques et mesures pour éviter les erreurs lors de la spécification des exigences de conception des systèmes E/E/PE (voir 7.2)

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Gestion de projet	B.1.1	M faible	M faible	M moyenne	M élevée
	Documentation	B.1.2	M faible	M faible	M moyenne	M élevée
	Séparation des systèmes E/E/PE relatifs à la sécurité et des systèmes non relatifs à la sécurité	B.1.3	HR faible	HR faible	HR moyenne	HR élevée
	Spécification structurée	B.2.1	HR faible	HR faible	HR moyenne	HR élevée
	Inspection de la spécification	B.2.6	– faible	HR faible	HR moyenne	HR élevée
	Méthodes semi-formelles	B.2.3, voir également Tableau B.7 de la CEI 61508-3	R faible	R faible	HR moyenne	HR élevée
	Listes de contrôle	B.2.5	R faible	R faible	R moyenne	R élevée
	Outils de spécification assistée par ordinateur	B.2.4	- faible	R faible	R moyenne	R élevée
	Méthodes formelles	B.2.2	– faible	– faible	R moyenne	R élevée

Toutes les techniques repérées par «R» dans le groupe ombré sont remplaçables, mais au moins une d'entre elles est requise.

Pour la vérification de cette phase du cycle de vie de sécurité, au moins une des techniques ou mesures ombrées dans ce tableau ou énumérées dans le Tableau B.5 doit être utilisée.

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède ce tableau.

NOTE 2 Les mesures décrites dans ce tableau peuvent être utilisées pour faire varier l'efficacité conformément au Tableau B.6 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans l'Annexe B de la CEI 61508-7. Les paragraphes applicables sont référencés dans la deuxième colonne.

Tableau B.2 – Techniques et mesures pour éviter l'introduction d'anomalies lors de la conception et du développement des systèmes E/E/PE (voir 7.4)

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Respect des lignes directrices et normes	B.3.1	M élevée	M élevée	M élevée	M élevée
	Gestion de projet	B.1.1	M faible	M faible	M moyenne	M élevée
	Documentation	B.1.2	M faible	M faible	M moyenne	M élevée
	Conception structurée	B.3.2	HR faible	HR faible	HR moyenne	HR élevée
	Modularisation	B.3.4	HR faible	HR faible	HR moyenne	HR élevée
	Utilisation d'éléments ayant fait leurs preuves	B.3.3	R faible	R faible	R moyenne	R élevée
	Méthodes semi-formelles	B.2.3, voir également Tableau B.7 de la CEI 61508-3	R faible	R faible	HR moyenne	HR élevée
	Listes de contrôle	B.2.5	– faible	R faible	R moyenne	R élevée
	Outils de conception assistée par ordinateur	B.3.5	– faible	R faible	R moyenne	R élevée
	Simulation	B.3.6	– faible	R faible	R moyenne	R élevée
	Inspection du matériel ou sondage du matériel	B.3.7 B.3.8	– faible	R faible	R moyenne	R élevée
	Méthodes formelles	B.2.2	– faible	– faible	R moyenne	R élevée

Toutes les techniques repérées par «R» dans le groupe ombré sont remplaçables, mais au moins une d'entre elles est requise.

Pour la vérification de cette phase du cycle de vie de sécurité, au moins une des techniques ou mesures ombrées dans ce tableau ou énumérées dans le Tableau B.5 doit être utilisée.

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède le Tableau B.1.

NOTE 2 La plupart de ces mesures décrites dans ce tableau peuvent être utilisées pour faire varier l'efficacité conformément au Tableau B.6 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans l'Annexe B de la CEI 61508-7. Les paragraphes applicables sont référencés dans la deuxième colonne.

Tableau B.3 – Techniques et mesures pour éviter les anomalies lors de l'intégration des systèmes E/E/PE (voir 7.5)

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Essais fonctionnels	B.5.1	M élevée	M élevée	M élevée	M élevée
	Gestion de projet	B.1.1	M faible	M faible	M moyenne	M élevée
	Documentation	B.1.2	M faible	M faible	M moyenne	M élevée
	Essai «boîte noire»	B.5.2	R faible	R faible	R moyenne	R élevée
	Expérience pratique	B.5.4	R faible	R faible	R moyenne	R élevée
	Essais statistiques	B.5.3	– faible	– faible	R moyenne	R élevée

Toutes les techniques repérées par «R» dans le groupe ombré sont remplaçables, mais au moins une d'entre elles est requise.

Pour la vérification de cette phase du cycle de vie de sécurité, au moins une des techniques ou mesures ombrées dans ce tableau ou énumérées dans le Tableau B.5 doit être utilisée.

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède le Tableau B.1.

NOTE 2 La plupart de ces mesures décrites dans ce tableau peuvent être utilisées pour faire varier l'efficacité conformément au Tableau B.6 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans l'Annexe B de la CEI 61508-7. Les paragraphes applicables sont référencés dans la deuxième colonne.

Tableau B.4 – Techniques et mesures pour éviter les anomalies et les défaillances pendant les procédures d'exploitation et de maintenance des systèmes E/E/PE (voir 7.6)

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Instructions d'exploitation et de maintenance	B.4.1	HR élevée	HR élevée	HR élevée	HR élevée
	Facilité d'utilisation	B.4.2	HR élevée	HR élevée	HR élevée	HR élevée
	Facilité de maintenance	B.4.3	HR élevée	HR élevée	HR élevée	HR élevée
	Gestion de projet	B.1.1	M faible	M faible	M moyenne	M élevée
	Documentation	B.1.2	M faible	M faible	M moyenne	M élevée
	Possibilités d'exploitation limitées	B.4.4	– faible	R faible	HR moyenne	HR élevée
	Protection contre les erreurs humaines	B.4.6	– faible	R faible	HR moyenne	HR élevée
	Exploitation uniquement par des opérateurs qualifiés	B.4.5	– faible	R faible	R moyenne	HR élevée

Toutes les techniques repérées par «R» dans le groupe ombré sont remplaçables, mais au moins une d'entre elles est requise.

La vérification de cette phase du cycle de vie de sécurité doit être effectuée au moyen de listes de contrôle (voir B.2.5 de la CEI 61508-7) ou par inspection (voir B.2.6 de la CEI 61508-7).

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède le Tableau B.1.

NOTE 2 La plupart de ces mesures décrites dans ce tableau peuvent être utilisées pour faire varier l'efficacité conformément au Tableau B.6 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans l'Annexe B de la CEI 61508-7. Les paragraphes applicables sont référencés dans la deuxième colonne.

Tableau B.5 – Techniques et mesures pour éviter les anomalies lors de la validation de sécurité des systèmes E/E/PE (voir 7.7)

	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	Essais fonctionnels	B.5.1	HR élevée	HR élevée	HR élevée	HR élevée
	Essais fonctionnels dans des conditions environnementales	B.6.1	HR élevée	HR élevée	HR élevée	HR élevée
	Essai d'immunité aux interférences/et aux ondes de choc	B.6.2	HR élevée	HR élevée	HR élevée	HR élevée
	Essai d'insertion d'anomalie (le cas échéant couverture de diagnostic ≥ 90 %)	B.6.10	HR élevée	HR élevée	HR élevée	HR élevée
	Gestion de projet	B.1.1	M faible	M faible	M moyenne	M élevée
	Documentation	B.1.2	M faible	M faible	M moyenne	M élevée
	Analyse statique, analyse dynamique et analyse de défaillance	B.6.4 B.6.5 B.6.6	– faible	R faible	R moyenne	R élevée
	Simulation et analyse des défaillances	B.3.6 B.6.6	– faible	R faible	R moyenne	R élevée
	Analyse du «cas le plus défavorable», analyse dynamique et analyse de défaillance	B.6.7 B.6.5 B.6.6	– faible	– faible	R moyenne	R élevée
	Analyse statique et analyse de défaillance (voir Note 4)	B.6.4 B.6.6	R faible	R faible	NR	NR
	Essais fonctionnels étendus	B.6.8	– faible	HR faible	HR moyenne	HR élevée
	Essai «boîte noire»	B.5.2	R faible	R faible	R moyenne	R élevée
	Essai d'insertion d'anomalie (le cas échéant couverture de diagnostic < 90 %)	B.6.10	R faible	R faible	R moyenne	R élevée
	Essais statistiques	B.5.3	– faible	– faible	R moyenne	R élevée
	Essai du «cas le plus défavorable»	B.6.9	– faible	– faible	R moyenne	R élevée
	Expérience pratique	B.5.4	R faible	R faible	R moyenne	NR

Ce tableau est divisé en trois groupes, comme indiqué par l'ombrage de la barre latérale. Toutes les techniques marquées «R» dans les groupes ombrés de couleur grise et noire peuvent être remplacées par d'autres techniques dans ce même groupe, mais au moins une des techniques du groupe grisé (techniques d'analyse) et au moins une des techniques du groupe ombré en noir (techniques d'essai) est requise.

NOTE 1 Pour la signification des entrées dans chaque niveau d'intégrité de sécurité, voir le texte qui précède le Tableau B.1.

NOTE 2 La plupart de ces mesures décrites dans ce tableau peuvent être utilisées pour faire varier l'efficacité conformément au Tableau B.6 qui donne des exemples d'efficacité faible et élevée. L'effort requis pour une efficacité moyenne se situe entre l'effort spécifié pour une efficacité faible et l'effort spécifié pour une efficacité élevée.

NOTE 3 La présentation générale des techniques et mesures examinées dans ce tableau est donnée dans l'Annexe B de la CEI 61508-7. Les paragraphes applicables sont référencés dans la deuxième colonne.

NOTE 4 Il n'est pas recommandé d'analyse statique et d'analyse des défaillances pour les SIL 3 et SIL 4, dans la mesure où ces techniques ne sont pas suffisantes à moins qu'elles ne soient utilisées en association avec une analyse dynamique.

