IEC 61508-2

Edition 1.0 2000-05

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: Prescriptions 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 It also gives information on projects, withdrawn and replaced publications.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 1.0 2000-05

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: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XB
CODE PRIX

ICS 25.040.40

ISBN 2-8318-5195-5

CONTENTS

Page

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 IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The 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 and control.

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/294/FDIS	65A/303/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 3.

Annexes A, B, and C form an integral part of this standard.

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

– Part 1: General requirements
– Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
– Part 3: Software requirements
– Part 4: Definitions and abbreviations
– Part 5: Examples of methods for the determination of safety integrity levels
– Part 6: Guidelines on the application of parts 2 and 3
– Part 7: Overview of techniques and measures

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

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

INTRODUCTION

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

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

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

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

This International Standard

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

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

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

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

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

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

1 Scope

1.1 This part of IEC 61508

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, which contains at least one electrical, electronic or programmable electronic based component;

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

d) specifies how to refine the information developed in accordance with IEC 61508-1, concerning the overall safety requirements and their allocation to E/E/PE safety-related systems, and specifies how the overall safety requirements are refined into E/E/PES safety functions requirements and E/E/PES safety integrity requirements;

e) specifies 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/PES safety lifecycle model), except for software, which is dealt with by IEC 61508-3 (see figures 2 and 3) – these requirements include the application of techniques and measures, which 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 3.

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 3.4.4 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 is also intended for use as a stand-alone standard.

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 1 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.

NOTE 2 In the USA and Canada, until the proposed sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA-S84.01) can be applied to the process sector instead of IEC 61508.

1.3 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 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.

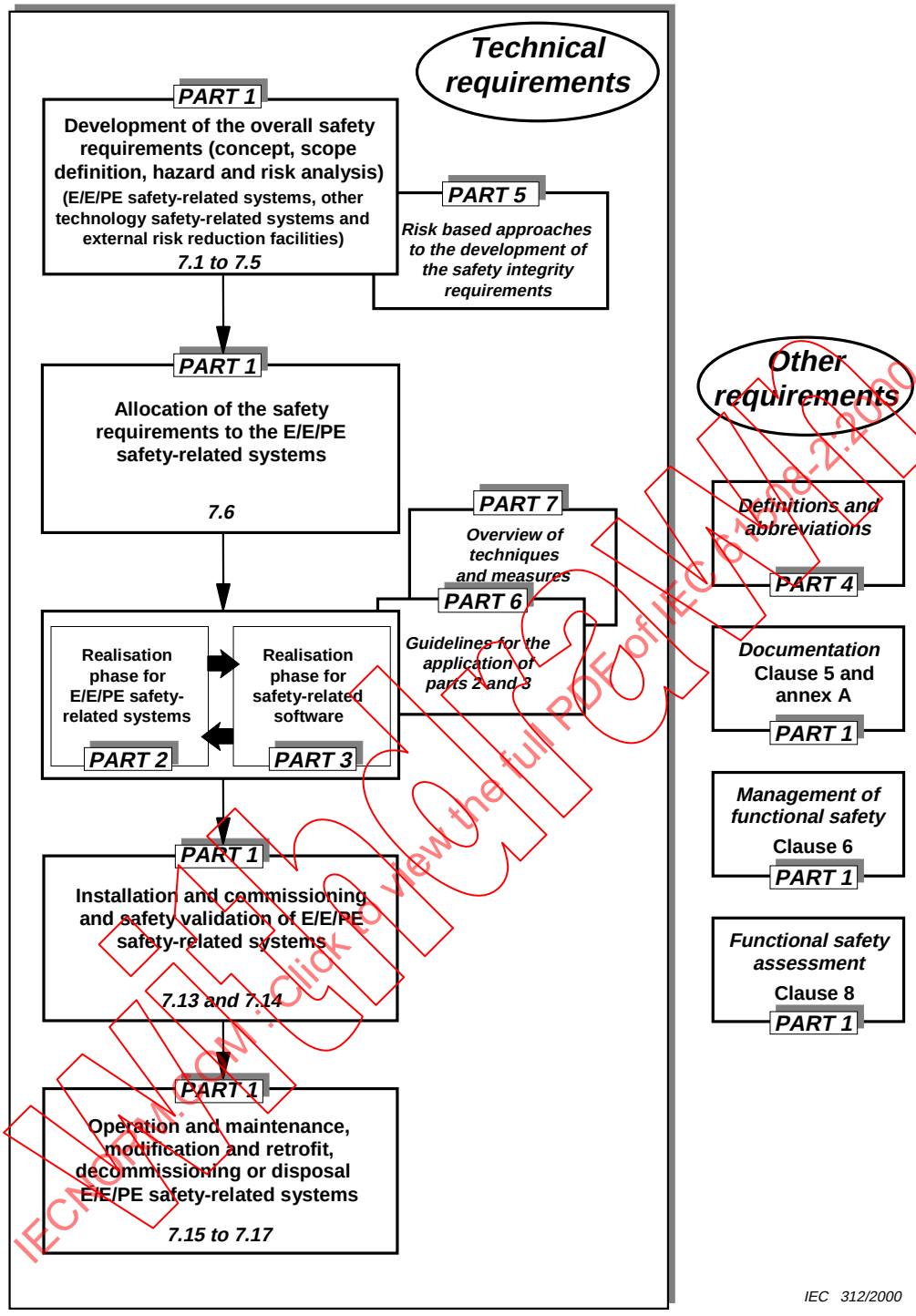


Figure 1 – Overall framework of IEC 61508

2 Normative references

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

IEC 60050(371):1984, *International Electrotechnical Vocabulary – Chapter 371: Telecontrol*

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

IEC 61000-1-1:1992, *Electromagnetic compatibility (EMC) – Part 1: General – Section 1: Application and interpretation of fundamental definitions and terms*

IEC 61000-2-5:1995, *Electromagnetic compatibility (EMC) – Part 2: Environment – Section 5: Classification of electromagnetic environments – Basic EMC publication*

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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

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

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

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

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

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

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

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

1) To be published.

3 Definitions and abbreviations

For the purposes of this part of IEC 61508, 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/PES 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/PES 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/PES 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/PES 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/PES safety lifecycle.

7.1.3 Requirements

7.1.3.1 The E/E/PES safety lifecycle that shall be used in claiming conformance with this standard is that specified in figure 2. If another E/E/PES safety lifecycle is used, it shall be specified during functional safety planning (see clause 6 of IEC 61508-1), and all the objectives and requirements of each subclause of IEC 61508-2 shall be met.

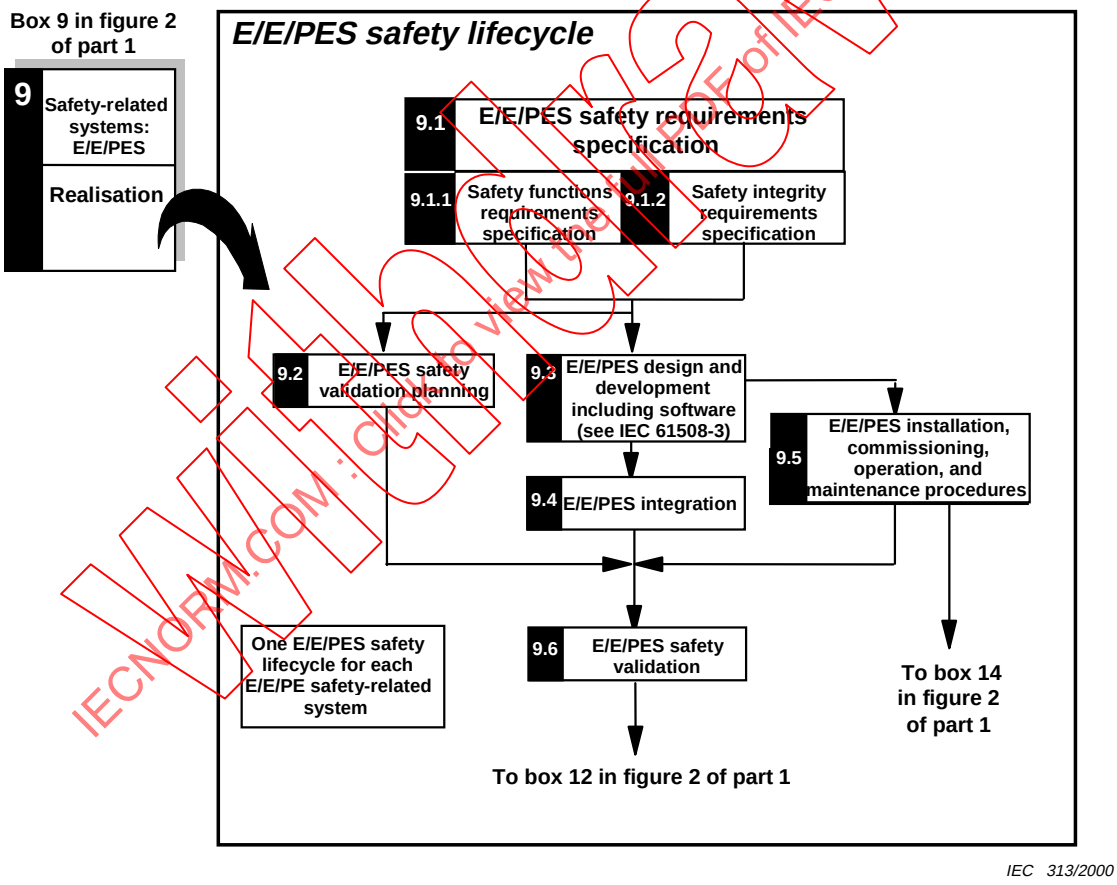
NOTE The relationship and scope for IEC 61508-2 and IEC 61508-3 are shown in figure 3.

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/PES safety lifecycle phases.

7.1.3.3 Each phase of the E/E/PES 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 during functional safety planning, the outputs of each phase of the E/E/PES safety lifecycle shall be documented (see clause 5 of IEC 61508-1).

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



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

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

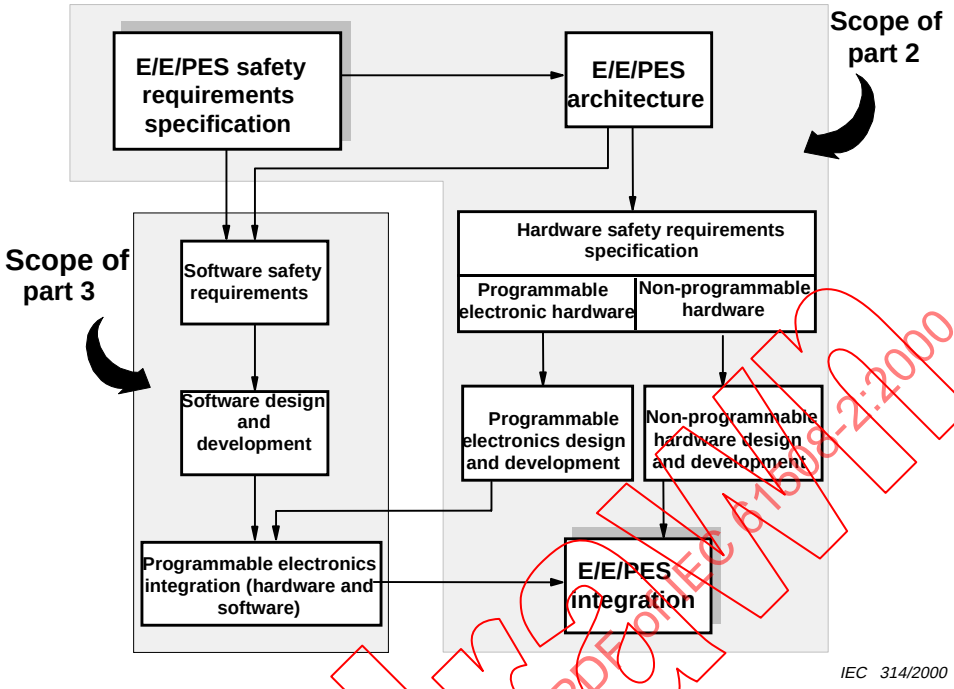


Figure 3 – Relationship and scope for IEC 61508-2 and IEC 61508-3

Table 1 – Overview – Realisation phase of the E/E/PES safety lifecycle

Safety lifecycle phase or activity		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	Title					
9.1	E/E/PES safety requirements specification	To specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety	E/E/PE safety-related systems	7.2.2	Description of allocation of safety requirements (see 7.6 of IEC 61508-1)	E/E/PES safety requirements Requirements for software safety as an input to the software safety requirements specification
9.2	E/E/PES safety validation lanning	To plan the validation of the safety of the E/E/PE safety-related systems	E/E/PE safety-related systems	7.3.2	E/E/PES safety requirements	Plan for the safety validation of the E/E/PE safety-related systems
9.3	E/E/PES design and development	To design the E/E/PE safety-related systems to meet the requirements for safety functions and safety integrity	E/E/PE safety-related systems	7.4.2 to 7.4.9	E/E/PES safety requirements	Design of the E/E/PE safety related systems in conformance with the E/E/PES safety requirements Plan for the E/E/PES integration test PES architectural information as an input to the software requirements specification
9.4	E/E/PES integration	To integrate and test the E/E/PE safety-related systems	E/E/PE safety-related systems	7.5.2	E/E/PES design E/E/PES integration test plan Programmable electronics hardware and software	Fully functioning E/E/PE safety-related systems in conformance with the E/E/PES design Results of E/E/PES integration tests
9.5	E/E/PES installation, commission in, operation, and maintenance procedures	To develop procedures to ensure that the functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance	E/E/PE safety-related systems EUC	7.6.2	E/E/PES safety requirements E/E/PES design	E/E/PES installation, commissioning, operation and maintenance procedures for each individual E/E/PES
9.6	E/E/PES safety validation	To validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the required safety integrity	E/E/PE safety-related systems	7.7.2	E/E/PES safety requirements 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/PES safety validation
–	E/E/PES modification	To make corrections, enhancements or adaptations to the E/E/PE safety-related systems, ensuring that the required safety integrity level is achieved and maintained	E/E/PE safety-related systems	7.8.2	E/E/PES safety requirements	Results of E/E/PES modification
–	E/E/PES 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 systems	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/PES functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems	E/E/PE safety-related systems	8	Plan for E/E/PES functional safety assessment	Results of E/E/PES functional safety assessment

7.2 E/E/PES safety requirements specification

NOTE This phase is box 9.1 of figure 2.

7.2.1 Objective

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

NOTE The safety functions may, for example, be required to put the EUC into a safe state or to maintain a safe state.

7.2.2 General requirements

7.2.2.1 The specification of the E/E/PES safety requirements shall be derived from the allocation of safety requirements, specified in 7.6 of IEC 61508-1, and from those requirements specified during functional safety planning (see clause 6 of IEC 61508-1). This information shall be made available to the E/E/PES developer.

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).

7.2.2.2 The E/E/PES safety requirements shall be expressed and structured in such a way that they are

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

b) written to aid comprehension by those who are likely to utilise the information at any stage of the E/E/PES safety lifecycle.

7.2.2.3 The specification of the E/E/PES safety requirements shall contain the requirements for the E/E/PES safety functions (see 7.2.3.1) and the requirements for E/E/PES safety integrity (see 7.2.3.2).

7.2.3 E/E/PES safety requirements

7.2.3.1 The E/E/PES safety functions requirements specification shall contain

a) a description of all the safety functions necessary to achieve the required functional safety, which shall, for each safety function,
   - provide comprehensive detailed requirements sufficient for the design and development of the E/E/PE safety-related systems,
   - include the manner in which the E/E/PE safety-related systems are intended to achieve or maintain a safe state for the EUC,
   - specify whether or not continuous control is required, and for what periods, in achieving or maintaining a safe state of the EUC, and
   - specify whether the safety function is applicable to E/E/PE safety-related systems operating in low demand or high demand/continuous modes of operation;

b) throughput and response time performance;

c) E/E/PE safety-related system and operator interfaces which are necessary to achieve the required functional safety;

d) all information relevant to functional safety which may have an influence on the E/E/PE safety-related system design;

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

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

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

NOTE 1 Reasonably foreseeable abnormal conditions are those reasonably foreseeable to either the developers or users.

NOTE 2 Additional safety functions may be required for particular modes of operation (for example setting, adjustment or maintenance), to enable these operations to be carried out safely.

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

h) the significance of all hardware/software interactions – where relevant, any required constraints between the hardware and the software shall be identified and documented;

NOTE 3 Where these interactions are not known before finishing the design, only general constraints can be stated.

i) limiting and constraint conditions for the E/E/PE safety-related systems and their associated subsystems, for example timing constraints;

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

7.2.3.2 The E/E/PES safety integrity requirements specification shall contain

a) the safety integrity level for each safety function and, when required (see note 2), the required target failure measure for the safety function;

NOTE 1 The safety integrity level of a safety function determines the target failure measure for the safety function according to IEC 61508-1, tables 2 and 3.

NOTE 2 The target failure measure of a safety function will need to be specified when the required risk reduction for the safety function has been derived using a quantitative method (see IEC 61508-1, 7.5.2.2).

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

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

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

e) the electromagnetic immunity limits (see IEC 61000-1-1) which are required to achieve electromagnetic compatibility – the electromagnetic immunity limits should be derived taking into account both the electromagnetic environment (see IEC 61000-2-5) and the required safety integrity levels;

NOTE 1 It is important to recognise that the safety integrity level is a factor in determining electromagnetic immunity limits, especially since the level of electromagnetic disturbance in the environment is subject to a statistical distribution. In most practical situations, it is not possible to specify an absolute level of disturbance, only a level which it is expected will not be exceeded in practice (this is the electromagnetic compatibility level). Unfortunately, practical difficulties make the probability associated with this expectation very hard to define. Therefore, the immunity limit does not guarantee that the E/E/PE safety-related system will not fail due to electromagnetic disturbances, it only provides some level of confidence that such a failure will not occur. The actual level of confidence achieved is a function of the immunity limit in relation to the statistical distribution of the disturbance levels in the operating environment. For higher safety integrity levels it may be necessary to have a higher level of confidence, which means that the margin by which the immunity limit exceeds the compatibility level should be greater for higher safety integrity levels.

NOTE 2 Also, guidance may be found in EMC product standards, but it is important to recognise that higher immunity levels than those specified in such standards may be necessary for particular locations or when the equipment is intended for use in harsher electromagnetic environments.

NOTE 3 In developing the E/E/PES safety requirements specification, the application in which the E/E/PE safety-related systems are to be used should be taken into consideration. This is particularly important for maintenance, where the specified proof test interval should not be less than can be reasonably expected for the particular application. For example, the time between services that can be realistically attained for mass-produced items used by the public is likely to be greater than in a more controlled application.

7.2.3.3 For the avoidance of mistakes during the specification of the E/E/PES safety requirements, an appropriate group of techniques and measures according to table B.1 shall be used.

7.3 E/E/PES safety validation planning

NOTE This phase is box 9.2 of figure 2. It will normally be carried out in parallel with E/E/PES 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 systems.

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 systems satisfy the E/E/PES safety requirements specification (see 7.2).

NOTE See IEC 61508-3 for the validation plan for the software.

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

a) all of the requirements defined in the E/E/PES safety 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 immunity test limits is given in IEC 61000-2-5 and IEC 61000-4.

g) policies for resolving validation failure.

7.4 E/E/PES design and development

NOTE This phase is box 9.3 of figure 2. It will normally be carried out in parallel with E/E/PES safety validation planning (see 7.3).

7.4.1 Objective

The objective of the requirements of this subclause is to ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and 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/PES safety requirements specification (see 7.2), taking into account all the requirements of 7.4.

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, embedded software, application software, etc.), see figure 4, shall be such as to meet all of the requirements a) to c) as follows:

a) the requirements for hardware safety integrity comprising
   - the architectural constraints on hardware safety integrity (see 7.4.3.1), and
   - the requirements for the probability of dangerous random hardware failures (see 7.4.3.2);

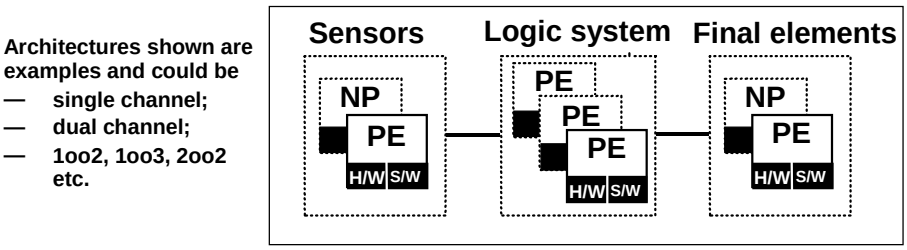
b) the requirements for systematic safety integrity comprising
   - the requirements for the avoidance of failures (see 7.4.4), and the requirements for the control of systematic faults (see 7.4.5), or
   - evidence that the equipment is "proven in use" (see 7.4.7.6 to 7.4.7.12);

c) the requirements for system behaviour on detection of a fault (see 7.4.6).

NOTE 1 Overall E/E/PES safety integrity framework: the overall method for selecting a design approach to demonstrate achievement of a safety integrity level (for both hardware and systematic safety integrity) in E/E/PE safety-related systems is as follows:

- determine the required safety integrity level (SIL) of the safety functions (see IEC 61508-1 and IEC 61508-5);
- set: hardware safety integrity = systematic safety integrity = SIL (see 7.4.3.2.1);
- for hardware safety integrity, determine the architecture to meet the architectural constraints (see 7.4.3.1) and demonstrate that the probabilities of failure of the safety functions due to random hardware failures meet the required target failure measures (see 7.4.3.2);
- for systematic safety integrity, select design features that control (tolerate) systematic faults in actual operation (see 7.4.5) or confirm that the 'proven-in-use' requirements have been met (see 7.4.7.6 to 7.4.7.12); and
- for systematic safety integrity, select techniques and measures that avoid (prevent the introduction of) systematic faults during design and development (see 7.4.4) or confirm that the 'proven-in-use' requirements have been met (see 7.4.7.6 to 7.4.7.12).

NOTE 2 IEC 61508-3 contains the requirements for the software architecture (see 7.4.2.2); the requirements to produce a programmable electronics and software integration test specification (see 7.5); and the requirements to integrate the programmable electronics and software according to that specification (see 7.5). In all cases, close co-operation between the developer of the E/E/PE safety-related systems and the software developer will be necessary.