Tableau B.6 – Efficacité des techniques et mesures d'évitement des défaillances systématiques

Technique/mesure	Voir CEI 61508-7	Faible efficacité	Efficacité élevée
Gestion de projet (voir Note)	B.1.1	Définition des actions et responsabilités; ordonnancement et affectation des ressources; formation du personnel correspondant; contrôles de cohérence après modifications	Validation indépendante de la conception; surveillance de projet; procédure de validation normalisée; gestion de configuration; statistique des défaillances; ingénierie assistée par ordinateur; ingénierie logicielle assistée par ordinateur
Documentation (voir Note)	B.1.2	Descriptions en langage graphique et naturel, par exemple, schémas fonctionnels, organigrammes	Recommandations pour contenu et représentation cohérents dans toute la topologie; listes de contrôle du contenu; gestion de la documentation assistée par ordinateur; maîtrise formelle des modifications
Séparation entre systèmes E/E/PE relatifs à la sécurité et systèmes non relatifs à la sécurité	B.1.3	Interfaces bien définies entre systèmes E/E/PE relatifs à la sécurité et systèmes non relatifs à la sécurité	Séparation totale entre les systèmes E/E/PE relatifs à la sécurité et les systèmes non relatifs à la sécurité, c'est-à-dire pas d'échange de données entre les systèmes non relatifs à la sécurité et emplacements physiques séparés pour éviter les influences de cause commune
Spécification structurée	B.2.1	Séparation hiérarchique manuelle en sous-exigences; description des interfaces	Séparation hiérarchique décrite en utilisant des outils d'ingénierie assistée par ordinateur; contrôles de cohérence automatique; affinage jusqu'au niveau fonctionnel
Méthodes formelles	B.2.2	Utilisé par un personnel expérimenté dans le domaine des méthodes formelles	Utilisé par un personnel expérimenté dans le domaine des méthodes formelles pour des applications similaires, au moyen d'outils informatisés
Méthodes semi-formelles	B.2.3	Description de certaines parties critiques au moyen de méthodes semi-formelles	Description de l'ensemble des systèmes E/E/PE relatifs à la sécurité au moyen de différentes méthodes semi-formelles pour illustrer les différents aspects; contrôle de cohérence entre les méthodes
Outils de spécification assistée par ordinateur	B.2.4	Outils sans aucune préférence pour une méthode de conception particulière	Procédures orientées modèle avec subdivision hiérarchique; description de tous les objets et de leurs relations; base de données commune; contrôles de cohérence automatique
Listes de contrôle	B.2.5	Listes de contrôle préparées pour toutes les phases du cycle de vie de sécurité; concentration sur les principaux problèmes de sécurité	Listes de contrôle détaillées préparées pour toutes les phases du cycle de vie de sécurité
Inspection de la spécification	B.2.6	Inspection de la spécification des exigences de sécurité par une personne indépendante	Inspection et réinspection par un organisme indépendant en utilisant une procédure formelle, avec correction de toutes les anomalies constatées
Conception structurée	B.3.2	Conception hiérarchique des circuits, produite manuellement	Réutilisation des parties de circuit soumises à essai; traçabilité entre spécification, conception, diagramme de circuit et listes de composants; conception informatisée; fondée sur des méthodes définies (voir également 7.4.6)

Tableau B.6 *(suite)*

Technique/mesure	Voir CEI 61508-7	Faible efficacité	Efficacité élevée
Utilisation d'éléments ayant fait leurs preuves (voir Note)	B.3.3	Surdimensionnement suffisant; caractéristiques de construction	Efficacité éprouvée par une utilisation antérieure (voir 7.4.10)
Modularisation (voir Note)	B.3.4	Modules de taille limitée; chaque module fonctionnellement isolé	Réutilisation de modules éprouvés par une utilisation antérieure; modules facilement compréhensibles; chaque module a au maximum une entrée, une sortie et une sortie de défaillance
Outils de conception assistée par ordinateur	B.3.5	Support informatique pour les phases complexes du cycle de vie de sécurité	Utilisation d'outils qui sont éprouvés par une utilisation antérieure (voir 7.4.10) ou validés; développement général informatisé pour toutes les phases du cycle de vie de sécurité
Simulation	B.3.6	Modélisation au niveau module, y compris les données limites des unités périphériques	Modélisation au niveau composant, y compris les données limites
Inspection du matériel	B.3.7	Inspection par une personne indépendante de la conception	Inspection et réinspection par un organisme indépendant en utilisant une procédure formelle, avec correction de toutes les anomalies constatées
Sondage du matériel	B.3.8	Le sondage comprend une personne indépendante de la conception	Le sondage comprend un organisme indépendant et suit une procédure formelle, avec correction de toutes les anomalies constatées
Possibilités d'exploitation limitées (voir Note)	B.4.4	Commutateur à clé ou mot de passe pour régir les changements de mode d'exploitation	Procédure définie et robuste pour permettre l'exploitation
Exploitation uniquement par des opérateurs qualifiés	B.4.5	Formation de base dans le type de système de sécurité en exploitation, plus deux ans d'expérience du travail correspondant	Formation annuelle de tous les opérateurs; chaque opérateur a au moins 5 années d'expérience en matière de dispositifs relatifs à la sécurité, à des niveaux d'intégrité de sécurité inférieurs
Protection contre les erreurs humaines (voir Note)	B.4.6	Accusé de réception des entrées	Confirmation et contrôles de cohérence sur chaque commande de saisie
Essai «boîte noire» (voir Note)	B.5.2	Classes d'équivalence et essais de partition des entrées, essais des valeurs limites, en utilisant des essais élémentaires préécrits	Exécution de l'essai élémentaire à partir de diagrammes cause/conséquence, en combinant des cas critiques à des limites d'exploitation extrêmes
Essais statistiques (voir Note)	B.5.3	Répartition statistique de toutes les données en entrée	Comptes-rendus des essais effectués au moyen d'outils; essais élémentaires très nombreux; répartition des données d'entrée conformément aux conditions d'application réelles et aux modèles de défaillance supposés
Expérience pratique (voir Note)	B.5.4	10 000 h de temps d'exploitation; au moins une année d'expérience avec au moins 10 dispositifs dans différentes applications; précision statistique de 95 %; pas de défaillances critiques pour la sécurité	10 millions d'heures de temps d'exploitation; au moins 2 années d'expérience avec au moins 10 dispositifs dans différentes applications; précision statistique de 99,9 %; documentation détaillée de toutes les modifications (y compris les modifications mineures) effectuées lors d'une exploitation antérieure

Tableau B.6 *(suite)*

Technique/mesure	Voir CEI 61508-7	Faible efficacité	Efficacité élevée
Essai d'immunité aux ondes de choc	B.6.2		Il doit être possible de démontrer que l'immunité aux ondes de choc est supérieure aux valeurs limites pour des conditions de fonctionnement réelles
Analyse statique	B.6.4	Sur la base des schémas fonctionnels; en faisant ressortir les points faibles; en spécifiant les essais élémentaires	Sur la base des diagrammes détaillés; en prévoyant le comportement attendu lors des essais élémentaires; en utilisant des outils d'essai
Analyse dynamique	B.6.5	Sur la base des schémas fonctionnels; en faisant ressortir les points faibles; en spécifiant les essais élémentaires	Sur la base des diagrammes détaillés; en prévoyant le comportement attendu lors des essais élémentaires; en utilisant des outils d'essai
Analyse de la défaillance	B.6.6	Au niveau module, y compris les données limites des unités périphériques	Au niveau composant, y compris les données limites
Analyse du «cas le plus défavorable»	B.6.7	Effectuée sur des fonctions relatives à la sécurité; déduites en utilisant des combinaisons de valeurs limites pour des conditions réelles d'exploitation	Effectuée sur des fonctions non relatives à la sécurité; déduites en utilisant des combinaisons de valeurs limites pour des conditions réelles d'exploitation
Essais fonctionnels étendus	B.6.8	Essai permettant d'assurer que toutes les fonctions relatives à la sécurité sont maintenues en cas d'états d'entrée statiques dus à un processus défectueux ou à de mauvaises conditions d'exploitation	Essai permettant d'assurer que toutes les fonctions relatives à la sécurité sont maintenues en cas d'états d'entrée statiques et/ou changements inhabituels d'entrée dus à un processus défectueux ou à de mauvaises conditions d'exploitation (y compris celles qui peuvent être très rares)
Essai du «cas le plus défavorable»	B.6.9	Essai permettant d'assurer que les fonctions relatives à la sécurité sont maintenues pour une combinaison de valeurs limites rencontrées dans des conditions d'exploitation réelles	Essai permettant d'assurer que les fonctions non relatives à la sécurité sont maintenues pour une combinaison de valeurs limites rencontrées dans des conditions d'exploitation réelles
Essai d'insertion d'anomalie	B.6.10	Au niveau sous-unité, y compris des données limites ou les unités périphériques	Au niveau composant, y compris les données limites
NOTE Dans le cas des techniques référencées B.1.1, B.1.2, B.3.3, B.3.4, B.4.4, B.4.6, B.5.2, B.5.3, B.5.4, B.6.7 et B.6.9, il est supposé, pour une efficacité élevée de la technique ou de la mesure, que les approches de faible efficacité sont également utilisées.			

Annexe C
(normative)

Couverture de diagnostic et proportion de défaillances en sécurité

C.1 Calcul de la couverture de diagnostic et de la proportion de défaillances en sécurité d'un élément matériel

La couverture de diagnostic et la proportion de défaillances en sécurité d'un élément (voir 3.8.6 et 3.6.15 de la CEI 61508-4 respectivement) doivent être calculées de la façon suivante:

a) Effectuer l'analyse des modes de défaillance et de leurs effets afin de déterminer l'effet de chaque mode de défaillance de chaque composant ou groupe de composants de l'élément sur le comportement des systèmes E/E/PE relatifs à la sécurité en l'absence d'essais de diagnostic. Une information suffisante doit être disponible (voir les Notes 1 et 2) pour faire en sorte que l'analyse des modes de défaillance et de leurs effets à entreprendre permette qu'un niveau de confiance approprié soit établi en rapport avec les exigences d'intégrité de sécurité.

NOTE 1 Pour entreprendre cette analyse, les informations suivantes sont nécessaires:

– un diagramme détaillé du système E/E/PE relatif à la sécurité, décrivant l'élément avec ses interconnexions pour la partie de ce système qui affecte la ou les fonctions de sécurité considérées;

– la schématique du matériel de l'élément décrivant chaque composant ou groupe de composants ainsi que les interconnexions entre composants;

– les modes et taux de défaillance de chaque composant ou groupe de composants et les pourcentages correspondants de la probabilité de défaillance totale correspondant aux défaillances en sécurité et aux défaillances dangereuses.

NOTE 2 La rigueur nécessaire de cette analyse dépend d'un certain nombre de facteurs (voir la CEI 61508-1, 4.1). En particulier, le niveau d'intégrité de sécurité des fonctions de sécurité impliquées devra être pris en compte. Pour les niveaux d'intégrité de sécurité les plus élevés, il est prévu que l'analyse des modes de défaillance et de leurs effets soit très spécifique, en fonction de types particuliers de composants et des environnements de l'application. De même, une analyse exhaustive et détaillée est très importante pour un élément destiné à une utilisation dans une architecture matérielle ayant une tolérance nulle aux anomalies du matériel.

b) Classer chaque mode de défaillance par catégorie, selon qu'il donne lieu (en l'absence d'essais de diagnostic) à:
   – une défaillance en sécurité; ou
   – une défaillance dangereuse;

c) le calcul de la couverture de diagnostic ou de la proportion de défaillances en sécurité ne doit pas prendre en compte les défaillances sans effet et les défaillances partielles.

d) A partir d'une estimation du taux de défaillance de chaque composant ou groupe de composants, (λ_i) (voir Note 4) et des résultats de l'analyse des modes de défaillance et de leurs effets, pour chaque composant ou groupe de composants, calculer le taux de défaillance en sécurité, (λ_S), et le taux de défaillance dangereuse, (λ_D). Lorsque l'un de ces taux de défaillance n'est pas constant, sa moyenne sur la période doit être estimée et utilisée dans les calculs de DC et SFF.

NOTE 3 Le taux de défaillance de chaque composant ou groupe de composants peut être estimé sur la base de données provenant d'une origine industrielle reconnue, en prenant en compte l'environnement d'application. Toutefois, des données spécifiques à l'application sont préférables, particulièrement dans les cas où l'élément consiste en un petit nombre de composants et où toute erreur dans l'estimation de la probabilité de défaillances en sécurité et de défaillances dangereuses d'un composant particulier est susceptible d'avoir un impact significatif sur l'estimation de la proportion de défaillances en sécurité.

e) Pour chaque composant ou groupe de composants, estimer la proportion de défaillances dangereuses qui seront détectées par les essais de diagnostic (voir C.2) et, par conséquent, le taux de défaillances dangereuses détectées par les essais de diagnostic, (λ_{Dd}).

f) Pour l'élément, calculer le taux total de défaillances dangereuses, ($\Sigma\lambda_D$), le taux total de défaillances dangereuses détectées par les essais de diagnostic, ($\Sigma\lambda_{Dd}$) et le taux total de défaillances en sécurité, ($\Sigma\lambda_S$).

g) Calculer la couverture de diagnostic de l'élément sous la forme ($\Sigma\lambda_{Dd}/\Sigma\lambda_D$).

h) Calculer la proportion de défaillances en sécurité de l'élément sous la forme:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

NOTE 4 L'équation ci-dessus est applicable lorsque les taux de défaillance sont basés sur des taux de défaillance constants (voir 3.6.15 de la CEI 61508-4 pour la formule définitive).

NOTE 5 La couverture de diagnostic (le cas échéant) de chaque élément constitutif du système E/E/PE relatif à la sécurité est prise en compte dans l'estimation de la mesure de défaillance réalisée pour chaque fonction de sécurité (voir 7.4.5.2). La proportion de défaillances en sécurité est prise en compte lors de la détermination des contraintes architecturales sur l'intégrité de sécurité du matériel (voir 7.4.4).

L'analyse utilisée pour déterminer la couverture de diagnostic et la proportion de défaillances en sécurité doit couvrir tous les composants, y compris électriques, électroniques, électromécaniques, mécaniques, etc., nécessaires pour permettre l'exécution de la ou des fonctions de sécurité de l'élément, selon les exigences du système E/E/PE relatif à la sécurité. Tous les modes de défaillance dangereuse possibles conduisant à un état de non sécurité, empêchant une réponse en sécurité lorsqu'une telle réponse est exigée, ou compromettant autrement l'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité, doivent être considérés pour chacun des composants.

Le Tableau A.1 donne les anomalies ou les défaillances qui doivent être détectées en fonctionnement ou analysées dans la dérivation de la proportion de défaillances en sécurité.

Si des données d'expérience sont utilisées pour faciliter l'analyse des modes de défaillance et de leurs effets, elles doivent être suffisantes en rapport avec les exigences d'intégrité de sécurité. Au minimum, une limite de confiance inférieure, unilatérale, statistique de 70 % au moins est requise.

NOTE 6 Un exemple de calcul de la couverture de diagnostic et de la proportion de défaillances en sécurité est intégré à l'Annexe C de la CEI 61508-6.

NOTE 7 D'autres méthodes sont disponibles pour le calcul de la couverture de diagnostic, y compris, par exemple, la simulation d'anomalies par l'utilisation d'un modèle informatique décrivant à la fois les circuits des systèmes E/E/PE relatifs à la sécurité et les composants électroniques utilisés pour leur conception (par exemple jusqu'au niveau du transistor dans un circuit intégré).

C.2 Détermination des facteurs de couverture de diagnostic

Dans le calcul de la couverture de diagnostic pour un élément (voir C.1), il est nécessaire d'estimer, pour chaque composant ou groupe de composants, la proportion de défaillances dangereuses détectées par les essais de diagnostic. Les essais de diagnostic qui peuvent contribuer à la couverture de diagnostic comprennent, sans toutefois s'y limiter:

– les vérifications par comparaison, par exemple surveillance et comparaison de signaux redondants;

– les essais périodiques intégrés supplémentaires, par exemple les sommes de vérification d'une mémoire;

– les essais par des stimuli externes, par exemple l'envoi d'un signal pulsé par des canaux d'essai;

– la surveillance permanente d'un signal analogique, par exemple pour détecter des valeurs hors gamme indiquant la défaillance d'un capteur.

Le calcul de la couverture de diagnostic nécessite de déterminer les modes de défaillance qui sont détectés par les essais de diagnostic. Il est possible que les défaillances par circuits ouverts ou par courts-circuits, pour les composants simples (résistances, condensateurs, transistors), soient détectables avec une couverture de 100 %. Cependant pour des éléments

plus complexes de type B, voir 7.4.4.1.3, il convient de tenir compte des limites de la couverture de diagnostic pour les différents composants présentés dans le Tableau A.1. Cette analyse doit être effectuée pour chaque composant, ou groupe de composants, de chaque élément et pour chaque élément du système E/E/PE relatif à la sécurité.

NOTE 1 Les Tableaux A.2 à A.14 recommandent des techniques et mesures pour les essais de diagnostic et la couverture de diagnostic maximale qui peut être déclarée. Ces essais peuvent être permanents ou périodiques (en fonction de l'intervalle d'essais de diagnostic). Les tableaux ne se substituent pas aux exigences de la présente annexe.

NOTE 2 Les essais de diagnostic peuvent constituer un avantage significatif, dans la réalisation de la sécurité fonctionnelle d'un système E/E/PE relatif à la sécurité. Toutefois il faut veiller à ne pas accroître inutilement la complexité qui, par exemple, peut conduire à des difficultés supplémentaires lors des activités de vérification, de validation, d'évaluation de la sécurité fonctionnelle, de maintenance et de modification. Une complexité accrue peut également rendre plus difficile le maintien à long terme de la sécurité fonctionnelle du système E/E/PE relatif à la sécurité.

Les calculs d'obtention de la couverture de diagnostic et la façon d'utiliser celle-ci supposent que l'EUC peut être exploité en sécurité en présence d'une autre anomalie dangereuse détectée par les essais de diagnostic. Si cette hypothèse n'est pas correcte, le système E/E/PE relatif à la sécurité doit alors être traité comme étant exploité en mode sollicitation élevée/continu (voir 7.4.8.3, 7.4.5.3 et 7.4.5.4).

NOTE 3 La définition de la « couverture de diagnostic » est fournie en 3.8.6 de la CEI 61508-4. Il est important de noter que d'autres définitions de la couverture de diagnostic sont parfois prises comme hypothèses mais qu'elles ne sont pas applicables dans le cadre de la présente norme.

NOTE 4 Les essais de diagnostic utilisés pour détecter une défaillance dangereuse dans un élément peuvent être réalisés par un autre élément du système E/E/PE relatif à la sécurité.

NOTE 5 Les essais de diagnostic peuvent être permanents ou périodiques, en fonction de l'intervalle d'essais de diagnostic. Il peut y avoir des cas, ou des moments, pour lesquels il convient de ne pas exécuter un essai de diagnostic en raison de la possibilité d'affecter, par un essai, l'état du système d'une manière préjudiciable. Dans ce cas, aucun bénéfice ne peut être tiré des essais de diagnostic pour les calculs.

Annexe D
(normative)

Manuel de sécurité d'article conforme

D.1 Généralités

Le manuel de sécurité d'article conforme a pour objet de documenter toutes les informations, relatives à un article conforme, et qui sont nécessaires pour permettre d'intégrer cet article dans un système relatif à la sécurité, un sous-système ou un élément, conformément aux exigences de la présente norme.

D.2 Contenu

D.2.1 Le manuel de sécurité doit spécifier les fonctions de l'article conforme. Ces fonctions peuvent être utilisées pour assister une fonction de sécurité d'un système relatif à la sécurité, ou les fonctions d'un sous-système ou d'un élément. Il convient que la spécification décrive de manière claire à la fois les fonctions et les interfaces d'entrée et de sortie.