Programmable electronics architecture		
PE hardware architecture	**PE software architecture** (s/w architecture consists of embedded s/w and applications s/w)	
	PE embedded software	**PE applications software**
Generic and application specific features in PE hardware. Examples include — **diagnostic tests;** — **redundant processors;** — **dual I/O cards.**	**Examples include** — **communications drivers;** — **fault handling;** — **executive software.**	**Examples include** — **input/output functions;** — **derived functions (for example sensor checking if not provided as a service of the embedded software).**

IEC 315/2000

Key

PE programmable electronics
NP non-programmable devices
H/W hardware
S/W software
MooN M out of N (for example 1oo2 is 1 out of 2)

Figure 4 – Relationship between the hardware and software architectures of programmable electronics

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). Wherever practicable, the safety-related functions should be separated from the non-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/PES 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.

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/PES 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/PES 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 which 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/PES 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 7.4.7).

NOTE 1 A subsystem may be considered to comprise a single component or any group of components. 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 7.4.7.3.

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 functionality, capacity and performance on to the new requirement or the verified subsystem 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 is overly complicated or has unused features and if protection against unintended functions cannot be obtained.

7.4.2.12 Where a subsystem has multiple outputs then it is necessary to determine whether some combination of output states, which may be caused by a failure of the E/E/PE safety-related system, can directly cause a hazardous event (as determined by the hazard and risk analysis, see IEC 61508-1, 7.4.2.10). Where this has been established, then the prevention of that combination of output states shall be regarded as a safety function operating in the high demand/continuous mode of operation (see 7.4.6.3 and 7.4.3.2.5).

7.4.2.13 De-rating (see IEC 61508-7, A.2.8) shall be used as far as possible for all components. Justification for operating any components at their limits shall be documented (see IEC 61508-1, clause 5).

NOTE Where de-rating is appropriate, a de-rating factor of at least 0,67 should be used.

7.4.3 Requirements for hardware safety integrity

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.

7.4.3.1 Architectural constraints on hardware safety integrity

7.4.3.1.1 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 fault tolerance and safe failure fraction of the subsystems that carry out that safety function (see annex C). Tables 2 and 3 specify the highest safety integrity level that can be claimed for a safety function which uses a subsystem taking into account the hardware fault tolerance and safe failure fraction of that subsystem (see annex C). The requirements of tables 2 and 3 shall be applied to each subsystem carrying out a safety function and hence every part of the E/E/PE safety-related system; 7.4.3.1.2 to 7.4.3.1.4 specify which one of tables 2 and 3 apply to any particular subsystem. Subclauses 7.4.3.1.5 and 7.4.3.1.6 specify how the highest safety integrity level that can be claimed for a safety function is derived. With respect to these requirements,

a) a hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function. 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) in determining hardware fault tolerance, 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 3);

d) the safe failure fraction of a subsystem is defined as the ratio of the average rate of safe failures plus dangerous detected failures of the subsystem to the total average failure rate of the subsystem (see annex C).

NOTE 1 The architectural constraints have been included in order to achieve a sufficiently robust architecture, taking into account the level of subsystem complexity. The hardware safety integrity level for the E/E/PE safety-related system, derived through applying these requirements, is the maximum that is permitted to be claimed even though, in some cases, a higher safety integrity level could theoretically be derived if a solely mathematical approach had been adopted for the E/E/PE safety-related system.

NOTE 2 The architecture and subsystem derived to meet the hardware fault tolerance requirements is that used under normal operating conditions. The 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 must have been previously evaluated (for example mean time to restoration compared to the probability of a demand).

NOTE 3 This is necessary because if a component 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 which uses the component.

7.4.3.1.2 A subsystem (see 7.4.2.11, note 1) 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 subsystem under fault conditions can be completely determined; and

c) there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.7.3 and 7.4.7.4).

7.4.3.1.3 A subsystem (see 7.4.2.11, note 1) 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 subsystem under fault conditions cannot be completely determined; or

c) there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.7.3 and 7.4.7.4).

NOTE This means that if at least one of the components of a subsystem itself satisfies the conditions for a type B subsystem then that subsystem must be regarded as type B rather than type A. See also 7.4.2.11, note 1.

7.4.3.1.4 The architectural constraints of either table 2 or table 3 shall apply to each subsystem carrying out a safety function, so that

a) the hardware fault tolerance requirements shall be achieved for the whole of the E/E/PE safety-related system;

b) table 2 applies for every type A subsystem forming part of the E/E/PE safety-related systems;

NOTE 1 If the E/E/PE safety-related system contains only type A subsystems then the requirements in table 2 will apply to the entire E/E/PE safety-related system.

c) table 3 applies for every type B subsystem forming part of the E/E/PE safety-related systems;

NOTE 2 If the E/E/PE safety-related system contains only type B subsystems then the requirements in table 3 will apply to the entire E/E/PE safety-related system.

d) both tables 2 and 3 will be applicable to E/E/PE safety-related systems comprising both type A and type B subsystems, since the requirements in table 2 shall apply for the type A subsystems and the requirements in table 3 shall apply for the type B subsystems.

Table 2 – Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % – < 90 %	SIL2	SIL3	SIL4
90 % – < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.			
NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.			
NOTE 3 See annex C for details of how to calculate safe failure fraction.			

Table 3 – Hardware safety integrity: architectural constraints on type B safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.			
NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.			
NOTE 3 See annex C for details of how to calculate safe failure fraction.			

7.4.3.1.5 In E/E/PE safety-related systems where a safety function is implemented through a single channel (such as in figure 5), the maximum hardware safety integrity level that can be claimed for the safety function under consideration shall be determined by the subsystem that has met the lowest hardware safety integrity level requirements (determined by consideration of tables 2 and 3).

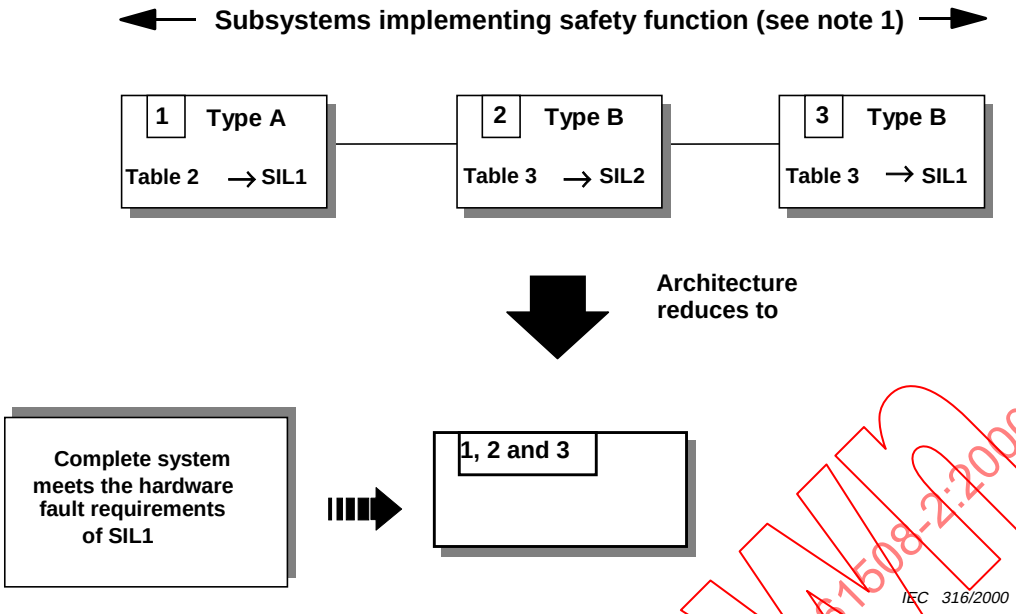
EXAMPLE Assume an architecture in which a particular safety function is performed by a single channel of subsystems 1, 2 and 3 as in figure 5 and the subsystems meet the requirements of tables 2 and 3 as follows:

– subsystem 1 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL1;

– subsystem 2 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

– subsystem 3 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL1.

For this particular architecture, subsystems 1 and 3 are each only able to achieve the hardware fault tolerance requirements of SIL1, while subsystem 2 is able to achieve the hardware fault tolerance requirements of SIL2. Therefore, both subsystem 1 and subsystem 3 restrict the hardware safety integrity level that can be claimed, in respect of the hardware fault tolerance, for the safety function under consideration, to just SIL1.



NOTE 1 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.

NOTE 2 For details on interpreting this figure, see the example to 7.4.3.1.5.

Figure 5 – Example limitation on hardware safety integrity for a single-channel safety function

7.4.3.1.6 In E/E/PE safety-related systems where a safety function is implemented through multiple channels of subsystems (such as in figure 6), the maximum hardware safety integrity level that can be claimed for the safety function under consideration shall be determined by

a) assessing each subsystem against the requirements of table 2 or 3 (as specified in 7.4.3.1.2 to 7.4.3.1.4); and

b) grouping the subsystems into combinations; and

c) analysing those combinations to determine the overall hardware safety integrity level.

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 either a combination of subsystems 1, 2 and 3 or a combination of subsystems 4, 5 and 3, as in figure 6. In this case, the combination of subsystems 1 and 2 and the combination of subsystems 4 and 5 have the same functionality as regards the safety function, and provide separate inputs into subsystem 3. In this example, the combination of parallel subsystems is based on each subsystem implementing the required part of the safety function independent of the other (parallel) subsystem. The safety function will be performed

– in the event of a fault in either subsystem 1 or subsystem 2 (because the combination of subsystems 4 and 5 is able to perform the safety function); or

– in the event of a fault in either subsystem 4 or subsystem 5 (because the combination of subsystems 1 and 2 is able to perform the safety function).

Each subsystem meets the requirements of tables 2 and 3 as follows:

– subsystem 1 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL3;

– subsystem 2 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

– subsystem 3 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

– subsystem 4 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

– subsystem 5 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL1.

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

a) Combining subsystems 1 and 2: The hardware fault tolerance and safe failure fraction achieved by the combination of subsystems 1 and 2 (each separately meeting the requirements for SIL3 and SIL2 respectively) meets the requirements of SIL2 (determined by subsystem 2).

b) Combining subsystems 4 and 5: The hardware fault tolerance and safe failure fraction achieved by the combination of subsystems 4 and 5 (each separately meeting the requirements for SIL2 and SIL1 respectively) meets the requirements of SIL1 (determined by subsystem 5).

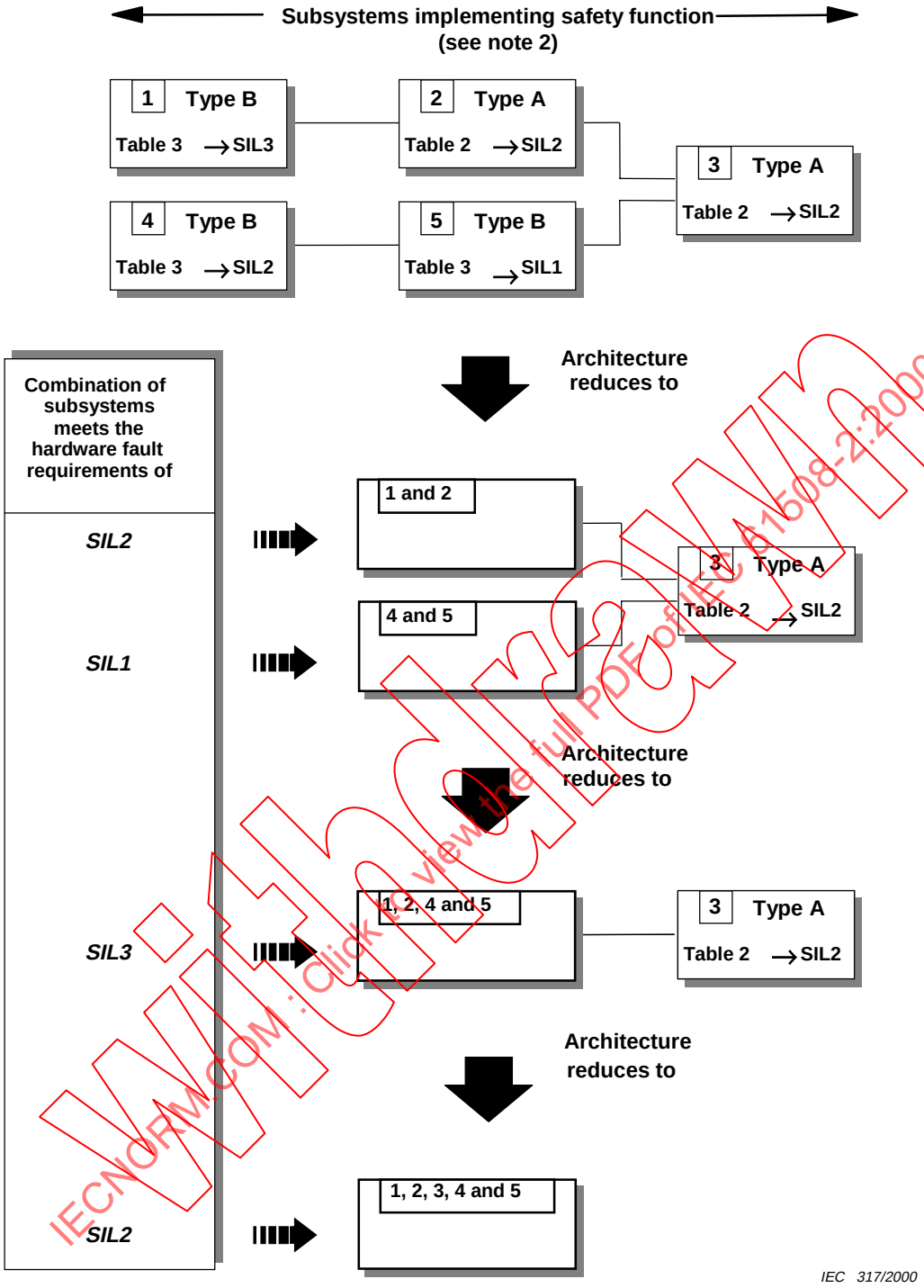
c) Further combining the combination of subsystems 1 and 2 with the combination of subsystems 4 and 5: The hardware safety integrity level, in respect of the hardware fault tolerance, of the combination of subsystems 1, 2, 4 and 5 is determined by

   – deciding which of the subsystem combinations (i.e. the combination of subsystems 1 and 2 or the combination of subsystems 4 and 5) has achieved the highest claimable hardware safety integrity level (in terms of meeting the hardware fault tolerance); and

   – analysing the effect the other subsystem combination has on the hardware fault tolerance for the combination of subsystems 1, 2, 4 and 5.

   In this example, the combination of subsystems 1 and 2 has a maximum allowable claim of SIL2 (see a) above) while the combination of subsystems 4 and 5 has a maximum allowable claim of SIL1 (see b) above). However, in the event of a fault occurring in the combination of subsystems 1 and 2, the safety function could be performed by the combination of subsystems 4 and 5. To take account of this effect, the hardware fault tolerance achieved by the combination of subsystems 1 and 2 is increased by 1. Increasing the hardware fault tolerance by 1 has the effect of increasing the hardware safety integrity level that can be claimed by 1 (see tables 2 and 3). Therefore, the combination of subsystems 1, 2, 4 and 5 has a maximum claimable hardware safety integrity level, with respect to the hardware fault tolerance and safe failure fraction, of SIL3 (i.e. the hardware safety integrity level achieved by the combination of subsystems 1 and 2 (which was SIL2) plus 1).

d) The complete E/E/PE safety-related system: The hardware safety integrity level, in respect of the hardware fault tolerance, that can be claimed for the safety function under consideration, is determined by analysing the combination of subsystems 1, 2, 4 and 5 (which achieved the fault tolerance requirements of SIL3 (see c)) and subsystem 3 (which achieved the fault tolerance requirements of SIL2). It is the subsystem that has achieved the lowest hardware safety integrity level requirements, in this case subsystem 3, which determines the maximum hardware safety integrity level for the complete E/E/PE safety-related system. Therefore, for this example, the maximum hardware safety integrity level, in respect of the hardware fault tolerance, that can be achieved for the safety function, is SIL2.



NOTE 1 Subsystems 1 and 2 and subsystems 4 and 5 have the same functionality as regards implementing the safety function, and provide separate inputs into subsystem 3.

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.

NOTE 3 For details on interpreting this figure, see the example to 7.4.3.1.6.

Figure 6 – Example limitation on hardware safety integrity for a multiple-channel safety function

7.4.3.2 Requirements for estimating the probability of failure of safety functions due to random hardware failures

7.4.3.2.1 The probability of failure of each safety function due to random hardware failures, estimated according to 7.4.3.2.2 and 7.4.3.2.3, shall be equal to or less than the target failure measure as specified in the safety requirements specification (see 7.2.3.2).

NOTE 1 In the case of a safety function operating in the low demand mode of operation, the target failure measure will be expressed in terms of the average probability of failure to perform its design function on demand, as determined by the safety integrity level of the safety function (see IEC 61508-1, table 2), unless there is a requirement in the E/E/PES safety integrity requirements specification (see 7.2.3.2) for the safety function to meet a specific target failure measure, rather than a specific SIL. For example, when a target failure measure of $1{,}5 \times 10^{-6}$ (probability of failure on demand) is specified in order to meet the required risk reduction, then the probability of failure on demand of the safety function due to random hardware failures will need to be equal to or less than $1{,}5 \times 10^{-6}$.

NOTE 2 In the case of a safety function operating in the high demand/continuous mode of operation, the target failure measure will be expressed in terms of the average probability of a dangerous failure per hour, as determined by the safety integrity level of the safety function (see IEC 61508-1, table 3), unless there is a requirement in the E/E/PES safety integrity requirements specification (see 7.2.3.2) for the safety function to meet a specific target failure measure, rather than a specific SIL. For example, when a target failure measure of $1{,}5 \times 10^{-6}$ (probability of failure of dangerous failure per hour) is specified in order to meet the required risk reduction, then the probability of failure of the safety function due to random hardware failures will need to be equal to or less than $1{,}5 \times 10^{-6}$ dangerous failures per hour.

NOTE 3 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 7.4.3.2.2) and compare the result to the target failure measure of the safety integrity requirement for the relevant safety function (see IEC 61508-1, tables 2 and 3).

7.4.3.2.2 The probability of failure of each safety function, due to random hardware failures shall be estimated taking into account

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

   NOTE 1 This involves deciding which failure modes 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. co-incident failures are necessary for the relevant safety function to fail).

b) the estimated rate of failure of each subsystem in any modes which would cause a dangerous failure of the E/E/PE safety-related system but which are detected by diagnostic tests (see 7.4.7.3 and 7.4.7.4);

c) the estimated rate of failure of each subsystem in any modes which would cause a dangerous failure of the E/E/PE safety-related system which are undetected by the diagnostic tests (see 7.4.7.3 and 7.4.7.4);

d) the susceptibility of the E/E/PE safety-related system to common cause failures (see notes 2 and 11);

   NOTE 2 For example, see IEC 61508-6, annex D.

e) the diagnostic coverage of the diagnostic tests (determined according to annex C) and the associated diagnostic test interval;

   NOTE 3 The diagnostic test interval and the subsequent time for repair together constitute the mean time for restoration which will be considered in the reliability model. Also, for E/E/PE safety-related systems operating in high demand or continuous mode of operation where any dangerous failure of a channel results in a dangerous failure of the E/E/PE safety-related system, the diagnostic test interval will need to be considered directly (i.e. in addition to the mean time to restoration) in the reliability model if it is not at least a magnitude less than the expected demand rate (see 7.4.3.2.5).

   NOTE 4 When establishing the diagnostic test interval, the intervals between all of the tests which contribute to the diagnostic coverage will need to be considered.

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

g) the repair times for detected failures;

NOTE 5 The repair time will constitute one part of the mean time to restoration (see IEV 191-13-08), which will also include the time taken to detect a failure and any time period during which repair is not possible (see IEC 61508-6, annex B for an example of how the mean time to restoration can be used to calculate the probability of failure). For situations where the repair can only be carried out during a specific period of time, for example while 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.

h) the probability of undetected failure of any data communication process (see note 11 and 7.4.8.1).

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

NOTE 7 IEC 61508-6, annex A, A.2 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 8 It is necessary to quantify separately for each safety function the reliability of the E/E/PE safety-related systems because different component failure modes will apply and the architecture of the E/E/PE safety-related systems (in terms of redundancy) may also vary.

NOTE 9 A number of modelling methods are available and the most appropriate method is a matter for the analyst and will depend on the circumstances. Available methods include:

– cause consequence analysis (see B.6.6.2 of IEC 61508-7);
– fault tree analysis (see B.6.6.5 of IEC 61508-7);
– Markov models (see C.6.4 of IEC 61508-7);
– reliability block diagrams (see C.6.5 of IEC 61508-7).

NOTE 10 The mean time to restoration (see IEV 191-13-08) which is considered in the reliability model will need to take into account the diagnostic test interval, the repair time and any other delays prior to restoration.

NOTE 11 Failures due to common cause effects and data communication processes may result from effects other than actual failures of hardware components (e.g. electromagnetic interference, decoding errors, etc). However, such failures are considered, for the purposes of this standard, as random hardware failures.

7.4.3.2.3 The diagnostic test interval of any subsystem having a hardware fault tolerance of more than zero shall be such as to enable the E/E/PE safety-related system to meet the requirement for the probability of random hardware failure (see 7.4.3.2.1).

7.4.3.2.4 The diagnostic test interval of any subsystem having a hardware fault tolerance of zero, on which a safety function is entirely dependent (see note 1), and which is only implementing safety function(s) operating in the low demand mode, shall be such as to enable the E/E/PE safety-related system to meet the requirement for the probability of random hardware failure (see 7.4.3.2.1).

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 When there is a possibility that some combination of output states of a subsystem can directly cause a hazardous event (as determined by the hazard and risk analysis, see IEC 61508-1, 7.4.2.10) and when the combination of output states in the presence of a fault in the subsystem cannot be determined (for example, in the case of Type B subsystems), then it will be necessary to regard the detection of dangerous faults in the subsystem as a safety function operating in the high demand/continuous mode and the requirements of 7.4.6.3 and 7.4.3.2.5 will apply.

7.4.3.2.5 The diagnostic test interval of any subsystem having a hardware fault tolerance of zero, on which a safety function is entirely dependent (see note 1), and which is implementing any safety function operating in the high/continuous mode (see note 2), shall be such that the sum of the diagnostic test interval and the time to perform the specified action (fault reaction) to achieve or maintain a safe state (see 7.2.3.1 g)) is less than the process safety time. The process safety time is defined as the period of time between a failure occurring in the EUC or the EUC control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed.

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 In the case of a subsystem implementing particular safety function where the ratio of the diagnostic test rate to the demand rate exceeds 100, then the subsystem can be treated as if it is implementing a safety function operating in the low demand mode (see 7.4.3.2.4), provided that the safety function is not preventing a combination of output states which could lead to a hazardous event (see note 3).

NOTE 3 If the safety function is to prevent a particular combination of output states which could directly cause a hazardous event, then it will always be necessary to regard such a safety function as operating in the high/continuous mode (see 7.4.2.12).

7.4.3.2.6 If, for a particular design, the target failure measure of the safety integrity requirement for the relevant safety function is not achieved then

– determine the critical components, subsystems and/or parameters;

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

– select and implement the applicable improvements;

– repeat the necessary steps to establish the new probability of a hardware failure.

7.4.4 Requirements for the avoidance of failures

NOTE Clauses 7.4.4.1 to 7.4.4.6 do not apply in the case of a subsystem which meets the requirements to be considered as "proven in use" (see 7.4.7.6 to 7.4.7.12).

7.4.4.1 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 of the E/E/PE safety-related system (see table B.2).

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

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

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

c) clear and precise documentation and communication of information;

d) verification and validation.

7.4.4.3 Maintenance requirements, to ensure the safety integrity of the E/E/PE safety-related systems is kept at the required level, shall be formalised at the design stage.

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

7.4.4.5 During the design, E/E/PES 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.

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

7.4.5 Requirements for the control of systematic faults

NOTE Clauses 7.4.5.1 to 7.4.5.3 do not apply in the case of a subsystem which meets the requirements to be considered as "proven in use" (see 7.4.7.6 to 7.4.7.12).

7.4.5.1 For controlling systematic faults, the E/E/PES 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.16);

b) environmental stresses, including electromagnetic disturbances (see table A.17);

c) mistakes made by the operator of the EUC (see table A.18);

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 7.4.8).

7.4.5.2 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.

7.4.5.3 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. The design of all interfaces 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.

7.4.6 Requirements for system behaviour on detection of a fault

7.4.6.1 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem which has a hardware fault tolerance of more than zero 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 time to restoration (MTTR) assumed in the calculation of the probability of random hardware failure (see 7.4.3.2.2), then a specified action shall take place to achieve or maintain a safe state (see note).

NOTE The specified action (fault reaction) required to achieve or maintain a safe state will be specified in the E/E/PES safety requirements (see 7.2.3.1). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC which relies, for risk reduction, on the faulty subsystem.

7.4.6.2 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 zero and on which a safety function is entirely dependent (see note 1) 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 time to restoration (MTTR) period assumed in the calculation of the probability of random hardware failure (see 7.4.3.2.2). During this time the continuing safety of the EUC shall be ensured by additional measures and constraints. The risk reduction provided by these measures and constraints shall be at least equal to the risk reduction 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/PES operation and maintenance procedures (see 7.6). If the repair is not undertaken within the specified mean time to restoration (MTTR), then a specified action shall be performed to achieve or maintain a safe state (see note 2).

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 The specified action (fault reaction) required to achieve or maintain a safe state will be specified in the E/E/PES safety requirements (see 7.2.3.1). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC which relies, for risk reduction, on the faulty subsystem.

7.4.6.3 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 zero, and on which a safety function is entirely dependent (see note 1) shall, in the case of a subsystem which is implementing any safety function(s) operating in the high/continuous demand mode (see notes 2, 3), result in a specified action to achieve or maintain a safe state (see note 3).

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 When there is a possibility that some combination of output states of a subsystem can directly cause a hazardous event (as determined by the hazard and risk analysis, (see 7.4.2.12)) and when the combination of output states in the presence of a fault in the subsystem cannot be determined (for example, in the case of Type B subsystems), then it will be necessary to regard the detection of dangerous faults in the subsystem as a safety function operating in the high demand/continuous mode and the requirements of 7.4.6.3 and 7.4.3.2.5 will apply.

NOTE 3 The specified action (fault reaction) required to achieve or maintain a safe state will be specified in the E/E/PES safety requirements (see 7.2.3.1). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC which relies, for risk reduction, on the faulty subsystem.

7.4.7 Requirements for E/E/PES implementation

7.4.7.1 The E/E/PE safety-related system shall be implemented according to the E/E/PES design.

7.4.7.2 All subsystems which are used by one or more safety functions shall be identified and documented as safety-related subsystems.

7.4.7.3 The following information shall be available for each safety-related subsystem (see also 7.4.7.4):

a) a functional specification of those functions and interfaces of the subsystem which can be used by safety functions;

b) the estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are detected by diagnostic tests (see 7.4.7.4);

c) the estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are undetected by diagnostic tests (see 7.4.7.4);

d) any limits on the environment of the subsystem which should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures;

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

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

g) the diagnostic coverage derived according to annex C (when required, see note 1)

h) the diagnostic test interval (when required, see note 1);

NOTE 1 Items g) and h) above relate to diagnostic tests which are internal to the subsystem. This information is only required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/E/PE safety-related system (see 7.4.3.2.2).

i) any additional information (for example repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics;

NOTE 2 Items b) to i) are needed to allow the probability of failure on demand, or the probability of failure per hour of the safety function to be estimated (see 7.4.3.2.2).

NOTE 3 Items b), c), g), h) and i) are only required as separate parameters for subsystems such as sensors and actuators which may be combined in redundant architectures to improve hardware safety integrity. For items such as logic solvers which will not themselves be combined in redundant architectures in the E/E/PE safety-related system, it is acceptable to specify performance in terms of probability of failure on demand, or probability of dangerous failure per hour taking into account items b), c), g), h) and i). For such items it will also be necessary to establish the proof test interval for failures which are undetected.

j) all information which is necessary to enable the derivation of the safe failure fraction (SFF) of the subsystem as applied in the E/E/PE safety-related system, determined according to annex C;

k) the hardware fault tolerance of the subsystem;

NOTE 4 Items j) and k) are needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints (see 7.4.3.1).

l) any limits on the application of the subsystem which should be observed in order to avoid systematic failures;

m) the highest safety integrity level that can be claimed for a safety function which uses the subsystem on the basis of

– measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software of the subsystem (see 7.4.4.1 and 7.4 of IEC 61508-3),

– the design features which make the subsystem tolerant against systematic faults (see 7.4.5.1);

NOTE 5 This is not required in the case of those subsystems which are considered to have been proven in use (see 7.4.7.5).

n) any information which is required to identify the hardware and software configuration of the subsystem in order to enable the configuration management of the E/E/PE safety-related system in accordance with IEC 61508-1, 6.2.1.

o) documentary evidence that the subsystem has been validated.

7.4.7.4 The estimated rates of failure, due to random hardware failures, for subsystems (see 7.4.7.3 b) and c)) can be determined either

a) by a failure modes and effects analysis of the design using component failure data from a recognised industry source,

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 IEEE 352. An equivalent term, significance level, is used in IEC 61164.

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 components 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 components' useful lifetimes. The useful lifetime is highly dependent on the component 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 components are operated near to their specification limits. Components with longer useful lifetimes tend to be considerably more expensive.

or

b) from experience of the previous use of the subsystem in a similar environment (see 7.4.7.9).

7.4.7.5 In the case of a subsystem which is regarded as proven in use (see 7.4.7.6), then information regarding the measures and techniques for the prevention and control of systematic faults (see 7.4.7.3 m)) is not required.

7.4.7.6 A previously developed subsystem shall only be regarded as proven in use when it has a clearly restricted functionality and when there is adequate documentary evidence which is based on the previous use of a specific configuration of the subsystem (during which time all failures have been formally recorded, see 7.4.7.10), and which takes into account any additional analysis or testing, as required (see 7.4.7.8). The documentary evidence shall demonstrate that the likelihood of any failure of the subsystem (due to random hardware and systematic faults) in the E/E/PE safety-related system is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

7.4.7.7 The documentary evidence required by 7.4.7.6 shall demonstrate that the previous conditions of use (see note) of the specific subsystem are the same as, or sufficiently close to, those which will be experienced by the subsystem in the E/E/PE safety-related system, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

NOTE The conditions of use (operational profile) include all the factors which may influence the likelihood of systematic faults in the hardware and software of the subsystem. For example, environment, modes of use, functions performed, configuration, interfaces to other systems, operating system, translator, human factors.

7.4.7.8 When there is any difference between the previous conditions of use and those which will be experienced in the E/E/PE safety-related system, then any such difference(s) shall be identified and there shall be an explicit demonstration, using a combination of appropriate analytical methods and testing, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

7.4.7.9 The documentary evidence required by 7.4.7.6 shall establish that the extent of previous use of the specific configuration of the subsystem (in terms of operational hours), is sufficient to support the claimed rates of failure on a statistical basis. As a minimum, sufficient operational time is required to establish the claimed failure rate data to a single-sided lower confidence limit of at least 70 % (see IEC 61508-7, annex D and IEEE 352). An operational time of any individual subsystem of less than one year shall not be considered as part of the total operational time in the statistical analysis (see note).

NOTE The necessary time, in terms of operational hours, required to establish the claimed rates of failure may result from the operation of a number of identical subsystems, provided that failures from all the subsystems have been effectively detected and reported (see 7.4.7.10). If, for example, 100 subsystems each work fault-free for 10,000 h, then the total time of fault-free operation may be considered as 1,000,000 h. In this case, each subsystem has been in use for over a year and the operation therefore counts towards the total number of operational hours considered.

7.4.7.10 Only previous operation where all failures of the subsystem have been effectively detected and reported (for example, when failure data has been collected in accordance with the recommendations of IEC 60300-3-2) shall be taken into account when determining whether the above requirements (7.4.7.6 to 7.4.7.9) have been met.

7.4.7.11 The following factors shall be taken into account when determining whether or not the above requirements (7.4.7.6 to 7.4.7.9) 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 subsystem;

b) the contribution made by the subsystem to the risk reduction;

c) the consequence associated with a failure of the subsystem;

d) the novelty of design.

7.4.7.12 The application of a "proven-in-use" safety-related subsystem in the E/E/PE safety-related system should be restricted to those functions and interfaces of the subsystem which meet the relevant requirements (see 7.4.7.6 to 7.4.7.10).

NOTE The measures 7.4.7.4 to 7.4.7.12 are also applicable for subsystems which contain software. In this case it has to be assured that the subsystem performs in its safety related application only that function for which evidence of the required safety integrity is given. See also 7.4.2.11 of IEC 61508-3.

7.4.8 Requirements for data communications

7.4.8.1 When any form of data communication is used in the implementation of a safety function then the probability of undetected failure of the communication process shall be estimated taking into account transmission errors, repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade (see also 7.4.8.2). This probability shall be taken into account when estimating the probability of dangerous failure of the safety function due to random hardware failures (see 7.4.3.2.2).

NOTE The term masquerade means that the true contents of a message are not correctly identified. For example, a message from a non-safety component is incorrectly identified as a message from a safety component.

7.4.8.2 In particular, the following parameters shall be taken into account when estimating the probability of failure of the safety function due to the communication process:

a) the residual error rate (see IEV 371-08-05);

b) the rate of residual information loss (see IEV 371-08-09);

c) the limits, and variability, of the rate of information transfer (bit rate);

d) the limits, and variability, of the information propagation delay time.

NOTE 1 It can be shown that the probability of a dangerous failure per hour is equal to the quotient of the residual error probability and the message length (in bits) multiplied by the bus transmission rate for safety-related messages and a factor of 3600.

NOTE 2 Further information can be found in IEC 60870-5-1 and in EN 50159-1 and EN 50159-2.

7.5 E/E/PES integration

NOTE This phase is box 9.4 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 systems.

7.5.2 Requirements

7.5.2.1 The E/E/PE safety-related systems shall be integrated according to the specified E/E/PES design and shall be tested according to the specified E/E/PES 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 systems, the E/E/PE safety-related systems 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. In case of development according to the rules leading to structured design (see B.3.2 of 61508-7), or semi-formal methods (see B.2.3 of 61508-7), the requirements are easier to fulfil than if not.

NOTE 2 Where the development uses formal methods (see B.2.2 of IEC 61508-7) or formal proofs or assertions (see C.5.13 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 PES 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 systems 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 systems shall be subject to an impact analysis which shall identify all components affected and the necessary re-verification activities.

7.5.2.6 The E/E/PES 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 systems 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/PES integration, an appropriate group of techniques and measures according to table B.3 shall be used.

7.6 E/E/PES operation and maintenance procedures

NOTE This phase is box 9.5 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 systems is maintained during operation and maintenance.

7.6.2 Requirements

7.6.2.1 E/E/PES operation and maintenance procedures shall be prepared which shall specify the following:

a) the routine actions which need to be carried out to maintain the "as-designed" functional safety of the E/E/PE safety-related systems, including routine replacement of components 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 hazardous event;

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

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

e) the maintenance procedures to be followed when faults or failures occur in the E/E/PE safety-related systems, including
   - procedures for fault diagnoses and repair,
   - procedures for revalidation,
   - maintenance reporting requirements;

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/PES operation and maintenance procedures with the EUC overall operation and maintenance procedures.

NOTE 2 The E/E/PES 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 systems.

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

- examination of fault trees;
- failure mode and effect analysis;
- reliability centred maintenance.

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 systems.

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 7.4.3.2.2) is to ensure that the frequencies of the two types of tests are appropriate for the target hardware safety integrity.

7.6.2.4 The E/E/PES 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/PES operation and maintenance procedures, an appropriate group of techniques and measures according to table B.4 shall be used.

7.7 E/E/PES safety validation

NOTE This phase is box 9.6 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 systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity (see 7.2).

7.7.2 Requirements

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

NOTE 1 The E/E/PES safety validation is shown on the E/E/PES safety lifecycle as being carried out prior to installation but, in some cases, the E/E/PES 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 Each safety function specified in the requirements for E/E/PES safety (see 7.2), and all the E/E/PES operation and maintenance procedures shall be validated by test and/or analysis.

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

a) the version of the E/E/PES 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/PES 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/PES 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/PES 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/PES safety validation, an appropriate group of techniques and measures according to table B.5 shall be used.

7.8 E/E/PES modification

7.8.1 Objective

The objective of the requirements of this subclause is to ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

7.8.2 Requirements

7.8.2.1 Appropriate documentation shall be established and maintained for each E/E/PES 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 components including revalidation data;

f) E/E/PES 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 which 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/PES 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 across several phases.

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/PES safety lifecycle, and shall be documented.

7.9.2.2 The E/E/PES 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/PES 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/PES 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 which do not conform to one or more relevant requirements of the E/E/PES safety lifecycle (see 7.2);

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

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

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

a) determine whether the E/E/PES safety requirements are adequate to satisfy the requirements set out in the E/E/PES safety requirements allocation (see IEC 61508-1) for safety, functionality, and other requirements specified during safety planning, and

b) check for incompatibilities between
   - the E/E/PES safety requirements (7.2),
   - the safety requirements allocation (IEC 61508-1),
   - the E/E/PES tests (see 7.4), and
   - the user documentation and all other system documentation.

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

a) determine whether the E/E/PES tests (see 7.4) are adequate for the E/E/PES design and development (see 7.4);

b) determine the consistency and completeness (down to and including module level) of the E/E/PES design and development (see 7.4) with respect to the E/E/PES safety requirements (see 7.2); and

c) check for incompatibilities between
   - the E/E/PES safety requirements (7.2),
   - the E/E/PES design and development (7.4), and
   - the E/E/PES 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/PES integration verification, the integration of the E/E/PE safety-related systems 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 components); 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/PES 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 is determined on the basis of table A.1 and according to procedures detailed in annex C. Tables A.2 to A.15 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.15 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.16 to A.18 recommend techniques and measures for each safety integrity level for controlling systematic failures. Table A.16 recommends overall measures to control systematic failures (see also IEC 61508-3), table A.17 recommends measures to control environmental failures and table A.18 recommends measures to control operational failures. Most of these control measures can be graded according to table A.19.

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 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.15 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.15 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.15.

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 detected during operation or to be analysed in the derivation of safe failure fraction

Component	See table(s)	Requirements for diagnostic coverage or safe failure fraction claimed		
		Low (60 %)	**Medium (90 %)**	**High (99 %)**
Electromechanical devices	A.2	Does not energize or de-energize Welded contacts	Does not energize or de-energize Individual contacts welded	Does not energize or de-energize 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 EN 60947-5-1, or equivalent)
Discrete hardware	A.3, A.7, A.9, A.11			
Digital I/O		Stuck-at	DC fault model	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	A.8	Stuck-at of data or addresses	Wrong address decoding	Wrong address decoding
Direct memory access		No or continuous access	DC fault model for data and addresses	All faults which affect data in the memory
			Wrong access time	Wrong data or addresses Wrong access time
Bus-arbitration (see note 1)		Stuck-at of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration
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 Dynamic cross-over for memory cells 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
Program counter, stack pointer		Stuck-at	DC fault model	DC fault model
Interrupt handling	A.4	No or continuous interrupts	No or continuous interrupts Cross-over of interrupts	No or continuous interrupts Cross-over of interrupts

Table A.1 *(continued)*

Component	See table(s)	Requirements for diagnostic coverage or safe failure fraction claimed		
		Low (60 %)	**Medium (90 %)**	**High (99 %)**
Invariable memory	A.5	Stuck-at for data and addresses	DC fault model for data and addresses	All faults which affect data in the memory
Variable memory	A.6	Stuck-at for data and addresses	DC fault model for data and addresses Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher	DC fault model for data and addresses Dynamic cross-over for memory cells No, wrong or multiple addressing Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher
Clock (quartz)	A.12	Sub- or super-harmonic	Sub- or super-harmonic	Sub- or super-harmonic
Communication and mass storage	A.13	Wrong data or addresses No transmission	All faults which affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence	All faults which affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence
Sensors	A.14	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation
Final elements	A.15	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation

NOTE 1 Bus-arbitration is the mechanism for deciding which device has control of the bus.

NOTE 2 "Stuck-at" is a fault category which can be described with continuous "0" or "1" or "on" at the pins of a component.

NOTE 3 "DC fault model" (DC = direct current) includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines.

Table A.2 – Electrical subsystems

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	
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
Idle current principle	A.1.5	Low	Only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC

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 subsystems

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.			

Table A.5 – Invariable memory ranges

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Word-saving multi-bit redundancy	A.4.1	Medium	
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	High	
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 which is read/written only infrequently (for example during configuration) the measures A.4.1 to A.4.4 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
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	
Multi-bit hardware redundancy	A.7.2	Medium	
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	Recommended always to be used in addition to other techniques in this table
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	Recommended always to be used in addition to other techniques in this table
Idle current principle	A.1.5	Low	Useful only against power-down
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 – Ventilation and heating system (if necessary)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Temperature sensor	A.10.1	Medium	
Fan control	A.10.2	Medium	
Actuation of the safety shut-off via thermal fuse	A.10.3	High	
Staggered message of thermo-sensors and conditional alarm	A.10.4	High	
Connection of forced-air cooling and status indication	A.10.5	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.12 – 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.13 – 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
Separation of electrical energy lines from information lines	A.11.1	High	Recommended to be always used in addition to other techniques in this table
Spatial separation of multiple lines	A.11.2	High	
Increase of interference immunity	A.11.3	High	
Antivalent signal transmission	A.11.4	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 – 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
Idle current principle	A.1.5	Low	Only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC
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.15 – 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	
Idle current principle	A.1.5	Low	Only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC
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 and software design (see table A.16);
– control failures due to environmental stress or influences (see table A.17); and
– control failures during operation (see table A.18).

In tables A.16 to A.18, recommendations are made 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.

– 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. At least one of the techniques in the light grey shaded group is required;
– -: 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.

– Mandatory: the technique or measure is required for all safety integrity levels and shall be used as effectively as possible (i.e. giving high effectiveness).
– 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.19.

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/PES 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.16 to A.18 can be used with varying effectiveness according to table A.19, 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.

Table A.16 – Techniques and measures to control systematic failures caused by hardware and software design

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	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
	Fault detection and diagnosis	C.3.1	See table A.2 of IEC 61508-3			
	Error detecting and correcting codes	C.3.2				
	Failure assertion programming	C.3.3				
	Safety bag techniques	C.3.4				
	Diverse programming	C.3.5				
	Recovery block	C.3.6				
	Backward recovery	C.3.7				
	Forward recovery	C.3.8				
	Re-try fault recovery mechanisms	C.3.9				
	Memorising executed cases	C.3.10				
	Graceful degradation	C.3.11				
	Artificial intelligence fault correction	C.3.12				
	Dynamic reconfiguration	C.3.13				

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 this table.

NOTE 2 The measures in this table which do not refer to table A.2 of IEC 61508-3 can be used to varying effectiveness according to table A.19, 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.17 – Techniques and measures to control systematic failures caused by environmental stress or influences

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Measures against voltage breakdown, voltage variations, overvoltage, low voltage	A.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Separation of electrical energy lines from information lines (see note 4)	A.11.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Increase of interference immunity	A.11.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	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
	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 table A.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.16.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table A.19, 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 which are designed for energising components of the E/E/PES and carrying information from or to these components.

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.18 – Techniques and measures to control systematic operational failures

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Modification protection	B.4.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	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 table A.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.16.

NOTE 2 Two of these measures in this table can be used to varying effectiveness according to table A.19, 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.19 – 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
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	Temperature sensor, detecting over-temperature	Actuation of the safety shut-off via thermal fuse
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 which 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
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 components); 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/PES 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 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:

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

– -: 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.