Pour chaque article conforme, le manuel de sécurité doit contenir:

a) une spécification fonctionnelle des fonctions pouvant être exécutées;

b) l'identification de la configuration matérielle et/ou logicielle de l'article conforme afin de permettre la gestion de configuration du système E/E/PE relatif à la sécurité, conformément à 6.2.1 de la CEI 61508-1;

c) les contraintes associées à l'utilisation de l'article conforme et/ou les hypothèses sur lesquelles l'analyse du comportement ou les taux de défaillance de l'article sont fondés.

D.2.2 Pour chaque fonction, le manuel de sécurité doit contenir:

a) les modes de défaillance de l'article conforme (en termes du comportement de ses sorties), dus aux défaillances aléatoires du matériel, qui entraînent une défaillance de la fonction et qui ne sont pas détectés par les essais de diagnostic internes à cet article;

b) pour chaque mode de défaillance défini en a), un taux de défaillance estimé;

c) les modes de défaillance de l'article conforme (en termes du comportement de ses sorties), dus aux défaillances aléatoires du matériel, qui entraînent une défaillance de la fonction et qui sont détectés par les essais de diagnostic internes à cet article;

d) les modes de défaillance du diagnostic, interne à l'article conforme (en termes du comportement de ses sorties), dus aux défaillances aléatoires du matériel, qui entraînent une défaillance du diagnostic à détecter les défaillances de la fonction;

e) pour chaque mode de défaillance défini en c) et en d), le taux de défaillance estimé;

f) pour chaque mode de défaillance défini en c) qui est détecté par un diagnostic interne à l'article conforme, l'intervalle des essais de diagnostic;

g) pour chaque mode de défaillance défini en c), les résultats de l'article conforme initiés par le diagnostic interne;

NOTE 1 Les résultats du diagnostic interne peuvent être utilisés pour générer des mesures supplémentaires (techniques/procédurales) applicables au système, sous-système ou élément E/E/PE relatif à la sécurité afin d'obtenir ou de maintenir un état de sécurité de l'EUC.

h) tout essai périodique et/ou toutes exigences de maintenance;

i) pour les modes de défaillance, par rapport à une fonction spécifiée, qui peuvent être détectés par un diagnostic externe, un nombre suffisant d'informations doit être fourni pour faciliter le développement d'une capacité de diagnostic externe. Ces informations

doivent comporter les détails des modes de défaillance, ainsi que les taux de défaillance associés à ces modes;

j) la tolérance aux anomalies du matériel;

k) le classement en type A ou B de la partie de l'article conforme qui garantit la fonction, (voir 7.4.4.1.2 et 7.4.4.1.3);

NOTE 2 Les modes de défaillance peuvent être classés comme « sûrs » ou « dangereux » uniquement lorsque l'application de l'article conforme est connue par rapport aux dangers que présente l'EUC. Par exemple, si un capteur est appliqué de manière à utiliser une sortie élevée pour indiquer un danger présenté par l'EUC (par exemple pression élevée), alors un mode de défaillance qui prévient toute indication correcte de ce danger (par exemple immobilisation basse de la sortie) serait classé comme dangereux, tandis qu'un mode de défaillance qui génère une sortie élevée du capteur serait classé comme sûr. Cela dépend de la méthode d'interprétation du signal du capteur par la logique du système relatif à la sécurité et ne peut donc pas être spécifié sans limiter la méthode d'application du capteur.

Le niveau de couverture de diagnostic déclaré pour un article conforme peut également varier d'une application à une autre selon l'étendue de tout diagnostic de la logique du système ou du traitement du signal externe susceptible de compléter tout diagnostic interne de l'article conforme.

Il s'ensuit que toute estimation de la tolérance aux anomalies du matériel ou de la proportion de défaillances en sécurité peut être effectuée uniquement si l'application de l'article conforme fait l'objet de contraintes. Ces contraintes ne sont pas maîtrisées par le fournisseur de l'article conforme. Par conséquent, le manuel de sécurité ne doit faire état d'aucune déclaration par rapport à la tolérance aux anomalies du matériel, à la proportion de défaillances en sécurité ou à toute caractéristique de sécurité fonctionnelle qui dépend de la connaissance des modes de défaillance en sécurité et de défaillance dangereuse, sauf spécification claire des hypothèses sous-jacentes par rapport à ce qui constitue ces modes.

D.2.3 Pour chaque fonction de l'article conforme susceptible d'une défaillance systématique, le manuel doit contenir:

a) la capabilité systématique de l'article conforme ou de la partie de l'élément qui garantit la fonction;

b) toutes instructions ou contraintes relatives à l'application de l'article conforme, et pertinentes pour la fonction, qu'il convient d'observer afin d'éviter des défaillances systématiques de cette entité.

NOTE L'intégrité de la sécurité systématique indiquée par la capabilité systématique peut être obtenue par le seul respect des instructions et des contraintes. Dans le cas de violations, la déclaration de la capabilité systématique est partiellement ou entièrement non valable.

D.2.4 Pour les exigences supplémentaires relatives aux articles conformes au logiciel, voir 7.4.2.12 et l'Annexe D de la CEI 61508-3.

Annexe E
(normative)

Exigences d'architecture particulières relatives aux circuits intégrés (CI) avec redondance sur la puce

E.1 Généralités

La présente annexe est référencée par 7.4.2.2 b).

Un ensemble d'exigences est donné ci-dessous afin de permettre l'utilisation de redondances internes sur la puce dans des circuits intégrés ayant un substrat semi-conducteur commun. Cette approche revêt pour des raisons de sécurité un caractère de prudence illustré par exemple par une limitation au SIL 3, un ensemble d'exigences restrictives ayant par ailleurs été spécifié. Les exigences suivantes sont associées aux seuls circuits intégrés numériques. Aucune exigence générale ne peut être actuellement spécifiée pour les circuits intégrés à mode mixte et analogiques. L'analyse de cause commune (voir 7.6.2.7 de la CEI 61508-1) peut exclure l'utilisation de la redondance à circuit imprimé pour une application individuelle. La redondance sur la puce utilisée dans la présente norme signifie une duplication (ou triplication, etc.) des unités fonctionnelles afin d'établir une tolérance aux anomalies du matériel supérieure à zéro. Selon 7.4.4.1.1 a), la détermination de la tolérance aux anomalies du matériel ne tient aucun compte des mesures susceptibles de maîtriser les effets des anomalies, telles que les diagnostics.

Un sous-système ayant une tolérance aux anomalies supérieure à zéro peut être réalisé avec un seul substrat semi-conducteur de circuit intégré (redondance sur la puce). Dans ce cas, l'ensemble des exigences suivantes a) à q) doit être satisfait et la conception du système E/E/PE et du circuit intégré doivent satisfaire à ces exigences. Un circuit intégré avec redondance sur la puce doit disposer de son propre manuel de sécurité d'article conforme (voir Annexe D).

a) le niveau d'intégrité de sécurité le plus élevé pouvant être déclaré pour une fonction de sécurité utilisant un circuit intégré tel que décrit ci-dessus, est limité au SIL 3;

NOTE 1 L'état de la technique, les connaissances et l'expérience actuels ne permettent pas de prendre en considération tous les effets associés à cet élément (circuit intégré simple), et de prendre les mesures nécessaires contre ces effets, et ce, afin d'avoir une confiance suffisante dans le SIL 4.

b) une combinaison des éléments ne doit pas contribuer à l'augmentation de la capabilité systématique (voir 7.4.3.2);

c) les effets de la montée en température dus, par exemple, à une (des) anomalie(s) aléatoire(s) du matériel, doivent être pris en compte de manière à éviter une ou des défaillances de cause commune. Au moins une des mesures énumérées dans le Tableau E.2, n°6 doit être appliquée. Des mesures appropriées doivent être prises dans le cas d'une conception pour laquelle une anomalie locale peut générer une montée en température critique pour la sécurité.

"les effets de la montée en température dus, par exemple, à une (des) anomalie(s) aléatoire(s) du matériel, doivent être pris en compte de manière à éviter une ou des défaillances de cause commune."

– restructuration pour éviter toute ambiguïté

"pour éviter une ou des défaillances de cause commune, les effets de la montée en température dus, par exemple, à une (des) anomalie(s) aléatoire(s) du matériel, doivent être pris en compte."

NOTE 2 Alors que dans la conception d'un circuit d'alimentation, une anomalie locale peut générer une montée en température importante, l'impact d'un court-circuit local dans un circuit logique peut être négligeable. Les

exemples à prendre en considération dans les circuits numériques incluent la surface tampon du dispositif et les régulateurs de tension.

d) la création de blocs physiques distincts sur le substrat du circuit intégré pour chaque canal et chaque élément de contrôle tel qu'un chien de garde. Les blocs doivent comporter des fils de connexion et des broches de sortie. Chaque canal doit comporter ses propres entrées et sorties séparées qui ne doivent pas être acheminées via un autre canal/bloc;

NOTE 3 Ceci n'exclut pas les connexions internes entre les blocs par un câblage entre les cellules de sortie et d'entrée des différents blocs (voir également Tableau E.1, 3a et 3b).

NOTE 4 Les entrées et les sorties incluent, sans toutefois s'y limiter:

– Les signaux DFT (Conception pour Testabilité, par exemple, chaînes de balayage);
– Les signaux d'horloge et les signaux d'activation d'horloge;
– L'alimentation;
– Les signaux de remise à zéro
– Les signaux de configuration et de sélection de mode;
– Les signaux de mise au point et d'analyse.

e) des mesures appropriées doivent être prises pour éviter toute défaillance dangereuse due à des anomalies de l'alimentation, y compris les défaillances de cause commune;

NOTE 5 Les anomalies de l'alimentation incluent, sans toutefois s'y limiter:

– le bruit;
– la propagation des perturbations sur les lignes d'alimentation;
– la mise sous tension non simultanée de l'alimentation; par exemple pour éviter les effets tels que le verrouillage ou un courant d'appel élevé;
– un appel de courant excessif généré par un court-circuit.