– Mandatory: the technique or measure is required for all safety integrity levels and shall be used as effectively as possible (i.e. giving high effectiveness);

– 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 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 – Recommendations to avoid mistakes during specification of E/E/PES requirements (see 7.2)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Separation of E/E/PE safety-related systems from non-safety-related systems	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 – Recommendations to avoid introducing faults during E/E/PES design and development (see 7.4)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Observance of guidelines and standards	B.3.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR 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 – Recommendations to avoid faults during E/E/PES integration (see 7.5)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Functional testing	B.5.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR 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 – Recommendations to avoid faults and failures during E/E/PES operation and maintenance procedures (see 7.6)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Operation and maintenance instructions	B.4.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	User friendliness	B.4.2	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Maintenance friendliness	B.4.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR 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 – Recommendations to avoid faults during E/E/PES safety validation (see 7.7)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Functional testing	B.5.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Functional testing under environmental conditions	B.6.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Interference surge immunity testing	B.6.2	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Fault insertion testing (when required diagnostic coverage ≥ 90 %)	B.6.10	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR 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 SIL3 and SIL4, 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 safety-related systems from non safety-related systems	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 subrequirements; 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 7.4.4)
Use of well-tried components (see note)	B.3.3	Sufficient over-dimensioning; constructive characteristics	Proven in use (see 7.4.7.6)
Modularisation (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 which are proven in use (see 7.4.7.6) 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 and B.5.4, 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 subsystem

The diagnostic coverage and safe failure fraction of a subsystem 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 subsystem 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 subsystem 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 subsystem 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 a subsystem which 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 (i.e. leading to the safety integrity of an E/E/PE safety-related system not being compromised, for example, a failure leading to a safe shut-down or having no impact on the safety integrity of the E/E/PE safety-related system); or

– a dangerous failure (i.e. leading to an E/E/PE safety-related system, or part thereof, failing to function, or leading to the safety integrity of the E/E/PE safety-related system being otherwise compromised).

c) From an estimate of the failure probability of each component or group of components, λ, (see notes 2 and 3) and the results of the failure mode and effect analysis, for each component or group of components, calculate the probability of safe failure, λ_S, and the probability of dangerous failure, λ_D.

NOTE 3 The failure probability of each component or group of components is the probability of a failure occurring within a relatively small period of time, t. This can be considered as being equal to λ, the failure rate per unit time, t, in cases where λt is much less than 1.

NOTE 4 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 subsystem 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.

d) For each component or group of components, estimate the fraction of dangerous failures which will be detected by the diagnostic tests (see C.2) and therefore the probability of a dangerous failure which is detected by the diagnostic tests, λ_{DD}.

e) For the subsystem, calculate the total probability of dangerous failure, $\Sigma\lambda_D$, the total probability of dangerous failures that are detected by the diagnostic tests, $\Sigma\lambda_{DD}$, and the total probability of safe failures $\Sigma\lambda_S$,

f) Calculate the diagnostic coverage of the subsystem as $\Sigma\lambda_{DD}/\Sigma\lambda_D$.

g) Calculate safe failure fraction of the subsystem as $(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

NOTE 5 The diagnostic coverage (if any) of each subsystem in the E/E/PE safety-related system is taken into account in the calculation of the probability of random hardware failures (see 7.4.3.2.2). The safe failure fraction is taken into account when determining the architectural constraints on hardware safety integrity (see 7.4.3.1).

The analysis used to determine the diagnostic coverage and safe failure fraction shall include all of the components, including electrical, electronic, electromechanical, mechanical etc, which are necessary to allow the subsystem 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 provides the faults or failures that shall, as a minimum, be detected in order to achieve the relevant diagnostic coverage or that shall, as a minimum, be included in the determination of 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 a subsystem (see C.1) it is necessary to estimate, for each component or group of components, the fraction of dangerous failures which are detected by the diagnostic tests. The diagnostic tests which 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 components (see 7.4.3.1.3), 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 subsystem and for each subsystem of the E/E/PE safety-related systems.

NOTE 1 Tables A.2 to A.15 recommend techniques and measures for diagnostic tests and recommend maximum diagnostic coverage which 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 annex C.

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, 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.

NOTE 3 The calculations to obtain the diagnostic coverage, and the ways it is used, assume that the E/E/PE safety-related systems 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 is to be treated as operating in the high demand/continuous mode of operation (see 7.4.6.3 and 7.4.3.2.5).

NOTE 4 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.

NOTE 5 The diagnostic tests used to detect a dangerous failure within a subsystem may be implemented by another subsystem within the E/E/PE safety-related system.

NOTE 6 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.

Bibliography

IEC 61000-4, *Electromagnetic compatibility – Part 4: Testing and measurement techniques*

IEC 60870-5-1:1990, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section one: Transmission frame formats*

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

EN 50159-1, *Railway applications – Safety-related communication in closed transmission systems*

EN 50159-2, *Railway applications – Safety-related communication in open transmission systems*

ANSI/ISA-S84.01:1996, *Application of safety-instrumented systems for the process industry*

ANSI/IEEE Std 352:1987, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Stations Safety Systems*

SOMMAIRE

Pages

Pages

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

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

AVANT-PROPOS

1) La CEI (Commission Électrotechnique Internationale) 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. 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 intéressés sont représentés dans chaque comité d'études.
3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale 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 élaborée par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure et commande dans les processus industriels.

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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/294/FDIS	65A/303/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 3.

Les annexes A, B et C font partie intégrante de la présente norme.

La CEI 61508 est composée des parties suivantes, regroupées sous le titre général *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*:

– Partie 1: Prescriptions générales
– Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
– Partie 3: Prescriptions concernant les logiciels
– Partie 4: Définitions et abréviations
– Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité
– Partie 6: Lignes directrices pour l'application des parties 2 et 3
– Partie 7: Présentation de techniques et mesures

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2006. A cette date, la publication sera

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

INTRODUCTION

Les systèmes électriques/électroniques sont utilisés depuis des années pour exécuter des fonctions liées à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (que l'on nommera de façon générique: systèmes électroniques programmables (PES)) sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non liées à la sécurité, mais aussi de plus en plus souvent liées 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 liés 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/électroniques/électroniques programmables (E/E/PES) 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 appareils électriques liés à la sécurité. L'un des principaux objectifs poursuivis consiste à faciliter l'élaboration de normes par secteur d'application.

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes de protection 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, les actionneurs), mais elle doit aussi considérer tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. C'est pourquoi la présente Norme internationale, bien que traitant essentiellement des systèmes E/E/PE relatifs à la sécurité, fournit néanmoins un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

Personne n'ignore la grande variété des applications E/E/PES. Celles-ci recouvrent, à des degrés de complexité très divers, un fort potentiel de danger et de risques dans tous les secteurs d'application. Pour chaque application, la nature exacte des mesures de sécurité envisagées dépendra de plusieurs facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rendra désormais possible la prescription de ces mesures dans des Normes internationales par secteur d'application.

La présente Norme internationale

– concerne toutes les phases appropriées du cycle de vie de sécurité global des E/E/PES et du logiciel (depuis la conceptualisation initiale, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service) lorsque les E/E/PES exécutent des fonctions de sécurité;

– a été élaborée dans le souci 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 par secteur d'application concernant les E/E/PES relatifs à la sécurité – l'élaboration de Normes internationales par secteur d'application à partir de la présente Norme internationale devrait permettre d'atteindre un haut niveau de cohérence (par exemple pour ce qui est des principes sous-jacents, de la terminologie, de la documentation, etc.) à la fois au sein de chaque secteur d'application, et d'un secteur à l'autre. La conséquence en étant une amélioration en termes de sécurité et de bénéfices économiques;

– fournit une méthode de développement des prescriptions de sécurité nécessaires pour réaliser la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité;

– utilise des niveaux d'intégrité de sécurité afin de spécifier les niveaux cibles d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes E/E/PE relatifs à la sécurité;

– adopte une approche basée sur le risque encouru pour déterminer les niveaux d'intégrité de sécurité prescrits;

– fixe des objectifs quantitatifs pour les mesures de défaillances des systèmes E/E/PE relatifs à la sécurité qui sont en rapport avec les niveaux d'intégrité de sécurité;

– fixe une limite inférieure pour les mesures de défaillances, dans le cas d'un mode de défaillance dangereux, cette limite pouvant être exigée pour un système E/E/PE relatif à la sécurité unique; dans le cas d'un système E/E/PE relatif à la sécurité fonctionnant

  – dans un mode de faible sollicitation, la limite inférieure est fixée à une probabilité moyenne de défaillance de 10^{-5} afin que les fonctions pour lesquelles le système a été conçu soient exécutées lorsqu'elles sont requises,

  – dans un mode de fonctionnement continu ou de forte sollicitation, la limite inférieure est fixée à une probabilité de défaillance dangereuse de 10^{-9} par heure;

NOTE Un système E/E/PE relatif à la sécurité unique n'implique pas nécessairement une architecture à une seule voie.

– 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 le concept de sécurité intrinsèque qui peut être intéressant lorsque les modes de défaillances sont bien définis et que le niveau de complexité est relativement faible. Le concept de sécurité intrinsèque a été considéré comme inadéquat en raison de l'immense gamme de complexité des systèmes E/E/PE relatifs à la sécurité qui entrent dans le domaine d'application de la présente norme.

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

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

1 Domaine d'application

1.1 La présente partie de la norme CEI 61508

a) est destinée à être utilisée uniquement après avoir compris de manière approfondie la CEI 61508-1 qui fournit le cadre global permettant de réaliser 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 sous-systèmes et leurs composants dans 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 les informations développées conformément à la CEI 61508-1, relatives aux prescriptions de sécurité globales et leur affectation aux systèmes E/E/PE relatifs à la sécurité, et spécifie la manière dont les prescriptions de sécurité globales sont affinées en prescriptions de sécurité E/E/PES et en prescriptions d'intégrité de sécurité E/E/PES;

e) spécifie les prescriptions 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 E/E/PES), à l'exception du logiciel qui est traité dans la CEI 61508-3 (voir figures 2 et 3) – ces prescriptions comprennent l'application de techniques et de mesures qui sont classées en fonction du niveau d'intégrité de sécurité pour éviter et maîtriser les défauts 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 effectivement les prescriptions de 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 prescriptions auxquelles doit satisfaire l'organisation qui effectue une éventuelle 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. C'est pour cette raison qu'elle comprend les prescriptions applicables en matière de modification.

NOTE 2 La relation entre la CEI 61508-2 et la CEI 61508-3 est illustrée à la figure 3.

1.2 Les CEI 61508-1, 61508-2, 61508-3 et 61508-4 sont des publications fondamentales de sécurité, bien que ce statut ne s'applique pas dans le cas de systèmes E/E/PE de sécurité de faible complexité (voir 3.4.4 de la CEI 61508-4). En tant que publications fondamentales de sécurité, elles sont destinées à être utilisées par tous les comités d'études pour la mise au point de leurs normes, conformément aux principes décrits dans le Guide 104 de la CEI et dans le Guide 51 ISO/CEI. La CEI 61508 est également prévue pour une utilisation en tant que norme autonome.

L'une des responsabilités d'un comité d'études est, chaque fois que cela peut s'appliquer, d'utiliser les publications fondamentales de sécurité pour préparer ses propres publications. Dans ce contexte, les prescriptions, les méthodes d'essais ou les conditions d'essais de la présente publication fondamentale de sécurité ne sont pas applicables, sauf s'il y est spécifiquement fait référence, ou si elles sont incorporées dans les publications préparées par ces comités d'études.

NOTE 1 La sécurité fonctionnelle d'un système E/E/PE relatif à la sécurité ne peut être réalisée que lorsque toutes les prescriptions pertinentes sont remplies. En conséquence, il est important que toutes les prescriptions pertinentes soient prises en considération avec soin et référencées de façon appropriée.

NOTE 2 Aux Etats-Unis et au Canada, dans l'attente de la publication de la future CEI 61511 (la version de la CEI 61508 pour le processus) les normes nationales existantes pour la sécurité des processus industriels basés sur la CEI 61508 (c'est-à-dire ANSI/ISA-S84.01) peuvent être appliquées au domaine des processus industriels à la place de la CEI 61508.

1.3 La figure 1 montre la structure générale des parties 1 à 7 de la CEI 61508 et indique le rôle que la CEI 61508-2 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.

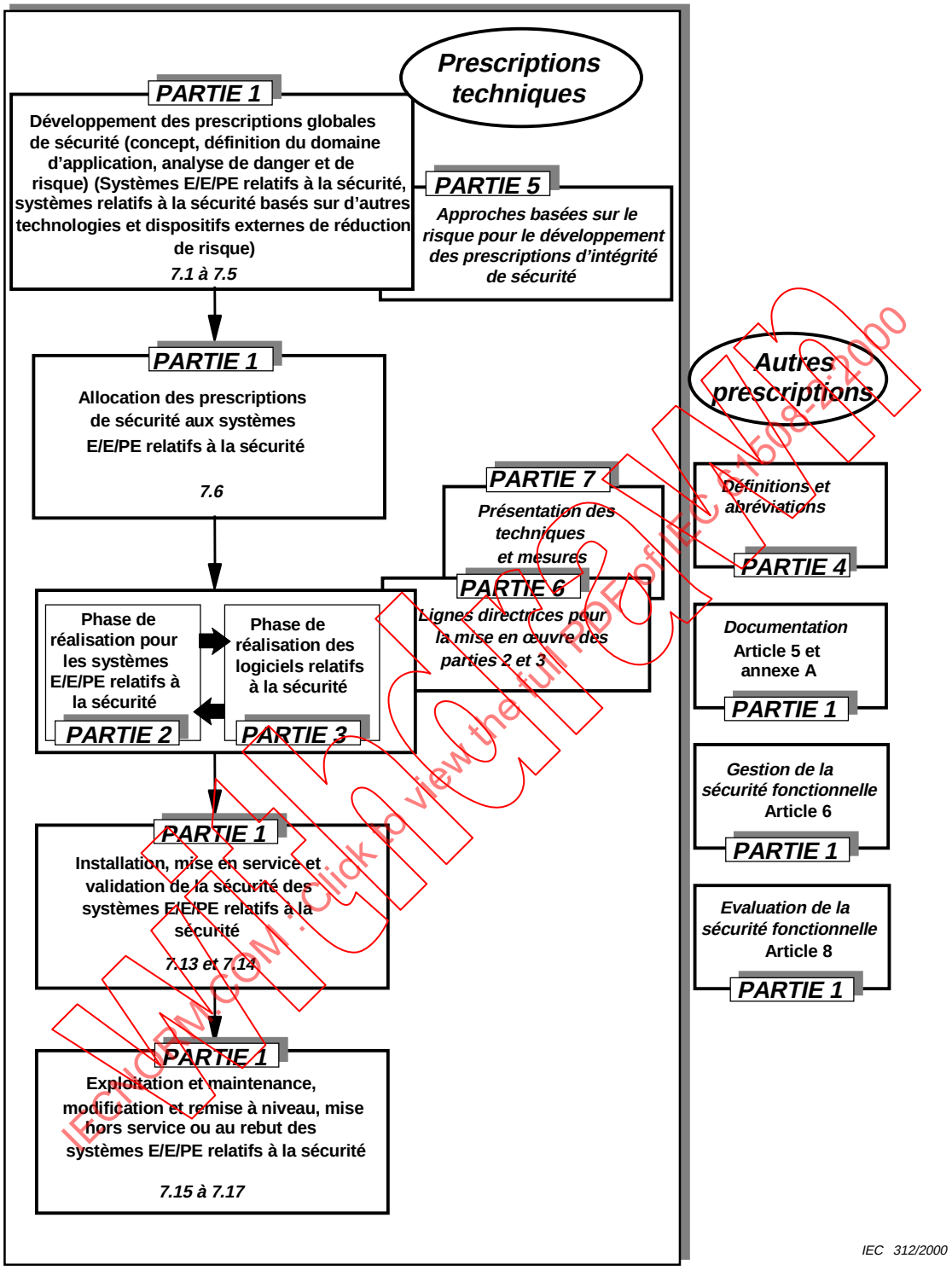


Figure 1 – Structure générale de la CEI 61508

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente partie de la CEI 61508. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de la CEI 61508 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 60050(371):1984, *Vocabulaire Electrotechnique International (VEI) – Chapitre 371: Téléconduite*

CEI 60300-3-2:1993, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 2: Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

CEI 61000-1-1:1992, *Compatibilité électromagnétique (CEM) – Partie 1: Généralités – Section 1: Application et interprétation de définitions et termes fondamentaux*

CEI 61000-2-5:1995, *Compatibilité électromagnétique (CEM) – Partie 2: Environnement – Section 5: Classification des environnements électromagnétiques – Publication fondamentale en CEM*

CEI 61508-1:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-3:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-5:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

CEI 61508-6, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application des parties 2 et 3* [1)]

CEI 61508-7:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

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

Guide ISO/CEI 51:1990, *Principes directeurs pour inclure dans les normes les aspects liés à la sécurité*

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

[1)] A publier.

3 Définitions et abréviations

Pour les besoins de la présente partie de la CEI 61508, les définitions ainsi que les abréviations données dans la CEI 61508-4 s'appliquent.

4 Conformité à la présente norme

Les prescriptions de conformité à la présente norme sont détaillées à l'article 4 de la CEI 61508-1.

5 Documentation

Les prescriptions relatives à la documentation sont détaillées à l'article 5 de la 61508-1.

6 Gestion de la sécurité fonctionnelle

Les prescriptions pour la gestion de la sécurité fonctionnelle sont détaillées à l'article 6 de la CEI 61508-1.

7 Prescriptions du cycle de vie de sécurité E/E/PES

7.1 Généralités

7.1.1 Objectifs et prescriptions: Généralités

7.1.1.1 Le présent paragraphe établit les objectifs et les prescriptions pour les phases du cycle de vie de sécurité E/E/PES.

NOTE La CEI 61508-1 donne les objectifs et les prescriptions 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 E/E/PES, le tableau 1 indique

– les objectifs à atteindre;
– le domaine d'application de la phase concernée;
– une référence au paragraphe qui contient les prescriptions;
– les données requises pour les phases;
– les résultats requis pour satisfaire aux prescriptions du paragraphe concerné.

7.1.2 Objectifs

7.1.2.1 Le premier objectif des prescriptions de ce paragraphe est de structurer de manière systématique les phases du cycle de vie de sécurité E/E/PES qui doivent être prises en compte afin de réaliser la sécurité fonctionnelle exigée des systèmes E/E/PE relatifs à la sécurité.

7.1.2.2 Le second objectif des prescriptions de ce 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 E/E/PES.

7.1.3 Prescriptions

7.1.3.1 Le cycle de vie de sécurité E/E/PES qui doit être utilisé pour déclarer la conformité à la présente norme est celui spécifié à la figure 2. Si un autre cycle de vie de sécurité E/E/PES est utilisé, il doit être spécifié au cours de la planification de la sécurité fonctionnelle (voir article 6 de la CEI 61508-1) et satisfaire à l'ensemble des objectifs et prescriptions de chaque paragraphe de la CEI 61508-2.

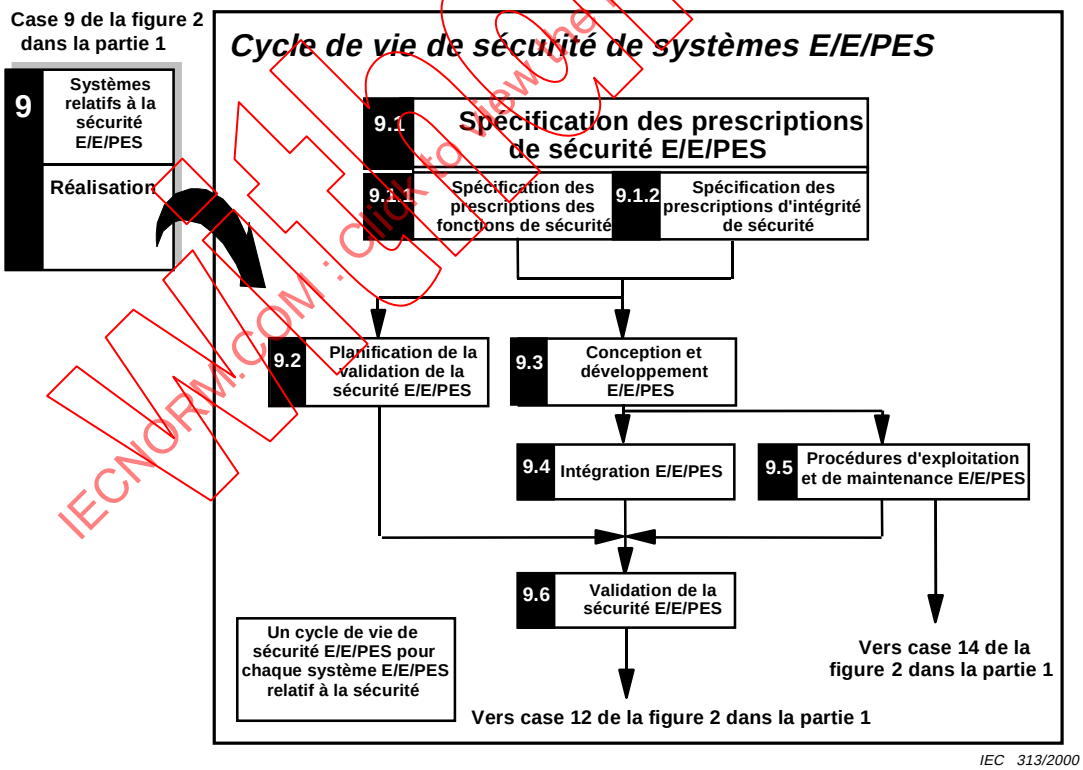
NOTE Les relations entre la CEI 61508-2 et la CEI 61508-3, ainsi que leurs domaines d'application respectifs sont illustrés à la figure 3.

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 E/E/PES.

7.1.3.3 Chaque phase du cycle de vie de sécurité E/E/PES doit être divisée en activités élémentaires, en tenant compte du domaine d'application, des données et des résultats spécifiés pour chaque phase (voir tableau 1).

7.1.3.4 Sauf lorsque cela est justifié lors de la planification de la sécurité fonctionnelle, les résultats de chaque phase du cycle de vie de sécurité E/E/PES 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 E/E/PES doivent satisfaire aux objectifs et prescriptions spécifiés pour chaque phase (voir 7.2 à 7.9).



NOTE Voir également la CEI 61508-6, A.2(b).

Figure 2 – Cycle de vie de sécurité E/E/PES (au cours de la phase de réalisation)

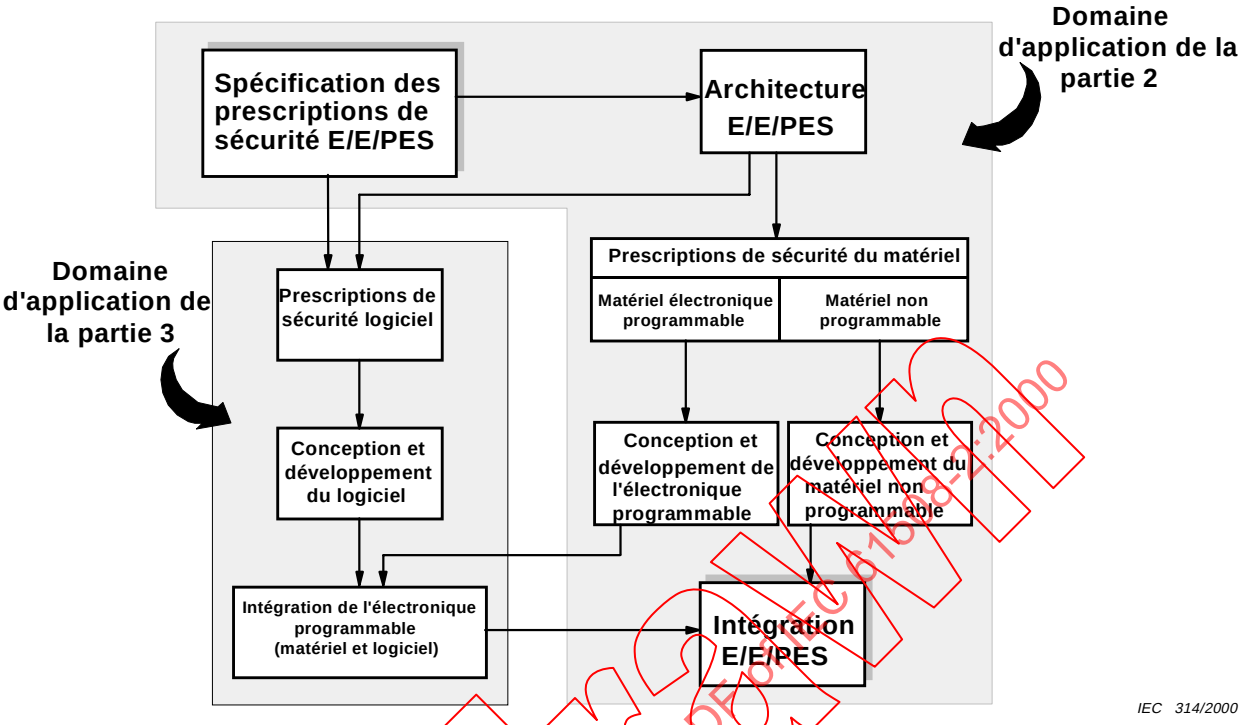


Figure 3 – Relation et domaine d'application de la CEI 61508-2 et de la CEI 61508-3

Tableau 1 – Présentation du cycle de vie de sécurité E/E/PES

Phase ou activité du cycle de vie de sécurité		Objectifs	Domaine d'application	Paragraphe des prescriptions	Données	Résultats
Figure 2 numéro de la case	Titre					
9.1	Spécification des prescriptions de sécurité E/E/PES	Spécifie des prescriptions pour chaque système E/E/PE relatif à la sécurité en termes de fonctions de sécurité requises et d'intégrité de sécurité requise afin d'obtenir la sécurité fonctionnelle requise	Systèmes E/E/PE relatifs à la sécurité	7.2.2	Description de l'attribution des prescriptions de sécurité (voir 7.6 de la CEI 61508-1).	Prescriptions de sécurité E/E/PES Prescriptions de sécurité du logiciel pour contribution à la spécification des prescriptions de sécurité du logiciel.
9.2	Planification de la validation de la sécurité E/E/PES	Planifie la validation de la sécurité des systèmes E/E/PE relatifs à la sécurité	Systèmes E/E/PE relatifs à la sécurité	7.3.2	Prescriptions de sécurité E/E/PES	Plan de validation de la sécurité des systèmes E/E/PE relatifs à la sécurité.
9.3	Conception et développement E/E/PES	Permet de concevoir les systèmes E/E/PE relatifs à la sécurité de manière qu'ils soient conformes aux prescriptions des fonctions de sécurité et d'intégrité de sécurité	Systèmes E/E/PE relatifs à la sécurité	7.4.2 à 7.4.9	Prescriptions de sécurité E/E/PES	Conception des systèmes E/E/PE relatifs à la sécurité, conformément aux prescriptions de sécurité E/E/PES Plan de tests d'intégration E/E/PES Information sur l'architecture PES en tant que contribution à la spécification de prescriptions de sécurité du logiciel
9.4	Intégration E/E/PES	Permet l'intégration et les tests des systèmes E/E/PE relatifs à la sécurité	Systèmes E/E/PE relatifs à la sécurité	7.5.2	Conception E/E/PES Plan de tests d'intégration E/E/PES Parties matériel et logiciel de l'électronique programmable	Systèmes E/E/PE relatifs à la sécurité, pleinement fonctionnels et conformes à la conception E/E/PES Résultats des tests d'intégration E/E/PES
9.5	Procédures d'exploitation et de maintenance E/E/PES	Développe des procédures permettant de s'assurer que la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité est maintenue en cours d'exploitation et de maintenance	Systèmes E/E/PE relatifs à la sécurité EUC	7.6.2	Prescriptions de sécurité E/E/PES Conception E/E/PES	Procédures d'installation, de mise en service, d'exploitation et de maintenance pour chaque E/E/PES individuel
9.6	Validation de la sécurité E/E/PES	Valide la conformité, à tous égards, des systèmes E/E/PE relatifs à la sécurité, aux prescriptions de sécurité en termes de fonctions de sécurité requises et d'intégrité de sécurité requise	Systèmes E/E/PE relatifs à la sécurité	7.7.2	Prescriptions de sécurité E/E/PES; Plan de validation de la sécurité des systèmes E/E/PE relatifs à la sécurité	Systèmes E/E/PE relatifs à la sécurité pleinement validés en termes de sécurité Résultats de la validation de sécurité E/E/PES
–	Modification E/E/PES	Mise en œuvre de corrections, d'amélioration ou d'adaptation aux systèmes E/E/PE relatifs à la sécurité afin de s'assurer que le niveau d'intégrité de sécurité exigé est effectivement réalisé et maintenu	Systèmes E/E/PE relatifs à la sécurité	7.8.2	Prescriptions de sécurité E/E/PES	Résultats de modification E/E/PES
–	Vérification E/E/PES	Permet de tester et d'évaluer les résultats d'une phase donnée afin de s'assurer qu'ils sont corrects et conformes aux produits et normes donnés pour cette phase	Systèmes E/E/PE relatifs à la sécurité	7.9.2	Comme ci-dessus – en fonction de la phase Pour chaque phase, plan de vérification des systèmes E/E/PE relatifs à la sécurité	Comme ci-dessus – en fonction de la phase Pour chaque phase, résultats de la vérification des systèmes E/E/PE relatifs à la sécurité
–	Evaluation de la sécurité fonctionnelle E/E/PES	Enquête et conclusion quant à la sécurité fonctionnelle réalisée par les systèmes E/E/PE relatifs à la sécurité	Systèmes E/E/PE relatifs à la sécurité	8	Plan d'évaluation de sécurité fonctionnelle E/E/PES	Résultats de l'évaluation de la sécurité fonctionnelle E/E/PES

7.2 Spécification des prescriptions de sécurité E/E/PES

NOTE Cette phase est représentée dans la case 9.1 de la figure 2.

7.2.1 Objectif

L'objectif des prescriptions de ce paragraphe est de spécifier les prescriptions pour chaque système E/E/PE relatif à la sécurité en termes de fonctions de sécurité requises et d'intégrité de sécurité requise, afin d'obtenir la sécurité fonctionnelle exigée.

NOTE Par exemple, des fonctions de sécurité peuvent être exigées pour mettre ou maintenir l'EUC dans un état sûr.

7.2.2 Prescriptions générales

7.2.2.1 La spécification des prescriptions de sécurité E/E/PES doit résulter de l'attribution des prescriptions de sécurité telles que décrites en 7.6 de la CEI 61508-1 et des prescriptions spécifiées lors de la planification de la sécurité fonctionnelle (voir article 6 de la CEI 61508-1). Ces informations doivent être mises à la disposition du responsable du développement E/E/PES.

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 la présence simultanée de ces types de fonction est admise dans la présente 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).

7.2.2.2 Les prescriptions de sécurité E/E/PES doivent être exprimées et structurées pour qu'elles soient

a) claires, précises, sans ambiguïté, vérifiables, testables, maintenables et faisables; et

b) écrites de manière à pouvoir être comprises par ceux qui sont susceptibles d'utiliser les informations à toute étape du cycle de vie de sécurité E/E/PES.

7.2.2.3 La spécification des prescriptions de sécurité E/E/PES doit contenir les prescriptions applicables aux fonctions de sécurité E/E/PES (voir 7.2.3.1) ainsi que les prescriptions applicables à l'intégrité de sécurité E/E/PES (voir 7.2.3.2).

7.2.3 Prescriptions de sécurité E/E/PES

7.2.3.1 La spécification des prescriptions des fonctions de sécurité E/E/PES doit contenir

a) une description de toutes les fonctions de sécurité nécessaires à la réalisation de la sécurité fonctionnelle requise et celle-ci doit, pour chaque fonction de sécurité
   - fournir des prescriptions globales suffisamment étendues et détaillées pour la conception et le développement des systèmes E/E/PE relatifs à la sécurité,
   - décrire la manière dont les systèmes E/E/PE relatifs à la sécurité ont l'intention de réaliser ou de maintenir un état sûr de l'EUC,
   - préciser la nécessité d'une commande continue ou non ainsi que les périodes correspondantes, lorsqu'il s'agit d'obtenir ou de maintenir un état sûr de l'EUC, et
   - spécifier l'applicabilité de la fonction de sécurité aux systèmes E/E/PE relatifs à la sécurité fonctionnant en mode demande faible ou demande élevée/continu;

b) performance en termes de vitesse de traitement et de temps de réponse;

c) interfaces entre système E/E/PE relatif à la sécurité et opérateur, nécessaires pour réaliser la sécurité fonctionnelle requise;

d) toutes les informations liées à la sécurité fonctionnelle peuvent avoir une influence sur la conception du système E/E/PE relatif à la sécurité;

e) toutes les interfaces entre les systèmes E/E/PE relatifs à la sécurité et tous les autres systèmes (soit directement associés à l'intérieur, ou à l'extérieur de l'EUC);

f) tous les modes d'exploitation pertinents de l'EUC qui comprennent

- la préparation pour l'utilisation, y compris l'initialisation et le réglage,
- démarrage, apprentissage, fonctionnement en mode automatique, manuel, semi-automatique ou en régime établi,
- non-fonctionnement en régime établi, réinitialisation, arrêt, maintenance,
- conditions anormales raisonnablement prévisibles;

NOTE 1 Les conditions anormales raisonnablement prévisibles sont les conditions anormales que le développeur ou l'utilisateur peuvent raisonnablement prévoir.

NOTE 2 Il est admis que des fonctions de sécurité supplémentaires soient prescrites pour des modes de fonctionnement (par exemple, l'initialisation, le réglage ou la maintenance), pour permettre de réaliser ces opérations en toute sécurité.

g) tous les modes de comportement du système E/E/PE relatif à la sécurité – en particulier le comportement en cas de défaillance et la réponse prescrite (par exemple, alarme, arrêt automatique, etc.) du système E/E/PE relatif à la sécurité doivent être détaillés;

h) l'importance de toutes les interactions entre matériel/logiciel – lorsque cela est pertinent, toutes les contraintes exigées entre le matériel et le logiciel doivent être identifiées et documentées;

NOTE 3 Lorsque de telles interactions ne sont pas connues avant achèvement de la conception, seules les contraintes d'ordre général peuvent être déclarées.

i) limitations et conditions de contraintes du système E/E/PE relatif à la sécurité et des sous-systèmes associés, par exemple les contraintes temporelles;

j) toutes prescriptions spécifiques liées aux procédures de démarrage et redémarrage des systèmes E/E/PE relatifs à la sécurité.

7.2.3.2 La spécification des prescriptions d'intégrité de sécurité E/E/PES doit contenir

a) le niveau d'intégrité de sécurité pour chaque fonction de sécurité;

NOTE 1 Le niveau d'intégrité de sécurité d'une fonction de sécurité détermine la mesure cible de défaillance de la fonction de sécurité conformément à la CEI 61508-1, tableaux 2 et 3.

NOTE 2 Il est nécessaire de spécifier la mesure cible de défaillance d'une fonction de sécurité lorsque la réduction nécessaire de risque pour la fonction de sécurité a été obtenue en utilisant une méthode quantitative (voir la CEI 61508-1, 7.5.2.2).

b) le mode de fonctionnement faible demande ou forte demande/continu de chaque fonction de sécurité;

c) les prescriptions, contraintes, fonctions et dispositifs permettant de réaliser le test périodique du matériel E/E/PE;

d) toutes les conditions environnementales extrêmes auxquelles le système E/E/PES sera vraisemblablement exposé au cours de son cycle de vie de sécurité, y compris lors de la fabrication, du stockage, du transport, du test, de l'installation, mise en service, de l'exploitation et de la maintenance;

e) les limites d'immunité électromagnétique (voir CEI 61000-1-1) qui sont nécessaires pour assurer la compatibilité électromagnétique – il convient de déduire les limites d'immunité électromagnétique en tenant compte à la fois de l'environnement électromagnétique (voir la CEI 61000-2-5) et des niveaux d'intégrité de sécurité requis;

NOTE 1 Il est important de noter que le niveau d'intégrité de sécurité est un facteur déterminant pour les limites d'immunité électromagnétique, notamment lorsque le niveau de perturbation électromagnétique dans l'environnement est soumis à une répartition statistique. Dans la pratique, il est souvent impossible de spécifier un niveau absolu de perturbation; on ne peut qu'indiquer quel niveau il est pratiquement prévu de ne pas dépasser (il s'agit du niveau de compatibilité électromagnétique). Malheureusement, des problèmes d'ordre pratique prouvent qu'il est très difficile de définir la probabilité liée à une telle prévision. Par conséquent, la limite d'immunité ne garantit pas que le système E/E/PE relatif à la sécurité ne subira pas de défaillances du fait des perturbations électromagnétiques; il fournit uniquement un certain niveau de confiance quant à la non-occurrence d'une telle défaillance. Le niveau réel de confiance obtenu dépend de la limite d'immunité par rapport à la répartition statistique des niveaux de perturbation dans l'environnement d'exploitation. Pour des niveaux d'intégrité de sécurité supérieurs, il est nécessaire d'avoir un niveau de confiance plus élevé et, pour cela, il est recommandé que la marge par laquelle la limite d'immunité dépasse le niveau de compatibilité soit plus importante pour des niveaux d'intégrité de sécurité supérieurs.

NOTE 2 On peut également trouver des lignes directrices dans les normes de CEM de familles de produits. Mais il est important de reconnaître que des niveaux d'immunité plus élevés que ceux spécifiés dans de telles normes peuvent être nécessaires dans des localisations particulières ou lorsque le matériel est prévu pour être utilisé dans un environnement électromagnétique plus sévère.

NOTE 3 Lors de l'élaboration de la spécification des prescriptions de sécurité E/E/PES, il convient de tenir compte de l'application dans laquelle les systèmes E/E/PE relatifs à la sécurité doivent être utilisés. Ceci est notamment important pour la maintenance lorsqu'il est recommandé que l'intervalle de test périodique spécifié ne soit pas inférieur à ce que l'on peut raisonnablement attendre pour l'application particulière. Par exemple, le temps entre entretiens qui peut être obtenu de manière réaliste pour des articles de série utilisés par le grand public, sera probablement supérieur à celui d'une application mieux contrôlée.

7.2.3.3 Pour éviter les erreurs au cours de la spécification des prescriptions de sécurité E/E/PES, il doit être utilisé un ensemble de techniques et de mesures approprié conformément au tableau B.1.

7.3 Planification de la validation de la sécurité E/E/PES

NOTE Cette phase est représentée par la case 9.2 de la figure 2. Elle sera normalement réalisée parallèlement aux activités de conception et de développement E/E/PES (voir 7.4).

7.3.1 Objectif

L'objectif des prescriptions de ce paragraphe est de planifier la validation de la sécurité des systèmes E/E/PE relatifs à la sécurité.

7.3.2 Prescriptions

7.3.2.1 La planification doit être effectuée 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 prescriptions de sécurité E/E/PES (voir 7.2).

NOTE Voir la CEI 61508-3 pour le plan de validation du logiciel.

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 prescriptions définies dans la spécification des prescriptions de sécurité E/E/PES;

b) les procédures à appliquer pour valider la mise en œuvre de chaque fonction de sécurité ainsi que les critères de réussite/échec pour la réalisation des tests;

c) les procédures à appliquer pour valider l'intégrité de sécurité requise pour chaque fonction de sécurité ainsi que les critères d'acceptation/de rejet pour la réalisation des tests;

d) l'environnement nécessaire à la réalisation des tests, y compris l'ensemble des outils et équipements étalonnés nécessaires;

e) les procédures d'évaluation du test (accompagnées des justifications correspondantes);

f) les procédures de test et les critères de performance à appliquer pour valider les niveaux d'immunité électromagnétique spécifiés;

NOTE Les normes CEI 61000-2-5 et CEI 61000-4 donnent les lignes directrices pour la spécification des niveaux d'essai d'immunité.

g) stratégies de résolution des défaillances lors de la validation.

7.4 Conception et développement E/E/PES

NOTE Cette phase est représentée dans la case 9.3 de la figure 2. Elle sera normalement exécutée parallèlement à la planification de la validation de sécurité E/E/PES (voir 7.3).

7.4.1 Objectif

L'objectif des prescriptions du présent paragraphe est d'assurer que la conception et la mise en œuvre des systèmes E/E/PE relatifs à la sécurité satisfont aux prescriptions des fonctions de sécurité et d'intégrité de sécurité spécifiées (voir 7.2).

7.4.2 Prescriptions générales

7.4.2.1 La conception du système E/E/PE relatif à la sécurité doit être créée conformément à la spécification des prescriptions de sécurité E/E/PES (voir 7.2), en tenant compte de toutes les prescriptions de 7.4.

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, le logiciel intégré, le logiciel d'application, etc.), voir la figure 4, doit satisfaire toutes les prescriptions a) à c) suivantes:

a) les prescriptions d'intégrité de sécurité du matériel qui comprennent
   - les contraintes architecturales relatives à l'intégrité de sécurité du matériel (voir 7.4.3.1), et
   - les prescriptions concernant la probabilité de défaillances aléatoires dangereuses du matériel (voir 7.4.3.2);

b) les prescriptions d'intégrité de sécurité concernant les défaillances systématiques, qui comprennent:
   - les prescriptions pour l'évitement des défaillances (voir 7.4.4), et les prescriptions pour la maîtrise des défauts systématiques (voir 7.4.5), ou
   - la preuve que le matériel est «validé en utilisation» (voir 7.4.7.6 à 7.4.7.12);

c) les prescriptions relatives au comportement du système lors de la détection d'un défaut (voir 7.4.6).

NOTE 1 Cadre général pour l'intégrité de sécurité E/E/PES: La méthode générale pour choisir une approche de conception qui démontre l'obtention d'un niveau d'intégrité de sécurité (à la fois pour le matériel et l'intégrité de sécurité des défaillances systématiques), dans les systèmes E/E/PE relatifs à la sécurité, est la suivante:

- déterminer le niveau d'intégrité de sécurité (SIL) nécessaire des fonctions de sécurité (voir les CEI 61508-1 et 61508-5);
- poser: intégrité de sécurité du matériel = intégrité de sécurité relative aux défaillances systématiques = SIL (voir 7.4.3.2.1);
- pour ce qui est de l'intégrité de sécurité du matériel, déterminer l'architecture qui remplit les contraintes architecturales (voir 7.4.3.1) et démontrer que les probabilités de défaillance des fonctions de sécurité, dues aux défaillances aléatoires du matériel, remplissent les mesures cibles de défaillance (voir 7.4.3.2);
- pour ce qui est de l'intégrité de sécurité des défaillances systématiques, choisir les caractéristiques de conception qui maîtrisent (tolèrent) les défauts systématiques en exploitation réelle (voir 7.4.5) ou confirmer que les prescriptions de «validation en utilisation» sont remplies (voir 7.4.7.6 à 7.4.7.12);
- pour ce qui est de l'intégrité de sécurité des défaillances systématiques, choisir des techniques et des mesures qui évitent (empêchent l'introduction) de défauts systématiques lors de la conception et du développement (voir 7.4.4) ou confirmer que les prescriptions de «validation en utilisation» sont remplies (voir 7.4.7.6 à 7.4.7.12).

NOTE 2 La CEI 61508-3 contient des prescriptions relatives à l'architecture logicielle (voir 7.4.2.2), des prescriptions permettant de produire une spécification de test d'intégration de l'électronique programmable et du logiciel, et des prescriptions pour intégrer l'électronique programmable et le logiciel conformément à cette spécification (voir 7.5). Dans tous les cas, une coopération étroite entre le développeur du système E/E/PE relatif à la sécurité et le développeur du logiciel est nécessaire.