NOTE 6 Cette exigence peut être satisfaite en appliquant des techniques appropriées telles que:

– fournir à chaque bloc ses propres broches d'alimentation de sorte qu'aucun bloc ne soit alimenté par la source d'alimentation d'un autre bloc (par exemple par l'intermédiaire de connexions internes) et ne pas connecter de puits de différents blocs à l'intérieur du circuit intégré (voir également Tableau E.2, n° 3).
– Il convient de prendre des mesures externes pour éviter toute défaillance dangereuse pouvant être générée par des tensions différentes des puits;
– détecter les anomalies d'alimentation au moyen des unités de contrôle de tension;
– utiliser partiellement une tolérance de tension plus élevée;
– tenir compte des problèmes de chute ohmique pour la conception des lignes d'alimentation.

f) la distance minimale entre les limites de différents blocs physiques doit être suffisante pour éviter tout court-circuit et toute interférence entre ces blocs;

NOTE 7 Un court-circuit peut typiquement être provoqué par une électro-migration, par migration, une migration par contact, un défaut local, une rupture par oxyde de grille, un verrouillage, etc.

NOTE 8 Une interférence peut typiquement être provoquée par des courants à substrat, un couplage capacitif, etc.

NOTE 9 Il convient de choisir la distance minimale en tenant compte des règles de conception appropriées avec un facteur de sécurité généralement compris entre 10 et 50.

NOTE 10 Les anneaux de potentiels conformes au Tableau E.2 ne sont pas considérés comme faisant partie intégrante d'un bloc lorsqu'il s'agit d'estimer la distance entre des blocs différents.

g) un court-circuit et/ou une interférence au niveau des lignes adjacentes de différents blocs ne doivent pas entraîner la perte d'une fonction de sécurité ou la perte non détectée d'une fonction de surveillance (Tableau E.2, n° 5);

h) le substrat doit être relié à la terre indépendamment du processus de conception du circuit intégré utilisé (puits-n ou puits-p);

NOTE 11 Pour les puits-p, cela signifie le recours à une alimentation négative. Il convient d'éviter toute logique négative dans la mesure où son utilisation peut être sensible aux erreurs de conception.

i) la sensibilité d'un circuit intégré avec redondance sur la puce aux défaillances de cause commune doit être estimée en déterminant un facteur β conformément à E.3. Ce facteur,

appelé $\beta_{IC,}$ doit être utilisé pour estimer l'intégrité de sécurité obtenue du système E/E/PE relatif à la sécurité conformément à 7.4.5.1, et sera par ailleurs utilisé pour le circuit intégré en lieu et place du facteur β déterminé par exemple conformément à l'Annexe D de la CEI 61508-6;

j) la détection d'une anomalie (par les essais de diagnostic, les essais périodiques ou tout autre moyen) dans un circuit intégré avec redondance sur la puce doit déclencher une action spécifiée pour obtenir ou maintenir un état de sécurité;

NOTE 12 Cette exigence ne s'applique pas si les effets d'une anomalie peuvent être maîtrisés, par exemple par la désactivation d'un bloc.

k) la couverture de diagnostic minimale de chaque canal doit être au moins de 60 %; Lorsqu'un élément de contrôle est mis en œuvre une seule fois, la couverture de diagnostic minimale applicable à cet élément doit également être au moins égale à 60 %;

l) s'il se révèle nécessaire de mettre en œuvre un chien de garde, par exemple pour la surveillance de la séquence de programme et/ou pour garantir la couverture de diagnostic requise ou une proportion de défaillances en sécurité, un canal ne doit pas servir de chien de garde d'un autre canal, sauf dans le cas de l'utilisation de différents canaux fonctionnels;

m) avec l'essai portant sur la compatibilité électromagnétique sans marge de sécurité supplémentaire, la fonction exécutée par le circuit intégré ne doit pas être altérée (par exemple critère de performance A) tel que décrit dans les normes d'immunité CEM, voir par exemple la CEI 61000-6-2 ou la CEI 61326-3-1);

n) avec l'essai portant sur la compatibilité électromagnétique avec marges de sécurité supplémentaires, la fonction de sécurité (y compris les circuits intégrés) doit satisfaire au critère "FS" défini dans la CEI 61326-3-1;

o) des mesures appropriées doivent être prises pour éviter toute défaillance dangereuse provoquée par des oscillations des ports à entrée numérique reliés à des signaux numériques asynchrones externes, par exemple, introduction de plusieurs étapes de synchronisation d'horloge respectives.

p) Le potentiel de cause commune des ressources communes telles que les circuits du type "registre à décalage périphérique" et les réseaux de registres de fonctions spéciales doit être analysé.

q) Les exigences a) à p) énumèrent les initiateurs de cause commune spécifiques aux circuits intégrés avec redondance sur la puce. Les autres initiateurs de cause commune pertinents doivent être pris en considération comme spécifié dans la présente norme internationale.

NOTE 13 En général, les exigences susmentionnées réduisent l'utilisation de la redondance sur la puce aux circuits intégrés personnalisés ou semi-personnalisés tels que les ASIC, microcontrôleurs ou autres systèmes avec redondance sur la puce spécialisés. Il est possible que d'autres conceptions telles que les matrices prédiffusées, les matrices prédiffusées programmables, etc., ne permettent pas de satisfaire à toutes ces exigences.

L'utilisation de circuits intégrés avec redondance sur la puce comme décrit ci-dessus doit être admise uniquement si une analyse de cause commune (CCA) complète a été effectuée. Cette analyse doit couvrir la gamme complète de défaillances potentielles de cause commune dues aux facteurs liés à la conception, fabrication, construction, procédure et à l'environnement. Plus particulièrement, la perte de séparation physique entre les canaux suite à l'utilisation de circuits intégrés avec redondance sur la puce doit être soumise à un examen particulier. Le niveau SIL final alloué au système E/E/PE relatif à la sécurité doit dépendre des résultats de l'analyse de cause commune.

NOTE 14 L'utilisation de la séparation physique (c'est-à-dire la ségrégation) des "canaux" peut assurer une protection contre un grand nombre de défaillances de cause commune dans les systèmes redondants.

NOTE 15 La méthodologie CCA proposée est structurée selon les étapes suivantes:

1. Identifier les initiateurs de cause commune (CCI) potentiels. Tenir compte des effets cités dans la présente annexe et des autres initiateurs de cause commune physiques et logiques prévisibles (partage des ressources et des signaux).

2. Identifier les blocs redondants du circuit intégré qui subissent les effets des initiateurs de cause commune.

3. Enumérer et évaluer de manière qualitative les mesures de sécurité prises contre les initiateurs de cause commune individuels identifiés à l'étape 1 pour chaque paire de blocs redondants identifiés à l'étape 2.
4. Compléter de manière quantitative (réponse) les Tableaux E.1 et E.2 pour chaque paire de blocs redondants identifiés à l'étape 2 et évaluer le facteur ß spécifique.
5. Utiliser les facteurs ß spécifiques dans la modélisation probabiliste.

E.2 Exigences supplémentaires relatives à la redondance sur la puce de SIL 3

Pour la redondance sur la puce de SIL 3, les exigences suivantes doivent être satisfaites outre les exigences indiquées en E.1:

a) une preuve documentée doit être fournie, attestant que toutes les conditions environnementales spécifiques à l'application sont conformes aux conditions prises en compte lors de la spécification, analyse, vérification et validation;
b) les mesures externes pouvant obtenir ou maintenir un état de sécurité du système E/E/PE; ces mesures doivent définir l'efficacité moyenne (voir également A.3) comme critère minimal. Toutes les mesures mises en œuvre à l'intérieur du circuit intégré pour maîtriser les effets de défaillances systématiques et/ou de cause commune doivent utiliser ces mesures externes pour obtenir ou maintenir un état de sécurité du système E/E/PE.

E.3 Facteur β

La sensibilité du circuit intégré avec redondance sur la puce aux défaillances de cause commune doit être estimée en déterminant le facteur β, β_{IC}, spécifique aux circuits intégrés avec redondance sur la puce (voir également E.1, i)). L'estimation doit être basée sur les éléments suivants:

a) un facteur β de base appelé $\beta_{B\text{-}IC,}$ d'une valeur de 33 %;
b) l'estimation de l'augmentation du facteur β de base, $\beta_{B\text{-}IC,}$ par la conception, en utilisant le Tableau E.1; et
c) l'estimation de la diminution du facteur β de base, $\beta_{B\text{-}IC}$, par la conception, en utilisant le Tableau E.2.

Le facteur β_{IC} est estimé en ajoutant le facteur $\beta_{B\text{-}IC}$ et tous les résultats du Tableau E.1, puis en soustrayant tous les résultats du Tableau E.2. Le facteur β_{IC} final estimé ne doit pas excéder 25 %.

NOTE 1 Ce facteur β appelé β_{IC} est utilisé pour l'estimation de l'intégrité de sécurité obtenue du système E/E/PE relatif à la sécurité selon 7.4.5.1 et est également utilisé pour le circuit intégré en lieu et place du facteur β déterminé, par exemple, selon l'Annexe D de la CEI 61508-6.

NOTE 2 Il convient d'effectuer une analyse spécifique des données de défaillance disponibles pour la méthodologie de conception appliquée, afin de corroborer le caractère prudent du facteur β choisi. Il convient d'utiliser uniquement les circuits intégrés à conception et processus de mise en œuvre évolués.

Tableau E.1 – Techniques et mesures d'accroissement du facteur $\beta_{B\text{-}IC}$

	Technique/mesure	Facteur β delta [%]	Remarque
1	Chien de garde sur puce, utilisé comme élément de contrôle	5	Il convient de constituer les éléments de contrôle, utilisés pour la fonction de chien de garde et nécessaires pour garantir la DC ou la SFF requise, à l'extérieur du circuit intégré, de préférence sous la forme de défaillances de cause commune. L'utilisation d'un ou de plusieurs chiens de garde sur puce peut entraîner une DC ou une SFF plus élevée par comparaison à une constitution externe. Voir également E.2 b).
2	Eléments de contrôle sur puce autres qu'un chien de garde, par exemple contrôle d'horloge	5	Il convient de constituer les éléments de contrôle, utilisés par exemple pour le contrôle d'horloge et nécessaires pour garantir la DC ou la SFF requise, à l'extérieur du circuit intégré, de préférence sous la forme de défaillances de cause commune. L'utilisation d'un ou de plusieurs éléments de contrôle peut entraîner une DC ou une SFF plus élevée par comparaison à une constitution externe.
3a	Connexions internes entre les blocs par câblage entre les cellules de sortie et d'entrée de différents blocs sans aire en recouvrement	2	Il convient de procéder à la comparaison des conditions et des résultats entre les différents blocs, de préférence à l'extérieur du circuit intégré. Il doit être procédé à l'analyse des défaillances de cause commune potentielles, incluant une AMDE des collages des connexions internes. Les effets de la montée en température due à des anomalies doivent plus particulièrement être pris en compte. Il convient d'effectuer une vérification de la topologie par une analyse de la topologie finale, par exemple, à l'aide d'outils.
3b	Connexions internes entre les blocs par câblage entre les cellules de sortie et d'entrée de différents blocs avec aire en recouvrement	4	Il convient de procéder à la comparaison des conditions et des résultats entre les différents blocs, de préférence à l'extérieur du circuit intégré. Il doit être procédé à l'analyse des défaillances de cause commune potentielles, incluant une AMDE des collages et du court-circuit des connexions internes. Les effets de la montée en température due à des anomalies doivent plus particulièrement être pris en compte.

Une lettre suivant le numéro désigne des techniques/mesures alternatives. Seule une des techniques/mesures alternatives peut être choisie.

Les techniques et mesures énumérées dans ce tableau ne sont pas exhaustives. D'autres techniques et mesures peuvent être utilisées, sous réserve qu'une preuve soit fournie pour appuyer le facteur β delta déclaré.

S'il peut être attesté, par une preuve, que des mesures ont été prises pour réduire l'impact des défaillances de cause commune, d'autres facteurs β delta peuvent être utilisés. Dans ce cas, il convient d'observer les recommandations générales données dans l'Annexe D de la CEI 61508-6.

NOTE Les signaux d'interface entre les blocs redondants comportent généralement plusieurs couches. Quelle que soit la composition d'un signal, et que ce dernier comporte uniquement une seule couche métallique ou qu'il soit constitué de plusieurs couches, *le signal d'interface entier sera considéré comme un seul fil*. Il convient, pour réduire au minimum toute interférence des deux canaux par une anomalie, qu'aucun signal d'interface ne « chevauche » le reste des signaux d'interface.

Tableau E.2 – Techniques et mesures de diminution du facteur $\beta_{B\text{-}IC}$

	Technique/mesure	Facteur β delta [%]	Remarque
1a	Mesures diverses de maîtrise des défaillances dans différents canaux	4	
1b	Diversité de fonction et mesures de maîtrise des défaillances dans différents canaux	6	
2	Non interférence des essais portant sur la vérification de la compatibilité électromagnétique du système E/E/PE avec marge de sécurité supplémentaire, sur la fonction de ce système (par exemple critère de performance A)	5	Le critère de performance A est décrit dans les normes d'immunité CEM, voir par exemple CEI 61000-6-2 ou CEI 61326-3-1.
3	Fournir à chaque bloc ses propres broches d'alimentation de sorte qu'aucun bloc ne soit alimenté par la source d'alimentation d'un autre bloc (par exemple par l'intermédiaire de connexions internes) et ne pas connecter de puits de différents blocs à l'intérieur du circuit intégré	6	Des mesures externes doivent être prises pour éviter toute défaillance dangereuse pouvant être générée par des tensions différentes des puits.
4	Structures d'isolement et de découplage des sites physiques	2 - 4	Utile pour le découplage de différents blocs.
5	Contact à la masse entre le brochage de sortie de différents blocs	2	En l'absence de cette mise en œuvre, il doit être procédé à un court-circuit entre les lignes adjacentes de différents blocs pour soumettre à l'essai les effets de détachement du câblage de connexion (voir également E.1, g). Le facteur β n'est pas réduit dans ce cas.
6a	Couverture de diagnostic élevée (DC ≥ 99 %) de chaque canal, détection de défaillance(s) par le processus technique et réalisation de l'état de sécurité en un temps restreint approprié	7	Peut convenir uniquement dans un cas exceptionnel.
6b	Sondes de température entre les blocs avec arrêt permanent (interne ou externe) à l'état de sécurité en un temps restreint approprié; faible efficacité sans diagnostic	2	Voir également Tableau A.18, mesures contre la montée en température.
6c	Sondes de température entre les blocs avec arrêt permanent (interne ou externe) à l'état de sécurité en un temps restreint approprié; efficacité élevée avec diagnostic	9	Voir également Tableau A.18, mesures contre la montée en température.
6d	Analyse/essai des effets des anomalies (par exemple montée en température). Selon le résultat de l'analyse/essai, une comparaison entre les canaux, y compris la détection des anomalies et la réalisation de l'état de sécurité en un temps restreint approprié, peut se révéler nécessaire	9	
6e	Conception du circuit de surveillance fonctionnel à la température plus élevée	7	La conception de la fonction de surveillance (par exemple, chien de garde) doit exécuter la fonction de sécurité dans les conditions de température les plus défavorables.

Une lettre suivant le numéro désigne des techniques/mesures alternatives. Seule une des techniques / mesures alternatives peut être choisie.

Les techniques et mesures énumérées dans ce tableau ne sont pas exhaustives. D'autres techniques et mesures peuvent être utilisées, sous réserve qu'une preuve soit fournie pour appuyer le facteur β delta déclaré.

NOTE Les techniques/mesures 6a à 6e ont pour objectif de maîtriser les effets de la montée en température due à une défaillance.

Annexe F
(informative)

Techniques et mesures pour les ASIC – évitement des défaillances systématiques

F.1 Généralités

Il convient, pour la conception des ASIC, d'appliquer les techniques et mesures suivantes permettant d'éviter les défaillances lors du développement de ces circuits.

NOTE 1 La présente annexe informative est référencée par 7.4.6.7.

NOTE 2 Les techniques et mesures suivantes sont associées uniquement aux ASIC numériques et aux circuits intégrés programmables par l'utilisateur. Aucune technique ou mesure générale ne peut être actuellement spécifiée pour les ASIC à mode mixte et analogique.

a) Il convient de documenter toutes les activités de conception et les dispositifs d'essai, ainsi que les outils utilisés pour la simulation fonctionnelle et les résultats de cette dernière.

b) Il convient d'éprouver tous les outils, bibliothèques et procédures de production par une utilisation antérieure. Ceci inclut:

- l'application de l'outil (y compris différentes versions avec caractéristiques équivalentes) sur une période importante, avec des projets de complexité similaire ou de plus grande complexité;

NOTE 3 Une période importante pourrait correspondre à une durée de 2 ans dans ce cas.

- l'application d'outils communs ou d'utilisation courante afin d'assurer que les informations concernant les erreurs et les restrictions potentielles sont identifiées pour l'outil donné et/ou la version fournie, qu'il convient de prendre en considération au cours de l'utilisation. Il convient que les fabricants effectuent le contrôle et la surveillance afin de repérer les anomalies existantes;
- la réalisation de contrôles de cohérence et de plausibilité de manière à éviter les anomalies dans les différentes bases de données créées par différents outils.

NOTE 4 La formation des utilisateurs constitue un élément très important du fait des changements et de l'évolution rapides dans ce domaine.

c) Il convient de vérifier toutes les activités et leurs résultats, par exemple par simulation, contrôles d'équivalence, analyse de durée ou vérification des contraintes d'ordre technologique.

d) Il convient d'appliquer les mesures de reproductibilité et d'automatisation du processus de mise en œuvre des nouveaux systèmes (travail automatisé basé sur des scripts et flux de mise en œuvre des nouveaux systèmes).

e) Pour les fonctions matérielles ou logicielles fournies par une tierce partie, il convient d'utiliser uniquement les macro-blocs validés, ces derniers satisfaisant généralement à toutes les contraintes et toutes les procédures définies par le fournisseur de macro-blocs si la pratique le permet. Il convient, sauf démonstration préalable en utilisation, de traiter chaque macro-bloc comme un code nouvellement écrit. Il convient, par exemple, de le valider en intégralité.

f) Il convient, pour la conception, d'utiliser une méthodologie de conception et un langage de description d'études utilitaires et évolués.

NOTE 5 Il convient que la description d'études utilise un langage de description de circuit tel que VHDL ou Verilog. Il s'agit des méthodologies de description de circuit les plus usuelles utilisées actuellement dans la conception des ASIC. Les deux langages sont définis par des normes IEEE et sont réputés satisfaire aux recommandations applicables aux langages de programmation évolués. Le langage de description de circuit peut être utilisé à la fois pour la description d'études et pour les modèles fonctionnels ou les bancs d'essai. Dans le cas de la description d'études, seul un sous-ensemble du langage peut être utilisé; ce code synthétisable est souvent

désigné comme code RTL (transfert au niveau des registres). Le code non synthétisable, convenant aux modèles fonctionnels et aux bancs d'essai, est appelé code comportemental.

g) Il convient d'obtenir une testabilité aux essais appropriée (pour l'essai de production de l'ASIC et semi-personnalisé).

h) Il convient de prendre en considération les temps de propagation et d'interconnexion au cours de l'essai et des étapes de vérification des ASIC.

i) Il convient d'éviter les portes internes avec circuits de sortie à trois états. Lorsque les circuits de sortie à trois états internes sont utilisés, il convient qu'ils soient équipés de résistances de polarisation à l'alimentation/la masse ou de bus-holders.

j) Il convient, avant production, d'effectuer une vérification appropriée de l'ASIC complet (c'est-à-dire comprenant chaque étape de vérification achevée lors de la conception et de la mise en œuvre afin d'assurer une fonctionnalité correcte du module et de la puce).

NOTE 6 Le caractère approprié de la vérification de l'ASIC dépend de la complexité de l'essai de l'élément et du niveau d'intégrité de sécurité requis.