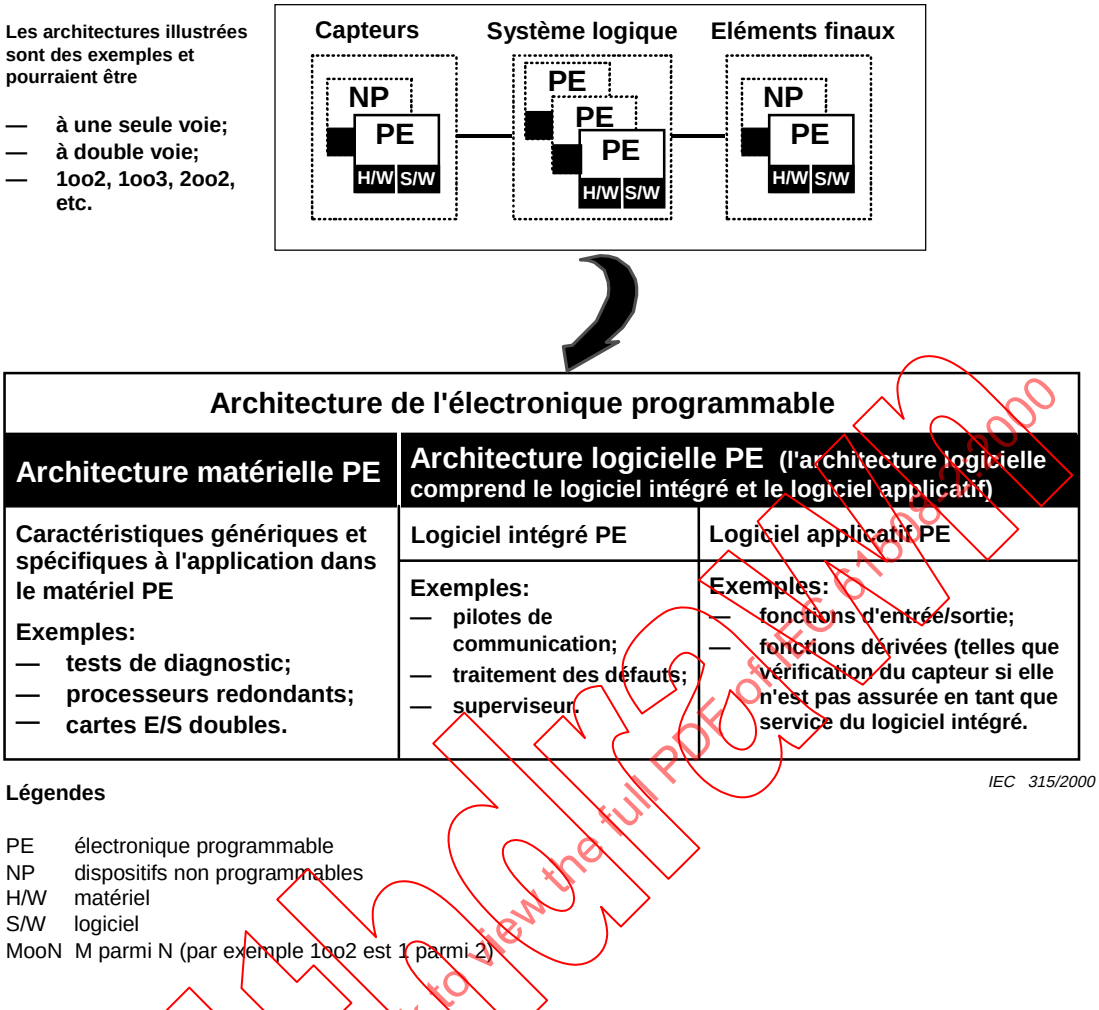


Figure 4 – Relation entre l'architecture matérielle et l'architecture logicielle de l'électronique programmable

7.4.2.3 Lorsqu'un système E/E/PE relatif à la sécurité doit mettre en œuvre des fonctions de sécurité et des fonctions non relatives à la sécurité, tout le matériel et le logiciel doivent 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 de fonctions non relatives à la sécurité est suffisamment indépendante (ce qui signifie que la défaillance de toute fonction non relative à la sécurité ne provoque pas de défaillance dangereuse). Il est recommandé, dans toute la mesure du possible, de séparer les fonctions relatives à la sécurité des fonctions non relatives à la sécurité.

NOTE 1 Une indépendance suffisante de la mise en œuvre est établie en démontrant que la probabilité d'une défaillance dépendante entre pièces non relatives à la sécurité et pièces de 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 faire particulièrement attention si des fonctions qui ne sont pas de sécurité sont mises en œuvre dans le même système E/E/PE relatif à la sécurité. Bien que cela soit autorisé par la présente norme, il peut en résulter une complexité plus grande et la difficulté pour conduire les activités liées au cycle de vie E/E/PES peut être accrue (par exemple, la conception, la validation, l'évaluation de la sécurité fonctionnelle et la maintenance).

7.4.2.4 Les prescriptions pour le matériel et le logiciel 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 de 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 d'une défaillance dépendante 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 uns système E/E/PE relatif à la sécurité, il est alors nécessaire de prendre en considération la possibilité d'un défaut unique qui pourrait provoquer la défaillance de plusieurs fonctions de sécurité. Dans une telle situation, il peut être approprié de déterminer les prescriptions concernant le matériel et le logiciel 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 une telle 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), alors les aspects suivants seront documentés lors de la conception:

a) la méthode pour réaliser l'indépendance;

b) la justification de cette méthode.

7.4.2.6 Les prescriptions concernant le logiciel relatif à la 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 revoir les prescriptions du logiciel et du matériel relatifs à la sécurité pour s'assurer qu'elles sont spécifiées de manière appropriée. Le développeur E/E/PES doit, notamment, tenir compte des éléments suivants:

a) fonctions de sécurité;

b) prescriptions d'intégrité de sécurité du système E/E/PE relatif à la sécurité;

c) interfaces entre équipements et opérateur.

7.4.2.8 La documentation de conception du système E/E/PE relatif à la sécurité doit spécifier les techniques et les mesures nécessaires au cours des phases du cycle de vie de sécurité E/E/PES pour obtenir le niveau d'intégrité de sécurité.

7.4.2.9 La documentation de conception du système E/E/PE relatif 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 tests 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 E/E/PES.

7.4.2.10 Lors des activités de conception et développement, l'importance de toutes les interactions entre le matériel et le logiciel (lorsque cela est approprié) 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 de tests d'intégration spécifiés (voir 7.4.7).

NOTE 1 On peut considérer qu'un sous-système comprend un seul composant ou un groupe quelconque de composants. 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 7.4.7.3.

NOTE 2 Chaque fois que possible, il convient d'utiliser des sous-systèmes existants et vérifiés pour la réalisation. Cette proposition n'est généralement valable que s'il est possible de mettre en correspondance, à presque 100 %, la fonctionnalité, la capacité et les caractéristiques du sous-système existant avec les nouvelles prescriptions, ou bien si le sous-système vérifié est structuré de telle sorte que l'utilisateur soit capable de choisir seulement les fonctions, les capacités et les caractéristiques nécessaires à l'application spécifique. Des fonctionnalités, des capacités ou des caractéristiques excessives peuvent porter détriment à la sécurité du système, lorsque le sous-système existant est d'une complexité trop grande, ou présente des caractéristiques non utilisées, ou s'il n'est pas possible d'obtenir la protection nécessaire contre les fonctions non souhaitées.

7.4.2.12 Lorsqu'un sous-système a des sorties multiples, il est alors nécessaire de déterminer si plusieurs combinaisons des états de sortie, ayant pour origine éventuelle une défaillance du système E/E/PE relatif à la sécurité, peuvent provoquer un événement dangereux (tel que déterminé par l'analyse de danger et de risque, voir la CEI 61508-1, 7.4.2.10). Lorsque cela a été établi, alors il faut considérer que l'empêchement de cette combinaison d'états de sorties est une fonction de sécurité exploitée en mode demande élevée/continu (voir 7.4.6.3 et 7.4.3.2.5).

7.4.2.13 La dévaluation (voir la CEI 61508-7, A.2.8) doit être utilisée autant que possible pour tous les composants. Toute justification pour utiliser un composant quelconque à ses limites doit être documentée (voir la CEI 61508-1, article 5).

NOTE Lorsque la dévaluation est pertinente, il convient d'utiliser un facteur de dévaluation d'au moins 0,67.

7.4.3 Prescriptions relatives à l'intégrité de sécurité du matériel

NOTE L'article A.2 de la CEI 61508-6 donne une vue générale des étapes nécessaires lors de la réalisation de l'intégrité de sécurité matérielle prescrite et présente la manière suivant laquelle le présent article se rapport à d'autres prescriptions de la présente norme.

7.4.3.1 Contraintes architecturales sur l'intégrité de sécurité du matériel

7.4.3.1.1 Dans le contexte de l'intégrité de sécurité du matériel, le niveau d'intégrité de sécurité le plus élevé qui peut être annoncé pour une fonction de sécurité donnée est limité par la tolérance aux anomalies du matériel et la proportion de défaillances en sécurité (voir l'annexe C) des sous-systèmes qui réalisent la fonction de sécurité. Les tableaux 2 et 3 spécifient le niveau d'intégrité de sécurité le plus élevé qui peut être annoncé pour une fonction de sécurité qui utilise un sous-système, en prenant en compte la tolérance aux anomalies du matériel et la proportion de défaillances en sécurité (voir annexe C) de ce sous-système. Les prescriptions des tableaux 2 et 3 peuvent être appliquées à chaque sous-système réalisant une fonction de sécurité et, par conséquent, à chaque partie du système E/E/PE relatif à la sécurité; les paragraphes 7.4.3.1.2 à 7.4.3.1.4 spécifient, parmi les tableaux 2 et 3, celui qui s'applique à un sous-système particulier. Les paragraphes 7.4.3.1.5 à 7.4.3.1.6 spécifient la manière dont est déduit le niveau d'intégrité de sécurité le plus élevé qui puisse être annoncé pour une fonction de sécurité donnée. Pour ce qui concerne ces prescriptions,

a) une tolérance aux anomalies du matériel N signifie que N + 1 anomalies sont susceptibles de provoquer la perte de la fonction de sécurité. Lors de la détermination de la tolérance aux anomalies du matériel, aucune autre mesure pouvant contrôler l'effet des anomalies, les diagnostics par exemple, ne doit être prise en compte; et

b) lorsqu'une anomalie donne directement lieu à l'apparition d'une ou de plusieurs anomalies subséquentes, celles-ci sont considérées comme une anomalie unique;

c) lors de la détermination de la tolérance aux anomalies du matériel, certaines anomalies peuvent être exclues pourvu que leur probabilité d'occurrence soit très faible par rapport aux prescriptions d'intégrité de sécurité du sous-système. De telles exclusions d'anomalies doivent être justifiées et documentées (voir la note 3);

d) la proportion de défaillances en sécurité d'un sous-système est définie par le rapport du taux moyen des défaillances en sécurité plus les défaillances dangereuses détectées au taux de défaillance moyen total du sous-système (voir l'annexe C).

NOTE 1 Les contraintes architecturales ont été incluses afin d'obtenir une architecture suffisamment robuste, en tenant compte du niveau de complexité du sous-système. Le niveau d'intégrité de sécurité du matériel pour le système E/E/PE relatif à la sécurité, obtenu par l'application de ces prescriptions, est le maximum qu'il est permis d'annoncer même si, dans certains cas, un niveau d'intégrité de sécurité supérieur pourrait théoriquement être calculé si une approche uniquement mathématique avait été adoptée pour le système E/E/PE relatif à la sécurité.

NOTE 2 L'architecture et le sous-système obtenu pour satisfaire aux prescriptions de tolérance aux anomalies matérielles est celui qui est utilisé dans des conditions de fonctionnement normal. Il est admis d'assouplir les prescriptions de tolérance aux anomalies lorsque le système E/E/PE relatif à la sécurité est en cours de réparation en ligne. Cependant, les paramètres clés relatifs à tout assouplissement éventuel doivent avoir été, préalablement, évalués (par exemple en comparant la durée moyenne de rétablissement à la probabilité d'une demande).

NOTE 3 Cela est nécessaire car si un composant possède 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), il n'est pas normalement considéré comme souhaitable de contraindre (sur la base de la tolérance aux anomalies du matériel) l'intégrité de sécurité d'une fonction de sécurité qui utilise ce composant.

7.4.3.1.2 Un sous-système (voir note 1 en 7.4.2.11) 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 du sous-système dans des conditions d'anomalie peut être entièrement déterminé; et

c) il existe des données de défaillance, obtenues à partir d'expérience sur le terrain, suffisamment fiables pour appuyer des taux de défaillance annoncés relatifs à des défaillances dangereuses détectées ou non détectées (voir 7.4.7.3 et 7.4.7.4).

7.4.3.1.3 Un sous-système (voir note 1 en 7.4.2.11) 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 du sous-système dans des conditions d'anomalie ne peut être entièrement déterminé; ou

c) il n'existe, pour le sous-système, aucune donnée de défaillance, obtenue à partir d'expérience sur le terrain suffisamment fiable pour appuyer des taux de défaillance annoncés relatifs à des défaillances dangereuses détectées ou non détectées (voir 7.4.7.3 et 7.4.7.4).

NOTE Cela signifie que si au moins un des composants du sous-système proprement dit satisfait aux conditions applicables à un sous-système de type B, dans ce cas, le sous-système doit être du type B plutôt que du type A. Voir également 7.4.2.11, note 1.

7.4.3.1.4 Les contraintes architecturales du tableau 2 ou du tableau 3 doivent s'appliquer à chaque sous-système réalisant une fonction de sécurité de telle sorte que

a) les prescriptions de tolérance aux anomalies matérielles soient obtenues pour l'ensemble du système E/E/PE relatif à la sécurité;

b) le tableau 2 s'applique à chaque sous-système de type A faisant partie des systèmes E/E/PE relatifs à la sécurité;

NOTE 1 Si le système E/E/PE relatif à la sécurité contient uniquement des sous-systèmes de type A, les prescriptions du tableau 2 s'appliqueront à l'ensemble du système E/E/PE relatif à la sécurité.

c) le tableau 3 s'applique à chaque sous-système de type B faisant partie des systèmes E/E/PE relatifs à la sécurité;

NOTE 2 Si le système E/E/PE relatif à la sécurité contient uniquement des sous-systèmes de type B, les prescriptions du tableau 3 s'appliqueront à l'ensemble du système E/E/PE relatif à la sécurité.

d) les tableaux 2 et 3 s'appliqueront tous les deux aux systèmes E/E/PE relatifs à la sécurité comprenant à la fois des sous-systèmes de type A et de type B, étant donné que les prescriptions du tableau 2 doivent s'appliquer aux sous-systèmes de type A et les prescriptions du tableau 3 doivent s'appliquer aux sous-systèmes de type B.

Tableau 2 – Intégrité de sécurité du matériel: contraintes architecturales sur les sous-systèmes relatifs à la sécurité de type A

Proportion de défaillances en sécurité	Tolérance aux anomalies matérielles (voir note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % – < 90 %	SIL2	SIL3	SIL4
90 % – < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE 1 Voir 7.4.3.1.1 à 7.4.3.1.4 pour plus de détails quant à l'interprétation de ce tableau. NOTE 2 Une tolérance aux anomalies du matériel N signifie que N + 1 anomalies sont susceptibles de provoquer la perte de la fonction de sécurité. NOTE 3 Voir l'annexe C pour les détails concernant le calcul de la proportion de défaillances en sécurité.			

Tableau 3 – Intégrité de sécurité du matériel: contraintes architecturales sur les sous-systèmes relatifs à la sécurité de type B

Proportion de défaillances en sécurité	Tolérance aux anomalies matérielles (voir note 2)		
	0	1	2
< 60 %	Non autorisé	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE 1 Voir 7.4.3.1.1 à 7.4.3.1.4 pour plus de détails quant à l'interprétation de ce tableau. NOTE 2 Une tolérance aux anomalies du matériel N signifie que N + 1 anomalies sont susceptibles de provoquer la perte de la fonction de sécurité. NOTE 3 Voir l'annexe C pour les détails concernant le calcul de la proportion de défaillances en sécurité.			

7.4.3.1.5 Dans des systèmes E/E/PE relatifs à la sécurité dont la fonction de sécurité est mise en œuvre par le biais d'un seul canal (comme illustré à la figure 5), le niveau d'intégrité de sécurité maximal du matériel qui peut être annoncé pour la fonction de sécurité considérée, doit être déterminé par le sous-système qui a satisfait aux prescriptions de niveau d'intégrité de sécurité du matériel le plus bas (déterminé en tenant compte des tableaux 2 et 3).

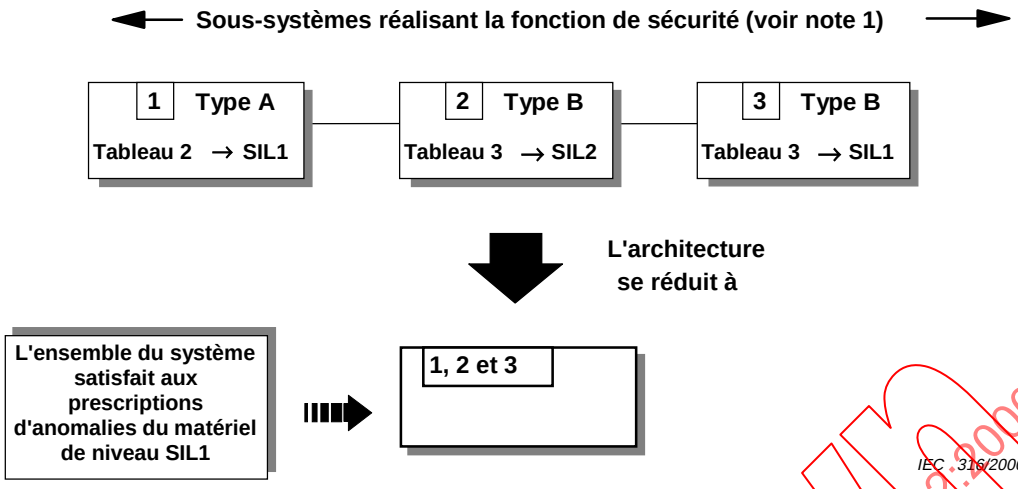
EXEMPLE Supposons une architecture dans laquelle une fonction de sécurité particulière est réalisée par un seul canal des sous-systèmes 1, 2 et 3 comme illustré à la figure 5 et dont les sous-systèmes satisfont aux prescriptions des tableaux 2 et 3 de la manière suivante:

– le sous-système 1 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL1, pour une proportion de défaillances en sécurité spécifique;

– le sous-système 2 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL2, pour une proportion de défaillances en sécurité spécifique;

– le sous-système 3 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL1, pour une proportion de défaillances en sécurité spécifique.

Pour cette architecture particulière, chacun des sous-systèmes 1 et 3 n'est capable de satisfaire qu'aux prescriptions de tolérance aux anomalies matérielles de niveau SIL1, tandis que le sous-système 2 est capable de satisfaire aux prescriptions de tolérance aux anomalies matérielles de niveau SIL2. En conséquence, les deux sous-systèmes 1 et 3 limitent le niveau d'intégrité de sécurité matériel qui peut être annoncé, en termes de tolérance aux anomalies matérielles, pour la fonction de sécurité considérée, au niveau SIL1.



NOTE 1 Les sous-systèmes réalisant la fonction de sécurité s'étendront sur l'ensemble du système E/E/PE en termes de portée, depuis les capteurs jusqu'aux actionneurs.

NOTE 2 Pour plus de détails quant à l'interprétation de cette figure, voir l'exemple du 7.4.3.1.5.

Figure 5 – Exemple de limitation de l'intégrité de sécurité du matériel pour une fonction de sécurité à un seul canal

7.4.3.1.6 Dans les systèmes E/E/PE relatifs à la sécurité dont une fonction de sécurité est mise en œuvre par le biais de plusieurs canaux de sous-systèmes (comme illustré à la figure 6), le niveau d'intégrité de sécurité maximal du matériel qui peut être annoncé pour la fonction de sécurité considérée, doit être déterminé par

a) l'évaluation de chaque sous-système par rapport aux prescriptions du tableau 2 ou 3 (comme spécifié de 7.4.3.1.2 à 7.4.3.1.4); et

b) en groupant les sous-systèmes par combinaisons; et

c) en analysant ces combinaisons pour déterminer le niveau d'intégrité de sécurité global du matériel.

EXEMPLE Il est admis d'effectuer le regroupement et l'analyse des combinaisons de diverses manières. Pour illustrer une méthode possible, on suppose une architecture dans laquelle une fonction de sécurité particulière est réalisée soit par une combinaison des sous-systèmes 1, 2 et 3, soit par une combinaison des sous-systèmes 4, 5 et 3, comme illustré à la figure 6. Dans ce cas, la combinaison des sous-systèmes 1 et 2 et la combinaison des sous-systèmes 4 et 5 ont la même fonctionnalité en termes de fonctions de sécurité et contribuent indépendamment à fournir des données au sous-système 3. Dans cet exemple, la combinaison de sous-systèmes parallèles est basée sur le fait que chaque sous-système réalise la fonction de sécurité prescrite qui le concerne indépendamment de l'autre sous-système (parallèle). La fonction de sécurité sera réalisée

– en cas d'anomalie, soit dans le sous-système 1, soit dans le sous-système 2 (car la combinaison des sous-systèmes 4 et 5 est capable d'assurer la fonction de sécurité); ou

– en cas d'anomalie soit dans le sous-système 4, soit dans le sous-système 5 (car la combinaison des sous-systèmes 1 et 2 est capable d'assurer la fonction de sécurité).

Chaque sous-système est conforme aux prescriptions des tableaux 2 et 3 de la manière suivante:

– le sous-système 1 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL3, pour une proportion de défaillances en sécurité spécifique;

– le sous-système 2 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL2, pour une proportion de défaillances en sécurité spécifique;

– le sous-système 3 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL2, pour une proportion de défaillances en sécurité spécifique;

– le sous-système 4 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL2, pour une proportion de défaillances en sécurité spécifique;

– le sous-système 5 est conforme aux prescriptions de tolérance aux anomalies matérielles d'un niveau SIL1, pour une proportion de défaillances en sécurité spécifique;

La détermination du niveau d'intégrité de sécurité maximal du matériel qui peut être annoncée, pour le système E/E/PE relatif à la sécurité complet, exécutant la fonction de sécurité considérée, est détaillée dans les étapes suivantes.

a) En combinant les sous-systèmes 1 et 2: La tolérance aux anomalies matérielles et la proportion de défaillances en sécurité réalisées par la combinaison des sous-systèmes 1 et 2 (chacun étant séparément conforme aux prescriptions des niveaux SIL3 et SIL2 respectivement) satisfait aux prescriptions du niveau SIL2 (déterminé par le sous-système 2).

b) En combinant les sous-systèmes 4 et 5: La tolérance aux anomalies matérielles et proportion de défaillances en sécurité réalisées par la combinaison des sous-systèmes 4 et 5 (chacun étant séparément conforme aux prescriptions des niveaux SIL2 et SIL1 respectivement) satisfait aux prescriptions du niveau SIL1 (déterminé par le sous-système 5).