F.2 Lignes directrices: Techniques et mesures

Il convient d'utiliser un ensemble approprié de techniques et de mesures essentielles pour éviter l'introduction d'anomalies pendant la conception et le développement des ASIC. Il est nécessaire, selon la réalisation technique, de différencier les circuits intégrés numériques spécifiques et semi-personnalisés des circuits intégrés programmables par l'utilisateur (FPGA/PLD/CPLD). Les techniques et mesures contribuant à la réalisation des propriétés appropriées sont définies dans le Tableau F.1 pour les ASIC spécifiques et semi-personnalisés et dans le Tableau F.2 pour les circuits intégrés programmables par l'utilisateur. Le cycle de vie de développement des ASIC associé est illustré à la Figure 3.

Les Tableaux F.1 et F2 donnent des recommandations par niveau d'intégrité de sécurité en indiquant, en premier lieu, l'importance de la technique ou de la mesure et, en second lieu, l'efficacité requise si cette technique ou mesure est utilisée. L'importance est décrite de la manière suivante:

– HR*: la technique ou mesure est vivement recommandée pour ce niveau d'intégrité de sécurité. Il convient qu'aucune conception n'exclut cette technique ou cette mesure;

– HR: la technique ou mesure est vivement recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure n'est pas utilisée, il convient alors de décrire de manière détaillée les motifs sous-jacents;

– R: la technique ou mesure est recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure n'est pas utilisée, ou si aucune des alternatives potentielles n'est utilisée, il convient alors de décrire de manière détaillée les motifs sous-jacents;

– -: la technique ou mesure ne porte aucune recommandation pour ou contre son utilisation;

– NR: la technique ou mesure n'est absolument pas recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure est utilisée, il convient alors de décrire de manière détaillée les motifs sous-jacents;

L'efficacité recommandée est décrite de la manière suivante:

– Faible: si elle est utilisée, il convient que la technique ou mesure soit appliquée dans la mesure nécessaire pour garantir au moins une faible efficacité contre les défaillances systématiques;

– Moyenne: si elle est utilisée, il convient que la technique ou mesure soit appliquée dans la mesure nécessaire pour garantir au moins une efficacité moyenne contre les défaillances systématiques;

– Elevée: Il convient que la technique ou mesure soit appliquée dans la mesure nécessaire pour garantir une efficacité élevée contre les défaillances systématiques.

Le fait de se conformer aux recommandations de la présente annexe ne garantit pas en soi l'intégrité de sécurité requise. Il est important de tenir compte des éléments suivants:

– la cohérence des techniques et mesures choisies ainsi que la manière dont elles se complètent;

– les techniques et mesures qui conviennent à chaque phase du cycle de vie de développement; et

– les techniques et mesures qui sont les mieux adaptées aux problèmes spécifiques rencontrés au cours du développement de chaque système E/E/PE relatif à la sécurité différent.

Tableau F.1 – Techniques et mesures pour éviter l'introduction d'anomalies lors de la conception et du développement des ASIC – circuits intégrés numériques spécifiques et semi-personnalisés (voir 7.4.6.7)

Phase de conception	Réf.	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
Elément d'entrée de conception	1	Description structurée	E.3	HR élevée	HR élevée	HR* élevée	HR* élevée
	2	Description de conception en (V)HDL (voir Note)	E.1	HR élevée	HR élevée	HR* élevée	HR* élevée
	3	Entrée schématique	E.2	NR	NR	NR	NR
	4	Simulation (V)HDL (voir Note)	E.5	HR élevée	HR élevée	HR* élevée	HR* élevée
	5	Application de simulateurs (V)HDL éprouvés par une utilisation antérieure (voir Note)	E.4	HR élevée	HR élevée	HR* élevée	HR* élevée
	6	Essai fonctionnel au niveau du module (en utilisant par exemple les bancs d'essai (V)HDL) (voir Note)	E.6	HR élevée	HR élevée	HR* élevée	HR* élevée
	7	Essai fonctionnel au niveau supérieur	E.7	HR élevée	HR élevée	HR* élevée	HR* élevée
	8	Essai fonctionnel intégré dans l'environnement système	E.8	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	9	Utilisation restreinte des constructions asynchrones	E.9	HR élevée	HR élevée	HR* élevée	HR* élevée
	10	Synchronisation des entrées préliminaires et contrôle de la métastabilité	E.10	HR élevée	HR élevée	HR* élevée	HR* élevée
	11	Conception pour testabilité (selon la couverture d'essai en pourcentage)	E.11	R ≥95 %	R ≥98 %	R ≥99 %	R ≥99 %
	12	Modularisation	E.12	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	13	Couverture des scénarios de vérification	E.13	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	14	Observation des recommandations de codage	E.14	HR élevée	HR élevée	HR* élevée	HR* élevée
	15	Application du système de vérification du code	E.15	R	R	R	R

Tableau F.1 *(suite)*

Phase de conception	Réf.	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	16	Programmation défensive	E.16	R faible	R moyenne	HR élevée	HR* élevée
	17	Documentation des résultats de simulation	E.17	HR faible	HR moyenne	HR élevée	HR* élevée
	18a	Inspection de code	E.18	R moyen-ne	R élevée	HR élevée	HR* élevée
	18b	Lecture croisée (sondage)	E.19	R moyen-ne	R élevée	HR élevée	HR* élevée
	19a	Application de fonctions logicielles validées	E.20	R moyen-ne	R élevée	HR* élevée	HR* élevée
	19b	Validation des fonctions logicielles	E.21	R moyen-ne	R élevée	HR* élevée	HR* élevée
Synthèse	20a	Simulation de la liste d'interconnexions des portes, afin de vérifier les contraintes de synchronisation	E.22	R moyen-ne	R moyen-ne	R élevée	R élevée
	20b	Analyse statique du temps de propagation (STA)	E.23	R moyen-ne	R moyen-ne	R élevée	R élevée
	21a	Vérification de la liste d'interconnexions des portes par rapport à un modèle de référence par simulation	E.24	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	21b	Comparaison de la liste d'interconnexions des portes avec le modèle de référence (contrôle d'équivalence formel)	E.25	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	22	Vérification des exigences et des contraintes des fournisseurs des ASIC	E.26	HR élevée	HR élevée	HR* élevée	HR* élevée
	23	Documentation des contraintes, résultats et outils de synthèse	E.27	HR élevée	HR élevée	HR* élevée	HR* élevée
	24	Application d'outils de synthèse éprouvés par une utilisation antérieure	E.28	HR* élevée	HR* élevée	HR* élevée	HR* élevée
	25	Application de bibliothèques cibles éprouvées par une utilisation antérieure	E.29	HR* élevée	HR* élevée	HR* élevée	HR* élevée
	26	Procédures à base de scripts	E.30	R moyen-ne	R moyen-ne	HR élevée	HR élevée
Intégration d'essai et génération de vecteurs d'essai	27	Mise en œuvre des structures d'essai	E.31	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	28a	Estimation de la couverture d'essai par simulation (sur la base de la couverture d'essai obtenue en pourcentage)	E.32	R > 95 %	R > 98 %	R > 99 %	R > 99 %

Tableau F.1 *(suite)*

Phase de conception	Réf.	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	28b	Estimation de la couverture d'essai par application de l'outil ATPG (sur la base de la couverture d'essai obtenue en pourcentage)	E.33	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	29a	Simulation de la liste d'interconnexions des portes, afin de vérifier les contraintes de synchronisation	E.22	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	29b	Analyse statique du temps de propagation (STA)	E.23	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	30a	Vérification de la liste d'interconnexions des portes par rapport à un modèle de référence par simulation	E.24	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	30b	Comparaison de la liste d'interconnexions des portes avec le modèle de référence (contrôle d'équivalence formel)	E.25	R moyen-ne	R moyen-ne	HR élevée	HR élevée
Placement, routage, génération de la topologie	31a	Justification des fonctions matérielles appliquées éprouvées par une utilisation antérieure	E.34	HR élevée	HR élevée	HR* élevée	HR* élevée
	31b	Application de fonctions matérielles validées	E.35	HR élevée	HR élevée	HR* élevée	HR* élevée
	31c	Essais en ligne des fonctions matérielles	E.36	HR élevée	HR élevée	HR* élevée	HR* élevée
	32a	Simulation de la liste d'interconnexions des portes, afin de vérifier les contraintes de synchronisation	E.22	HR élevée	HR élevée	HR* élevée	HR* élevée
	32b	Analyse statique du temps de propagation (STA)	E.23	HR élevée	HR élevée	HR* élevée	HR* élevée
	33a	Vérification de la liste d'interconnexions des portes par rapport à un modèle de référence par simulation	E.24	HR élevée	HR élevée	HR* élevée	HR* élevée
	33b	Comparaison de la liste d'interconnexions des portes avec le modèle de référence (contrôle d'équivalence formel)	E.25	HR élevée	HR élevée	HR* élevée	HR* élevée
	34	Vérification des règles de conception (DRC pour Design Rules Check)	E.37	HR élevée	HR élevée	HR élevée	HR* élevée
	35	Vérification de la topologie par rapport au schéma (LVS pour Layout Versus Schematic)	E.38	HR élevée	HR élevée	HR élevée	HR* élevée
	36	Application d'environnements de conception éprouvés par une utilisation antérieure, application de bibliothèques de cellules éprouvées par une utilisation antérieure	E.4	HR* élevée	HR* élevée	HR* élevée	HR* élevée
	37	Marge supplémentaire (> 20 %) pour les technologies de système appliquées depuis moins de 3 ans	E.39	HR élevée	HR élevée	HR élevée	HR* élevée

Tableau F.1 *(suite)*

Phase de conception	Réf.	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
Fabrication des puces	38	Application d'une technologie de système éprouvée par une utilisation antérieure		HR élevée	HR élevée	HR* élevée	HR* élevée
	39	Processus de fabrication de puces éprouvé	E.42	HR faible	HR moyen-ne	HR élevée	HR* élevée
	40	Assurance qualité pour la technologie de système		HR élevée	HR élevée	HR élevée	HR* élevée
	41	Contrôle qualité du processus de fabrication	E.43	HR élevée	HR élevée	HR élevée	HR* élevée
	42	Certificat de qualité de fabrication du dispositif	E.44	R faible	R moyen-ne	HR élevée	HR* élevée
	43	Certificat de qualité fonctionnelle du dispositif	E.45	HR élevée	HR élevée	HR* élevée	HR* élevée
	44	Couverture de l'essai de production		≥95 %	≥98 %	≥99 %	≥ 99 %
	45	Normes de qualité	E.46	HR faible	HR moyen-ne	HR élevée	HR* élevée
	46	Management de la qualité, par exemple conformément à l'ISO 9000		HR élevée	HR élevée	HR élevée	HR* élevée
	47	Essai de déverminage	E.40	R faible	R moyen-ne	HR élevée	HR* élevée

Il convient de choisir les techniques/mesures appropriées selon le niveau d'intégrité de sécurité. Une lettre suivant le numéro désigne des techniques/mesures alternatives ou équivalentes. Il convient d'appliquer au moins une des techniques/mesures alternatives ou équivalentes.