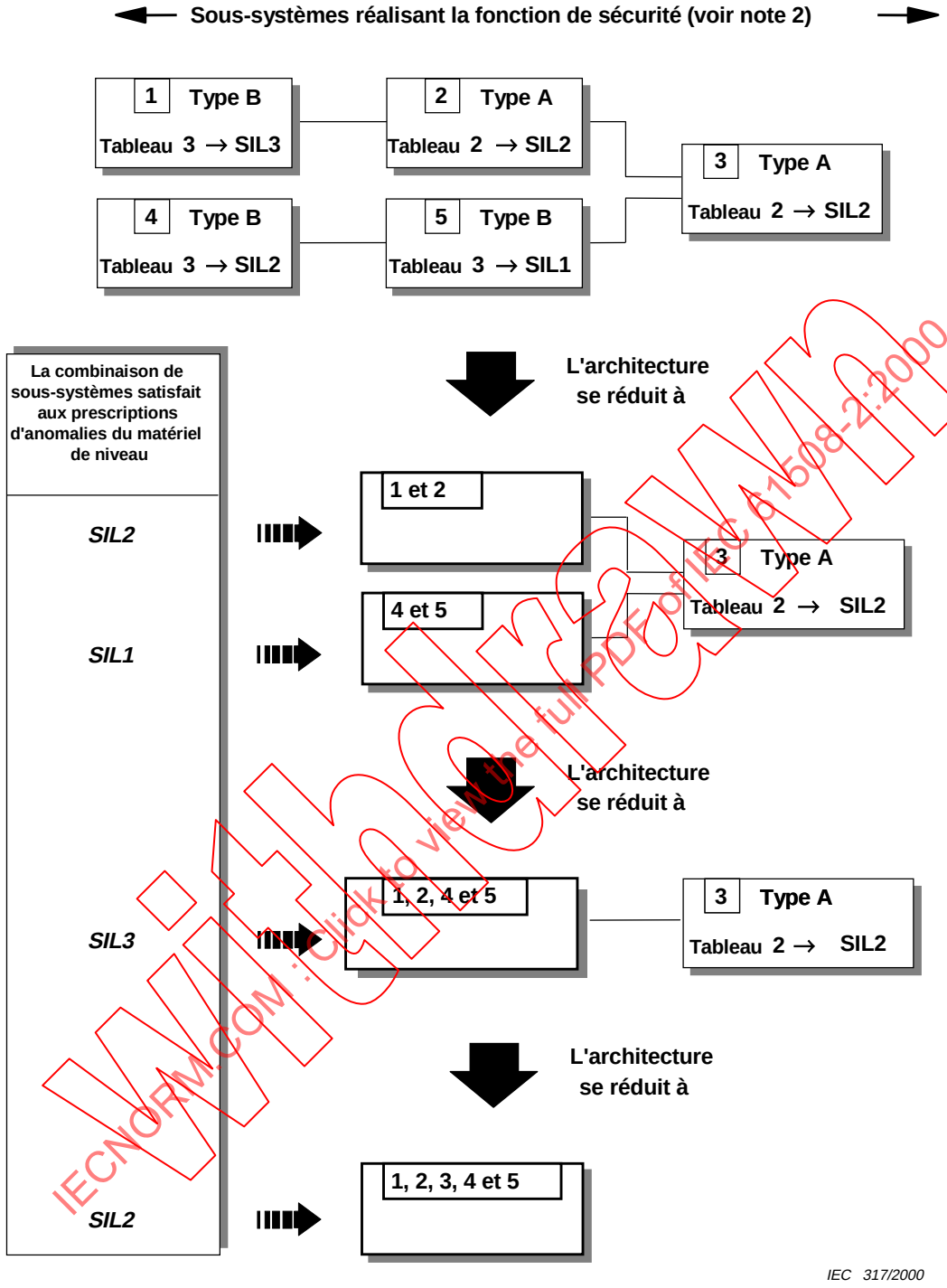
c) En outre, en associant la combinaison des sous-systèmes 1 et 2 avec la combinaison des sous-systèmes 4 et 5: Le niveau d'intégrité de sécurité du matériel, eu égard à la tolérance aux anomalies matérielles, de la combinaison des sous-systèmes 1, 2, 4 et 5 est déterminé de la manière suivante:

   – en décidant de la combinaison de sous-systèmes (c'est-à-dire la combinaison des sous-systèmes 1 et 2 ou la combinaison des sous-systèmes 4 et 5) qui a réalisé le niveau d'intégrité de sécurité du matériel revendicable le plus élevé (en termes de satisfaction aux tolérances aux anomalies matérielles); et

   – en analysant l'effet de l'autre combinaison de sous-systèmes sur la tolérance aux anomalies matérielles pour la combinaison de sous-systèmes 1, 2, 4 et 5.

   Dans cet exemple, la combinaison des sous-systèmes 1 et 2 a une revendication admissible maximale de niveau SIL2 (voir a) ci-dessus) tandis que la combinaison des sous-systèmes 4 et 5 a une revendication admissible maximale de niveau SIL1 (voir b) ci-dessus). Cependant, en cas d'anomalie dans la combinaison des sous-systèmes 1 et 2, la fonction de sécurité pourrait être assurée par la combinaison des sous-systèmes 4 et 5. Pour tenir compte de cet effet, la tolérance aux anomalies du matériel réalisée par la combinaison des sous-systèmes 1 et 2 est augmentée de 1. En augmentant de 1 la tolérance aux anomalies du matériel, on augmente également de 1 le niveau d'intégrité de sécurité du matériel (voir tableaux 2 et 3). En conséquence, eu égard à la tolérance aux anomalies du matériel et à la proportion de défaillances en sécurité, la combinaison des sous-systèmes 1, 2, 4 et 5 a un niveau d'intégrité de sécurité du matériel revendicable maximal SIL3 (c'est-à-dire le niveau d'intégrité de sécurité du matériel réalisé par la combinaison des sous-systèmes 1 et 2 (qui était SIL2) plus 1).

d) Le système E/E/PE relatif à la sécurité complet: Le niveau d'intégrité de sécurité du matériel, eu égard à la tolérance aux anomalies du matériel, qui peut être annoncé pour le système E/E/PE relatif à la sécurité complet mettant en œuvre la fonction de sécurité considérée, est déterminé en analysant la combinaison des sous-systèmes 1, 2, 4 et 5 (qui a satisfait aux prescriptions de tolérance aux anomalies de niveau SIL3 (voir c)) ainsi que le sous-système 3 (qui a satisfait aux prescriptions de tolérance aux anomalies de niveau SIL2). C'est le sous-système qui a satisfait aux prescriptions de niveau d'intégrité de sécurité du matériel le plus bas, dans le cas présent, le sous-système 3, qui détermine le niveau d'intégrité de sécurité maximum du matériel pour l'ensemble du système E/E/PE relatif à la sécurité. Par conséquent, dans cet exemple, le niveau d'intégrité de sécurité maximum du matériel, eu égard à la tolérance aux anomalies du matériel, qui a été obtenu pour le système E/E/PE relatif à la sécurité mettant en œuvre la fonction de sécurité, est le niveau SIL2.



NOTE 1 Les sous-systèmes 1 et 2 ainsi que les sous-systèmes 4 et 5 ont la même fonctionnalité en termes de réalisation de la fonction de sécurité et contribuent indépendamment à fournir des données au sous-système 3.

NOTE 2 Les sous-systèmes réalisant la fonction de sécurité s'étendront à l'ensemble du système E/E/PE en termes de couverture, des capteurs aux actionneurs.

NOTE 3 Pour plus de détails quant à l'interprétation de cette figure, voir l'exemple en 7.4.3.1.6.

Figure 6 – Exemple de limitation de l'intégrité de sécurité du matériel pour une fonction de sécurité à plusieurs canaux

7.4.3.2 Prescriptions relatives à l'estimation de la probabilité de défaillance des fonctions de sécurité due à des défaillances aléatoires du matériel

7.4.3.2.1 La probabilité de défaillance de chaque fonction de sécurité, due à des défaillances aléatoires du matériel, calculée conformément à 7.4.3.2.2 et 7.4.3.2.3, doit être inférieure ou égale à la mesure cible de défaillance telle que spécifiée dans la spécification des prescriptions de sécurité (voir 7.2.3.2).

NOTE 1 Dans le cas d'une fonction de sécurité en mode demande faible, la mesure cible de défaillance est exprimée en termes d'une probabilité moyenne de défaillance à exécuter, lors d'une demande, la fonction pour laquelle elle est conçue, déterminée par le niveau d'intégrité de sécurité de la fonction de sécurité (voir CEI 61508-1, tableau 2), sauf s'il existe une prescription, dans la spécification des prescriptions d'intégrité de sécurité E/E/PES (voir 7.2.3.2), imposant à la fonction de sécurité de remplir plutôt une mesure cible de défaillance qu'un SIL spécifique. Par exemple, lorsqu'une mesure cible de défaillance de $1,5 \times 10^{-6}$ (probabilité de défaillance lors d'une demande) est spécifiée afin de tenir la réduction nécessaire de risque, il est nécessaire que la probabilité de défaillance de la fonction de sécurité, due aux défaillances aléatoires du matériel, soit inférieure ou égale à $1,5 \times 10^{-6}$ défaillances dangereuses par heure.

NOTE 2 Dans le cas d'une fonction de sécurité exploitée en mode demande élevée/continu, la mesure cible de défaillance est exprimée en termes de la probabilité moyenne d'apparition d'une défaillance dangereuse par heure, déterminée par le niveau d'intégrité de sécurité de la fonction de sécurité (voir CEI 61508-1, tableau 3), sauf s'il existe une prescription, dans la spécification des prescriptions d'intégrité de sécurité E/E/PES (voir 7.2.3.2), imposant à la fonction de sécurité de remplir plutôt une mesure cible de défaillance qu'un SIL spécifique. Par exemple, lorsqu'une mesure cible de défaillance de $1,5 \times 10^{-6}$ (probabilité de défaillance lors d'une demande) est spécifiée afin de tenir la réduction nécessaire de risque, il est nécessaire que la probabilité de défaillance de la fonction de sécurité, due aux défaillances aléatoires du matériel, soit inférieure ou égale à $1,5 \times 10^{-6}$ défaillances dangereuses par heure.

NOTE 3 Afin de démontrer que cela a été réalisé, il est nécessaire d'effectuer une prédiction de fiabilité pour la fonction de sécurité correspondante, en utilisant la technique appropriée (voir 7.4.3.2.2), et de comparer le résultat à la mesure cible de défaillance de la prescription d'intégrité de sécurité, pour la fonction de sécurité considérée (voir CEI 61508-1, tableaux 2 et 3).

7.4.3.2.2 La probabilité de défaillance de chaque fonction de sécurité, due à des défaillance aléatoires du matériel, doit être estimée en prenant en compte

a) l'architecture du système E/E/PE relatif à la sécurité, puisqu'elle se rapporte à chacune des fonctions de sécurité considérée;

   NOTE 1 Ceci implique de décider quels sont les modes de défaillance des sous-systèmes qui sont en configuration série (c'est-à-dire que toute défaillance provoque la défaillance de la fonction de sécurité correspondante) 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).

b) le taux de défaillance estimé de chaque sous-système, dans tous les modes susceptibles de provoquer une défaillance dangereuse du système E/E/PE relatif à la sécurité, les défaillances étant détectées par des tests de diagnostic (voir 7.4.7.3 et 7.4.7.4);

c) le taux de défaillance estimé de chaque sous-système, dans tous les modes susceptibles de provoquer une défaillance dangereuse du système E/E/PE relatif à la sécurité, les défaillance n'étant pas détectées par des tests de diagnostic (voir 7.4.7.3 et 7.4.7.4);

d) la susceptibilité aux défaillances de cause commune du système E/E/PE relatif à la sécurité (voir les notes 2 et 11);

   NOTE 2 Par exemple, voir CEI 61508-6, annexe D.

e) la couverture de diagnostic des tests périodiques de diagnostic (déterminée conformément à l'annexe C), et l'intervalle correspondant des tests de diagnostic;

   NOTE 3 L'intervalle des tests de diagnostic et le temps de réparation qui en résulte constituent, ensemble, le temps moyen jusqu'à rétablissement qui est pris en compte dans le modèle de fiabilité. De même, dans le cas d'un système E/E/PE relatif à la sécurité exploité en mode demande élevée/continu pour lequel toute défaillance dangereuse d'un canal entraîne une défaillance dangereuse du système E/E/PE relatif à la sécurité, l'intervalle des tests de diagnostic est pris en compte directement (c'est-à-dire qu'il s'ajoute au temps jusqu'à rétablissement) dans le modèle de fiabilité, s'il n'est pas d'un ordre de grandeur inférieur au taux de demande moyen (voir 7.4.3.2.5).

   NOTE 4 En déterminant l'intervalle des tests de diagnostic, les intervalles entre chacun des tests qui contribuent à la couverture de diagnostic sont pris en compte.

f) les intervalles de temps auxquels des tests périodiques sont effectués pour révéler les anomalies dangereuses qui ne sont pas détectées par les tests de diagnostic;

g) les temps de réparation correspondant aux défaillances détectées;

NOTE 5 Le temps de réparation constitue une partie du temps moyen de rétablissement (voir le VEI 191-13-08), qui doit également comprendre le temps passé à la détection de la défaillance et toute période de temps pendant laquelle la réparation n'est pas possible (voir la CEI 61508-6, annexe B qui donne un exemple de la manière suivant laquelle le temps moyen jusqu'à rétablissement peut être utilisé pour calculer la probabilité d'une défaillance). Dans les situations où la réparation ne peut être faite que dans une période de temps spécifique, par exemple lorsque l'EUC est arrêtée et dans un état sûr, il est particulièrement important que la période de temps pendant laquelle aucune réparation n'est possible soit bien prise en compte, particulièrement lorsque cette période de temps est importante.

h) la probabilité d'une défaillance non détectée d'un processus quelconque de communication de données (voir la note 11 et 7.4.8.1).

NOTE 6 La CEI 61508-6, annexe B, décrit une approche simplifiée qui peut être utilisée pour estimer la probabilité d'une défaillance dangereuse d'une fonction de sécurité due à une défaillance aléatoire du matériel, afin de déterminer qu'une architecture remplit la mesure cible de défaillance prescrite.

NOTE 7 La CEI 61508-6, annexe A, A.2 donne une vue d'ensemble des étapes nécessaires lors de la réalisation de l'intégrité de sécurité du matériel prescrite, et présente la manière suivant laquelle le présent paragraphe est en rapport avec d'autres prescriptions de la présente norme.

NOTE 8 Il est nécessaire de quantifier séparément, pour chaque fonction, la fiabilité du système E/E/PE relatif à la sécurité car différents modes de défaillance des composants s'appliquent et l'architecture des systèmes E/E/PE relatifs à la sécurité (en termes de redondance) peut également varier.

NOTE 9 Un certain nombre de méthodes de modélisation sont disponibles et il appartient à l'analyste de déterminer la plus appropriée, en fonction des cas. Les méthodes disponibles sont:

– l'analyse cause-conséquence (voir B.6.6.2 de la CEI 61508-7)

– l'analyse par arbre de panne (voir B.6.6.5 de la CEI 61508-7)

– les modèles de Markov (voir C.6.4 de la CEI 61508-7)

– les diagrammes de fiabilité (voir C.6.5 de la CEI 61508-7)

NOTE 10 Le temps moyen jusqu'à rétablissement (voir VEI 191-13-08) pris en compte dans le modèle de fiabilité nécessite de tenir compte de l'intervalle des tests de diagnostic, le temps de réparation et tous les autres délais préalables au rétablissement.

NOTE 11 Les défaillances de cause commune et celles dues aux processus de communication des données peuvent résulter d'effets autres que les défaillances des composants matériels (par exemple, perturbation électromagnétique, erreurs de décodage, etc.). Toutefois, de telles défaillances sont considérées, pour les besoins de la présente norme, comme des défaillances aléatoires du matériel.

7.4.3.2.3 L'intervalle des tests de diagnostic, pour chaque sous-système ayant une tolérance aux anomalies du matériel supérieure à zéro, doit être tel que le système E/E/PE relatif à la sécurité puisse remplir la prescription de probabilité de défaillance aléatoire du matériel (voir 7.4.3.2.1).

7.4.3.2.4 L'intervalle des tests de diagnostic de chaque sous-système ayant une tolérance aux anomalies du matériel nulle, dont la fonction de sécurité est entièrement dépendante (voir note 1), et qui réalise seulement des fonctions de sécurité exploitées en mode de faible sollicitation, doit être tel que le système E/E/PE relatif à la sécurité puisse remplir la prescription de probabilité de défaillance aléatoire du matériel (voir 7.4.3.2.1).

NOTE 1 On considère qu'une fonction de sécurité dépend entièrement d'un sous-système si la défaillance du sous-système provoque la défaillance de la fonction de sécurité dans le système E/E/PE relatif à la sécurité considéré, et que la fonction de sécurité n'a pas également été allouée à un autre système relatif à la sécurité (voir 7.6 de la CEI 61508-1).

NOTE 2 Lorsqu'il est possible qu'une certaine combinaison des états de sortie d'un sous-système provoque directement un événement dangereux (tel que déterminé par l'analyse de dangers et de risques, voir 7.4.2.10 de la CEI 61508-1) et lorsque la combinaison des états de sortie en présence d'une anomalie dans le sous-système ne peut pas être déterminée (par exemple dans le cas de sous-systèmes de type B), alors il est nécessaire de considérer que la détection d'anomalies dangereuses dans le sous-système est une fonction de sécurité exploitée en mode de demande élevée/continu et les prescriptions de 7.4.6.3 et 7.4.3.2.5 sont applicables.

7.4.3.2.5 L'intervalle des tests de diagnostic de chaque sous-système ayant une tolérance aux anomalies du matériel nulle, dont la fonction de sécurité est entièrement dépendante (voir la note 1) et qui réalise une fonction de sécurité exploitée en mode de demande élevée/continue (voir la note 2), doit être tel que la somme de l'intervalle des tests de diagnostic et du temps nécessaire à l'exécution de l'action spécifiée (réaction à l'anomalie) pour réaliser ou maintenir un état sûr (voir 7.2.3.1 g)) est inférieure au temps de sécurité du processus. Le temps de sécurité du processus est défini comme la période de temps entre l'apparition d'une défaillance dans l'EUC ou dans le système de commande de l'EUC (cette défaillance étant susceptible de donner lieu à un événement dangereux) et l'apparition de l'événement dangereux lorsque la fonction de sécurité n'est pas mise en œuvre.

NOTE 1 On considère qu'une fonction de sécurité dépend entièrement d'un sous-système si la défaillance du sous-système provoque la défaillance de la fonction de sécurité dans le système E/E/PE relatif à la sécurité considéré, et que la fonction de sécurité n'a pas également été allouée à un autre système relatif à la sécurité (voir 7.6 de la CEI 61508-1).

NOTE 2 Dans le cas d'un sous-système réalisant une fonction de sécurité particulière pour lequel le rapport du taux des tests de diagnostic au taux de demande dépasse 100, le sous-système peut être traité comme s'il réalisait une fonction de sécurité en mode demande faible (voir 7.4.3.2.4), pourvu que la fonction de sécurité n'empêche pas la combinaison d'états de sortie conduisant à un événement dangereux (voir la note 3).

NOTE 3 Si la fonction de sécurité consiste à empêcher une combinaison particulière d'états de sortie pouvant être à l'origine d'un événement dangereux, il est alors toujours nécessaire de considérer qu'une telle fonction de sécurité est exploitée en mode demande élevée/continu (voir 7.4.2.12).

7.4.3.2.6 Si, pour une conception particulière, la mesure cible de défaillance de la prescription d'intégrité de sécurité de la fonction de sécurité considérée n'est pas réalisée, alors

– déterminer les composants sous-systèmes et/ou paramètres critiques;
– évaluer l'effet des mesures possibles d'amélioration sur les composants, sous-systèmes et/ou paramètres critiques (par exemple, composants plus fiables, défenses supplémentaires contre les défaillances de mode commun, couverture de diagnostic accrue, redondance accrue, intervalle des tests périodiques réduit, etc.);
– choisir et mettre en œuvre les améliorations applicables;
– répéter les étapes nécessaires pour déterminer la nouvelle probabilité de défaillance du matériel.

7.4.4 Prescriptions d'évitement des défaillances

NOTE Les articles 7.4.4.1 à 7.4.4.6 ne sont pas applicables dans le cas d'un sous-système qui remplit les prescriptions permettant de le considérer comme «validé en utilisation» (voir 7.4.7.6 à 7.4.7.12).

7.4.4.1 Un ensemble convenable de techniques et de mesures doit être conçu et utilisé pour éviter l'introduction d'anomalies pendant la conception et le développement E/E/PES du système E/E/PE relatif à la sécurité (voir tableau B.2).

7.4.4.2 Conformément au niveau d'intégrité de sécurité exigé, 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 des sous-systèmes,
   – du séquencement et des informations temporelles,
   – de la simultanéité et de la synchronisation d'exécution;
c) une documentation claire et précise ainsi que la communication d'informations;
d) la vérification et la validation.

7.4.4.3 Les prescriptions de maintenance destinées à assurer le maintien de l'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité au niveau requis, doivent être formalisées pendant l'étape de conception.

7.4.4.4 Le cas échéant, des outils de tests automatiques et des outils de développement intégrés doivent être utilisés.

7.4.4.5 Pendant la conception, des tests d'intégration E/E/PES doivent être planifiés. La documentation du programme de test doit comprendre

a) les types de tests à réaliser ainsi que les procédures à suivre;

b) l'environnement, les outils, la configuration et les programmes de test;

c) les critères d'acceptation/de rejet des tests.

7.4.4.6 Pendant la conception, il faut séparer les activités qui peuvent être réalisées dans les locaux du développeur et celles qui nécessitent un accès au site de l'utilisateur.