NOTE Le terme (V)HDL désigne soit le langage (VHDL) soit le langage Verilog.

Tableau F.2 – Techniques et mesures pour éviter l'introduction d'anomalies lors de la conception et du développement des ASIC: Circuits intégrés programmables par l'utilisateur (FPGA/PLD/CPLD) (voir 7.4.6.7)

Phase de conception	Réf.	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
Elément d'entrée de conception	1	Description structurée	E.3	HR élevée	HR élevée	HR* élevée	HR* élevée
	2	Description de conception en (V)HDL (voir Note)	E.1	HR élevée	HR* élevée	HR* élevée	HR* élevée
	3	Entrée schématique	E.2	– élevée	– élevée	NR	NR
	4	Description d'études à l'aide des équations booléennes		R élevée	R élevée	NR	NR
	5a	Pour les descriptions de circuits qui utilisent les équations booléennes: inspection manuelle pour les conceptions de complexité limitée (faible)		HR élevée	HR élevée	HR* élevée	HR* élevée
	5b	Pour les descriptions de circuits qui utilisent les équations booléennes: simulation de transitions d'états avec des conceptions de complexité plus importante		HR élevée	HR élevée	HR* élevée	HR* élevée
	6	Application d'un environnement de conception éprouvé	E.4	HR élevée	HR élevée	HR* élevée	HR* élevée
	7	Application de simulateurs (V)HDL éprouvés par une utilisation antérieure (voir Note)	E.4	HR élevée	HR élevée	HR* élevée	HR* élevée
	8	Essai fonctionnel sur niveau de module (en utilisant par exemple les bancs d'essai (V)HDL) (voir Note)	E.6	HR élevée	HR élevée	HR* élevée	HR* élevée
	9	Utilisation restreinte des constructions asynchrones	E.9	HR élevée	HR élevée	HR* élevée	HR* élevée
	10	Conception pour testabilité (selon la couverture d'essai en pourcentage)	E.11	R > 95 %	R > 98 %	R > 99 %	R > 99 %
	11	Modularisation	E.12	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	12	Couverture des scénarios de vérification (bancs d'essai)	E.13	R moyenn e	R moyenn e	HR élevée	HR élevée
	13	Observation des recommandations de codage	E.14	HR élevée	HR élevée	HR* élevée	HR* élevée
	14	Documentation des résultats de simulation	E.17	HR faible	HR moyen-ne	HR élevée	HR* élevée
	15	Inspection de code	E.18	R moyen-ne	R élevée	HR élevée	HR* élevée
	15b	Lecture croisée (sondage)	E.19	R moyen-ne	R élevée	HR élevée	HR* élevée
	16a	Application de fonctions logicielles validées	E.20	R moyen-ne	R élevée	HR élevée	HR* élevée
	16b	Validation des fonctions logicielles	E.21	R moyen-ne	R élevée	HR* élevée	HR* élevée

Tableau F.2 *(suite)*

Phase de conception	Réf.	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
Synthèse	17	Vérifications de cohérence interne (voir par exemple CEI 61508-7, E.4)		HR élevée	HR élevée	HR* élevée	HR* élevée
	18a	Simulation de la liste d'interconnexions des portes, afin de vérifier les contraintes de synchronisation	E.22	R moyen-ne	R moyen-ne	R élevée	R élevée
	18b	Analyse statique du temps de propagation (STA)	E.23	R moyen-ne	R moyen-ne	R élevée	R élevée
	19a	Vérification de la liste d'interconnexions des portes par rapport à un modèle de référence par simulation	E.24	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	19b	Comparaison de la liste d'interconnexions des portes avec le modèle de référence (contrôle d'équivalence formel)	E.25	R moyen-ne	R moyen-ne	HR élevée	HR élevée
	20	Pour les PLD/CPLD avec des conceptions complexes: vérification de la conception par simulation		R moyen-ne	R moyen-ne	HR élevée	HR élevée
	21	Vérification des exigences et des contraintes des fournisseurs des circuits intégrés	E.26	HR élevée	HR élevée	HR* élevée	HR* élevée
	22	Documentation des contraintes, résultats et outils de synthèse	E.27	HR élevée	HR élevée	HR* élevée	HR* élevée
	23	Application d'outils de synthèse éprouvés par une utilisation antérieure	E.28	HR élevée	HR élevée	HR* élevée	HR* élevée
	24	Application de bibliothèques / technologies CPLD éprouvées par une utilisation antérieure	E.29	HR élevée	HR élevée	HR* élevée	HR* élevée
	25	Procédure à base de scripts	E.30	R élevée	R élevée	HR élevée	HR* élevée
Placement, routage, génération de la topologie	26a	Justification des fonctions matérielles appliquées et éprouvées par une utilisation antérieure	E.34	HR élevée	HR élevée	HR* élevée	HR* élevée
	26b	Application de fonctions matérielles validées	E.35	HR élevée	HR élevée	HR* élevée	HR* élevée
	26c	Essais en ligne des fonctions matérielles validées	E.36	HR élevée	HR élevée	HR* élevée	HR* élevée
	27a	Simulation de la liste d'interconnexions des portes, afin de vérifier les contraintes de synchronisation	E.22	HR élevée	HR élevée	HR* élevée	HR* élevée
	27b	Analyse statique du temps de propagation (STA)	E.23	HR élevée	HR élevée	HR* élevée	HR* élevée
	28a	Vérification de la liste d'interconnexions des portes par rapport à un modèle de référence par simulation	E.24	HR élevée	HR élevée	HR* élevée	HR* élevée
	28b	Comparaison de la liste d'interconnexions des portes avec le modèle de référence (contrôle d'équivalence formel)	E.25	HR élevée	HR élevée	HR* élevée	HR* élevée

Tableau F.2 *(suite)*

Phase de conception	Réf.	Technique/mesure	Voir CEI 61508-7	SIL1	SIL2	SIL3	SIL4
	29	Vérification des règles de conception (DRC)	E.37	HR élevée	HR élevée	HR élevée	HR* élevée
	30	Application d'environnements de conception éprouvés par une utilisation antérieure, application de bibliothèques de cellules éprouvées par une utilisation antérieure	E.4	HR* élevée	HR* élevée	HR* élevée	HR* élevée
	31	Marge supplémentaire (> 20 %) pour les technologies de système appliquées depuis moins de 3 ans	E.39	HR élevée	HR élevée	HR* élevée	HR* élevée
Production	32	Application d'une technologie de système éprouvée par une utilisation antérieure		HR élevée	HR élevée	HR* élevée	HR* élevée
	33	Application de séries de dispositifs éprouvés par une utilisation antérieure	E.41	HR élevée	HR élevée	HR* élevée	HR* élevée
	34	Processus de fabrication éprouvé	E.42	HR faible	HR moyen-ne	HR élevée	HR* élevée
	35	Contrôle qualité du processus de fabrication	E.43	HR élevée	HR élevée	HR élevée	HR* élevée
	36	Certificat de qualité de fabrication du composant	E.44	R faible	R moyen-ne	HR élevée	HR* élevée
	37	Certificat de qualité fonctionnelle du composant	E.45	HR élevée	HR élevée	HR* élevée	HR* élevée
	38	Normes de qualité	E.46	HR faible	HR moyen-ne	HR élevée	HR* élevée
	39	Management de la qualité, par exemple conformément à l'ISO 9000		HR élevée	HR élevée	HR élevée	HR* élevée
	40	Vérification et validation finales du prototype FPGA/PLD dans le système		HR élevée	HR élevée	HR* élevée	HR* élevée
	41	Vérification et validation finales lors de la production en série, vérification linéique		R élevée	R élevée	HR* élevée	HR* élevée
	42	Essai de déverminage	E.40	R faible	R faible	R moyen-ne	HR* élevée

Il convient de choisir les techniques/mesures appropriées selon le niveau d'intégrité de sécurité. Une lettre suivant le numéro désigne des techniques/mesures alternatives ou équivalentes. Il convient d'appliquer au moins une des techniques/mesures alternatives ou équivalentes.

NOTE Le terme (V)HDL désigne soit le langage (VHDL) soit le langage Verilog.

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 61508-5 : 2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

[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 60601 (toutes les parties), *Appareils électromédicaux*

[7] CEI 61165, *Application des techniques de Markov*

[8] CEI 61078, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

[9] CEI 61164, *Reliability growth – Statistical test and estimation methods* (disponible en anglais seulement)

[10] CEI 62308, *Fiabilité de l'équipement – Méthodes d'évaluation de la fiabilité*

[11] CEI 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

[12] ISO 14224, *Industries du pétrole, de la pétrochimie et du gaz naturel – Recueil et échange de données de fiabilité et de maintenance des équipements*

[13] CEI 60050-191, *Vocabulaire Electrotechnique International – Chapitre 191:Sûreté de fonctionnement et qualité de service*

[14] ISO 9000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

[15] CEI 60300-3-2, *Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

[16] IEEE 352:1987, *IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems* (disponible en anglais seulement)

———————

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