7.4.5 Prescriptions pour la maîtrise des anomalies systématiques

NOTE Les articles 7.4.5.1 à 7.4.5.3 ne sont pas applicables dans le cas d'un sous-système qui remplit les prescriptions permettant de le considérer comme «validé en utilisation» (voir 7.4.7.6 à 7.4.7.12).

7.4.5.1 Afin de maîtriser les anomalies systématiques, la conception E/E/PES doit avoir des caractéristiques de conception telles que les systèmes E/E/PE relatifs à la sécurité soient tolérants

a) à d'éventuelles anomalies de conception résiduelles du matériel, sauf si l'éventualité d'anomalies de conception du matériel peut être exclue (voir tableau A.16);

b) aux contraintes environnementales, y compris les perturbations électromagnétiques (voir le tableau A.17);

c) aux erreurs imputables à l'opérateur de l'EUC (voir tableau A.18);

d) à une éventuelle anomalie de conception résiduelle du logiciel (voir 7.4.3 de la CEI 61508-3 ainsi que le tableau correspondant);

e) aux erreurs et autres effets provenant d'un processus de communication de données (voir 7.4.8).

7.4.5.2 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 finaux relatifs à la sécurité.

7.4.5.3 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. La conception de toutes les interfaces doit être fondée sur de bonnes pratiques en termes de facteur humain et doit s'accommoder du niveau probable de formation et de connaissances des opérateurs comme, par exemple, dans le cas de systèmes E/E/PE relatifs à la sécurité de série destinés au grand public, où l'opérateur est un membre du public.

NOTE 1 Il est recommandé que l'objectif de la conception soit de prévenir 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 soit 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.

7.4.6 Prescriptions comportementales du système, lors de la détection d'une anomalie

7.4.6.1 La détection d'une anomalie dangereuse (par les tests de diagnostic, les tests périodiques ou tout autre moyen) dans un sous-système qui a une tolérance aux anomalies du matériel supérieure à zéro, doit déclencher

a) soit une action spécifiée pour atteindre ou maintenir un état sûr (voir note), ou

b) soit 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 durant le temps moyen jusqu'à rétablissement (MTTR) pris comme hypothèse dans le calcul de la probabilité de défaillance aléatoire du matériel (voir 7.4.3.2.2), une action spécifiée doit avoir lieu afin d'atteindre ou maintenir un état sûr (voir note).

NOTE L'action spécifiée (réaction à l'anomalie) prescrite pour atteindre ou maintenir un état sûr doit être spécifiée dans les prescriptions de sécurité E/E/PES (voir 7.2.3.1). Elle peut consister, par exemple, en l'arrêt de sécurité de l'EUC, ou de la partie de l'EUC qui repose, en ce qui concerne la réduction de risque, sur le sous-système qui présente une anomalie.

7.4.6.2 La détection d'une anomalie dangereuse (par les tests de diagnostic, les tests périodiques ou tout autre moyen) dans un sous-système qui a une tolérance aux anomalies du matériel nulle, et dont dépend entièrement une fonction de sécurité (voir note 1), doit dans le cas où ce sous-système est utilisé uniquement par une (des) fonction(s) de sécurité exploitée(s) en mode demande faible, déclencher

a) soit une action spécifiée pour atteindre ou maintenir un état sûr, ou

b) soit la réparation du sous-système présentant une défaillance, dans le délai imparti par le temps moyen jusqu'à rétablissement pris en hypothèse lors du calcul de la probabilité de défaillance aléatoire du matériel (voir 7.4.3.2.2). Pendant ce délai, la sécurité de l'EUC doit être assurée par des mesures et contraintes supplémentaires. La réduction de risque procurée par ces mesures et contraintes doit être au moins égale à la réduction de risque 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 de l'EUC (voir 7.6). Si la réparation n'est pas entreprise dans le délai imparti par le temps moyen jusqu'à rétablissement (MTTR), alors une action spécifiée doit être accomplie pour atteindre ou maintenir un état sûr (voir la note 2).

NOTE 1 On considère qu'une fonction de sécurité dépend entièrement d'un sous-système si la défaillance du sous-système provoque la défaillance de la fonction de sécurité dans le système E/E/PE relatif à la sécurité considéré, et que la fonction de sécurité n'a pas également été allouée à un autre système relatif à la sécurité (voir 7.6 de la CEI 61508-1).

NOTE 2 L'action spécifiée (réaction à l'anomalie) prescrite pour atteindre ou maintenir un état sûr doit être spécifiée dans les prescriptions de sécurité E/E/PES (voir 7.2.3.1). Elle peut consister, par exemple, en l'arrêt de sécurité de l'EUC, ou de la partie de l'EUC qui repose, en ce qui concerne la réduction de risque, sur le sous-système qui présente une anomalie.

7.4.6.3 La détection d'une anomalie dangereuse (par les tests de diagnostic, les tests périodiques ou tout autre moyen) dans un sous-système ayant une tolérance aux anomalies du matériel nulle, et dont dépend entièrement une fonction de sécurité (voir note 1), doit, dans le cas d'un sous-système réalisant une (des) fonction(s) de sécurité exploitée(s) en mode de demande élevée/continue (voir notes 2 et 3), déclencher une action spécifiée pour atteindre ou maintenir un état sûr (voir note 3).

NOTE 1 On considère qu'une fonction de sécurité dépend entièrement d'un sous-système si la défaillance du sous-système provoque la défaillance de la fonction de sécurité dans le système E/E/PE relatif à la sécurité considéré, et que la fonction de sécurité n'a pas également été allouée à un autre système relatif à la sécurité (voir 7.6 de la CEI 61508-1).

NOTE 2 Lorsqu'il est possible qu'une certaine combinaison des états de sortie d'un sous-système provoque directement un événement dangereux (tel que déterminé par l'analyse de dangers et de risques, voir 7.4.2.12) et lorsque la combinaison des états de sortie en présence d'une anomalie dans le sous-système ne peut pas être déterminée (par exemple dans le cas de sous-systèmes de type B), alors il est nécessaire de considérer que la détection d'anomalies dangereuses dans le sous-système est une fonction de sécurité exploitée en mode de demande élevée/continue et les prescriptions de 7.4.6.3 et 7.4.3.2.5 sont applicables.

NOTE 3 L'action spécifiée (réaction à l'anomalie) prescrite pour atteindre ou maintenir un état sûr doit être spécifiée dans les prescriptions de sécurité E/E/PES (voir 7.2.3.1). Elle peut consister, par exemple, en l'arrêt de sécurité de l'EUC, ou de la partie de l'EUC qui repose, en ce qui concerne la réduction de risque, sur le sous-système qui présente une anomalie.

7.4.7 Prescriptions de réalisation des E/E/PES

7.4.7.1 Les systèmes E/E/PE relatifs à la sécurité doivent être réalisés conformément à la conception E/E/PES.

7.4.7.2 Tous les sous-systèmes qui sont utilisés par une fonction de sécurité au moins doivent être identifiés et documentés en tant que sous-systèmes relatifs à la sécurité.

7.4.7.3 Les informations suivantes doivent être disponibles pour chaque sous-système relatif à la sécurité (voir également 7.4.7.4):

a) spécification fonctionnelle des fonctions et interfaces du sous-système qui peuvent être utilisées par des fonctions de sécurité;

b) taux de défaillance estimés (dus aux défaillances aléatoires du matériel) dans tous les modes susceptibles de provoquer une défaillance dangereuse du système E/E/PE relatif à la sécurité qui sont détectés par les tests de diagnostic (voir 7.4.7.4);

c) taux de défaillance estimés (dus aux défaillances aléatoires du matériel) dans tous les modes susceptibles de provoquer une défaillance dangereuse du système E/E/PE relatif à la sécurité qui ne sont pas détectés par les tests de diagnostic (voir 7.4.7.4);

d) les limitations concernant l'environnement du sous-système qu'il convient d'observer afin de maintenir la validité des taux de défaillance estimés dus à des défaillances aléatoires du matériel;

e) les limitations concernant la durée de vie du sous-système qu'il convient de ne pas dépasser afin de maintenir la validité des taux de défaillance estimés dus à des défaillances aléatoires du matériel;

f) les tests périodiques et/ou les prescriptions de maintenance;

g) la couverture de diagnostic déduite conformément à l'annexe C (lorsqu'elle est prescrite, voir la note 1);

h) l'intervalle des tests de diagnostic (lorsque prescrit, voir la note 1);

NOTE 1 Les alinéas g) à h) ci-dessus se rapportent aux tests de diagnostic qui sont internes au sous-système. Les informations correspondantes sont prescrites uniquement lorsque dans le modèle de fiabilité du système E/E/PE relatif à la sécurité, des tests de diagnostic sont annoncés comme étant exécutés dans le sous-système considéré (voir 7.4.3.2.2).

i) les informations supplémentaires (par exemple, les temps de réparation) qui sont nécessaires pour déduire un temps de rétablissement (MTTR) à la suite de la détection d'une anomalie par les diagnostics;

NOTE 2 Les alinéas b) à i) sont nécessaires pour permettre l'estimation de la probabilité de défaillance lors d'une sollicitation, ou de la probabilité de défaillance par heure, de la fonction de sécurité (voir 7.4.3.2.2).

NOTE 3 Les alinéas b), c), g), h) et i) sont prescrits uniquement en tant que paramètres distincts pour les sous-systèmes tels que capteurs et actionneurs qui peuvent être combinés dans des architectures redondantes afin d'améliorer l'intégrité de sécurité du matériel. Pour des entités telles que des unités logiques qui ne seront pas elles-mêmes combinées dans des architectures redondantes du système E/E/PE relatif à la sécurité, il est acceptable que la performance soit spécifiée en termes de probabilité de défaillance à la sollicitation, ou de probabilité de défaillance par heure, en prenant en compte les alinéas b), c), g), h) et i). Pour de telles entités, il est également nécessaire d'établir l'intervalle des tests périodiques pour les défaillances non détectées par les tests de diagnostic.

j) les informations nécessaires pour permettre de déduire la proportion de défaillances en sécurité (SFF) du sous-système telle qu'appliquée au système E/E/PE relatif à la sécurité, déterminée conformément à l'annexe C;

k) la tolérance aux anomalies du matériel, pour le sous-système;

NOTE 4 Les alinéas j) et k) sont nécessaires pour déterminer le niveau d'intégrité de sécurité le plus élevé qui peut être annoncé pour une fonction de sécurité, en prenant en compte les contraintes architecturales (voir 7.4.3.1).

l) les limitations concernant l'application du sous-système qu'il convient d'observer afin d'éviter les défaillances systématiques;

m) le niveau d'intégrité le plus élevé qui peut être annoncé pour une fonction de sécurité qui utilise le sous-système, sur la base

- de mesures et techniques utilisées pour empêcher l'introduction d'anomalies systématiques lors de la conception et de la réalisation du matériel et du logiciel du sous-système (voir 7.4.4.1 et 7.4 de la CEI 61508-3),
- des caractéristiques de conception qui rendent le sous-système tolérant aux anomalies systématiques (voir 7.4.5.1);

NOTE 5 Ceci n'est pas prescrit dans le cas des sous-systèmes qui sont considérés comme ayant été validés en utilisation (voir 7.4.7.5).

n) les informations nécessaires afin d'identifier les configurations du matériel et du logiciel 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;

o) la preuve documentée suivant laquelle le sous-système a été validé.

7.4.7.4 Les taux de défaillance estimés, dus à des défaillances aléatoires du matériel, pour les sous-systèmes (voir 7.4.7.3 b) et c)), peuvent être déterminés

a) soit par une analyse des modes de défaillance et de leurs effets de la conception utilisant des taux de défaillance de composants provenant d'une origine industrielle reconnue,

NOTE 1 Il convient que toutes les données utilisée relatives aux défaillances aient un niveau de confiance d'au moins 70 %. La détermination statistique du niveau de confiance est définie dans l'IEEE 352. Un terme équivalent, niveau de signification, est utilisé dans la CEI 61164.

NOTE 2 Lorsque des données relatives aux défaillances spécifiques à la localisation du matériel sont disponibles, il est préférable de les utiliser. Si tel n'est pas le cas, il est possible d'utiliser des données génériques.

NOTE 3 Bien qu'un taux de défaillance constant soit pris comme hypothèse pour la plupart des estimations statistiques, cela s'applique seulement si la durée de vie utile des composants n'est pas dépassée. Au delà de leur durée de vie utile (c'est-à-dire lorsque la probabilité de défaillance s'accroît en fonction du temps), les résultats de la plupart des méthodes de calcul probabilistes sont moins significatifs. C'est pourquoi il convient que toute estimation probabiliste inclue une spécification de la durée de vie utile des composants. La durée de vie utile dépend fortement du composant 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 permis de montrer que la durée de vie utile se situe souvent entre 8 et 12 ans. Elle peut toutefois être significativement moindre si les composants sont utilisés dans des conditions proches de leurs limites de spécification. Les composants ayant des durées de vie utile plus longues ont tendance à être considérablement plus chers.

ou

b) soit par expérience d'une utilisation antérieure du sous-système dans un environnement similaire (voir 7.4.7.9).

7.4.7.5 Dans le cas d'un sous-système considéré comme ayant été validé en utilisation (voir 7.4.7.6), les informations concernant les techniques et mesures pour la prévention et la maîtrise des anomalies systématiques (voir 7.4.7.3 m)) ne sont pas prescrites.

7.4.7.6 Un sous-système développé antérieurement doit être considéré comme ayant été validé en utilisation lorsqu'il a une fonctionnalité clairement restreinte et lorsqu'il existe une preuve documentaire appropriée, basée sur l'utilisation antérieure d'une configuration spécifique du sous-système (durant laquelle tous les temps de défaillance ont été formellement enregistrés, voir 7.4.7.10) qui prend en compte toutes les analyses ou tests supplémentaires, selon prescription (voir 7.4.7.8). La preuve documentaire doit démontrer que la vraisemblance d'une défaillance du sous-système (due à une défaillance aléatoire du matériel et aux anomalies systématiques), dans le système E/E/PE relatif à la sécurité, est suffisamment faible pour que le(s) niveau(x) d'intégrité de sécurité prescrit(s), pour la (des) fonction(s) de sécurité qui utilise(nt) le sous-système, soit (soient) atteint(s).

7.4.7.7 La preuve documentaire prescrite en 7.4.7.6 doit démontrer que les conditions de l'utilisation antérieure (voir la note) du sous-système spécifique sont les mêmes, ou suffisamment proches, que celles que rencontre le sous-système dans le système E/E/PE relatif à la sécurité, afin de déterminer que la vraisemblance de toute anomalie systématique non révélée est suffisamment faible pour que le(s) niveau(x) d'intégrité de sécurité prescrit(s), pour la fonction de sécurité qui utilise le sous-système, soit (soient) atteint(s).

NOTE Les conditions d'utilisation (profil d'exploitation) comprennent tous les facteurs qui peuvent influencer la probabilité d'anomalies systématiques dans le matériel et le logiciel du sous-système. 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.

7.4.7.8 Lorsqu'il existe une différence entre les conditions de l'utilisation antérieure et celles que rencontrera le sous-système dans le système E/E/PE relatif à la sécurité, elle doit être identifiée et une démonstration explicite doit être effectuée, sur la base d'une combinaison de méthodes analytiques appropriées et de tests, afin de déterminer que la probabilité d'une anomalie systématique non révélée est suffisamment faible pour que le(s) niveau(x) d'intégrité de sécurité de la (des) fonction(s) de sécurité qui utilise(nt) ce sous-système soit (soient) atteint(s).

7.4.7.9 La preuve documentaire prescrite en 7.4.7.6 doit établir que l'étendue de l'utilisation antérieure (en termes d'heures d'exploitation) de la configuration spécifique du sous-système est suffisante pour appuyer les taux de défaillance annoncés sur une base statistique. A minima, un temps d'exploitation suffisant est nécessaire pour établir que les données concernant les taux de défaillance annoncés ont une limite inférieure de confiance, monolatérale, à 70 % (voir la CEI 61508-7, annexe D et l'IEEE 352). Un temps d'exploitation inférieur à un an, pour un sous-système individuel, ne doit pas être pris en compte, dans le temps d'exploitation total, par l'analyse statistique (voir note).

NOTE Le temps nécessaire, en termes d'heures d'exploitation, prescrit pour obtenir les taux de défaillance annoncés peut résulter de l'exploitation d'un certain nombre de sous-systèmes identiques, pourvu que les défaillances de tous les sous-systèmes aient été effectivement détectées et rapportées (voir 7.4.7.10). Si, par exemple, 100 sous-systèmes sont exempts d'anomalie pendant 10 000 h, le temps d'exploitation total sans défaillance est considéré égal à 1 000 000 h. Dans ce cas, chaque sous-système a été utilisé sur l'ensemble d'une année et l'ensemble des heures écoulées en exploitation est pris en compte dans la durée d'exploitation totale.

7.4.7.10 Seules les utilisations antérieures pour lesquelles toutes les défaillances du sous-système ont été effectivement détectées et enregistrées (par exemple, lorsque les données concernant les défaillances ont été recueillies conformément aux recommandations de la CEI 60300-3-2) doivent être prises en compte en déterminant si les prescriptions ci-dessus (7.4.7.6 à 7.4.7.9) sont remplies.

7.4.7.11 Les facteurs suivants doivent être pris en compte en déterminant si les prescriptions ci-dessus (7.4.7.6 à 7.4.7.9) sont remplies, tant en termes de couverture que de degré de détail de l'information disponible (voir également 4.1 de la CEI 61508-1):

a) la complexité du sous-système;

b) la contribution du sous-système à la réduction de risque;

c) les conséquences associées à une défaillance du sous-système;

d) l'aspect innovateur de la conception.

7.4.7.12 Il convient que l'application d'un sous-système relatif à la sécurité validé en utilisation, dans le système E/E/PE relatif à la sécurité soit restreint aux fonctions et interfaces du sous-système qui remplissent les prescriptions appropriées (voir 7.4.7.6 à 7.4.7.10).

NOTE Les mesures 7.4.7.4 à 7.4.7.12 sont également applicables pour les sous-systèmes qui comprennent du logiciel. Dans ce cas, il est nécessaire de s'assurer que le sous-système n'exécute, dans son application de sécurité, que la fonction pour laquelle la preuve du niveau d'intégrité prescrit est fournie. Voir aussi 7.4.2.11 de la CEI 61508-3.

7.4.8 Prescriptions concernant les communications de données

7.4.8.1 Lorsqu'une forme quelconque de communication de données est utilisée dans la réalisation d'une fonction de sécurité, la probabilité de défaillance de la fonction de sécurité due au processus de communication doit être estimée en prenant en compte les erreurs de transmission, les répétitions, les suppressions, les insertions, les modifications du séquencement, la corruption, le retard et le masquage (voir aussi 7.4.8.2). Cette probabilité doit être prise en compte lors de l'estimation de la probabilité de défaillance dangereuse de la fonction de sécurité, due à une défaillance aléatoire du matériel (voir 7.4.3.2.2).

NOTE Le terme masquage signifie que le contenu exact d'un message n'est pas correctement identifié. Par exemple, un message provenant d'un composant qui n'est pas de sécurité est identifié incorrectement comme un message provenant d'un composant de sécurité.

7.4.8.2 En particulier, les paramètres suivants doivent être pris en compte en estimant la probabilité de défaillance de la fonction de sécurité due au processus de communication:

a) le taux d'erreur résiduel (voir VEI 371-08-05);

b) le taux de perte d'information résiduel (voir VEI 371-08-09);

c) les limites, et la variabilité de la vitesse de transfert de l'information (débit binaire);

d) les limites, et la variabilité, du temps de retard dû à la propagation de l'information.

NOTE 1 On peut démontrer que la probabilité d'une défaillance dangereuse (en h^{-1}) est égale au quotient de la probabilité d'erreur résiduelle par la longueur du message (en bits) multipliée par la vitesse de transmission sur le bus des messages relatifs à la sécurité ainsi que par un facteur de 3600.

NOTE 2 Des informations complémentaires figurent dans la CEI 60870-5-1 et dans l'EN 50159-1 et l'EN 50159-2.

7.5 Intégration E/E/PES

NOTE Cette phase est représentée dans la case 9.4 de la figure 2.

7.5.1 Objectif

L'objectif des prescriptions du présent paragraphe est d'intégrer et de soumettre les systèmes E/E/PE relatifs à la sécurité aux tests d'intégration.

7.5.2 Prescriptions

7.5.2.1 Les systèmes E/E/PE relatifs à la sécurité doivent être intégrés conformément à la conception E/E/PES spécifiée et doivent être soumis aux tests conformément aux tests d'intégration E/E/PES spécifiés (voir 7.4.2.11).

7.5.2.2 Dans le cadre de l'intégration de tous les modules dans les systèmes E/E/PE relatifs à la sécurité, les systèmes E/E/PE relatifs à la sécurité doivent être soumis aux tests comme spécifié (voir 7.4). Ces tests doivent démontrer que tous les modules interagissent de manière correcte pour remplir leurs fonctions prévues et sont conçus de manière à ne pas réaliser de fonctions non prévues.

NOTE 1 Ceci n'implique pas de soumettre aux tests toutes les combinaisons d'entrée. Il peut être suffisant de soumettre aux tests toutes les classes d'équivalence (voir B.5.2 de la CEI 61508-7). Il est admis que le nombre de cas de tests puisse 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). Lorsque le développement est réalisé conformément aux règles donnant lieu à une conception structurée (voir B.3.2 de la CEI 61508-7) ou selon des méthodes semi-formelles (voir B.2.3 de la CEI 61508-7) les prescriptions sont plus faciles à satisfaire que lorsque cela n'est pas le cas.

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.5.13 et C.3.3 de la CEI 61508-7), il est admis que le domaine d'application de ces tests 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 relatif à la sécurité dans le PES doit être réalisée conformément au paragraphe 7.5 de la CEI 61508-3.

7.5.2.4 La documentation appropriée des tests d'intégration des systèmes E/E/PE relatifs à la sécurité doit être produite, en indiquant les résultats des tests et en précisant la conformité aux objectifs et critères spécifiés pendant la phase de conception et de développement. En cas de défaillance, les raisons de la défaillance et les actions correctives doivent être documentées.

7.5.2.5 Pendant les tests d'intégration, toutes les modifications ou changement effectués sur les systèmes E/E/PE relatifs à la sécurité doivent faire l'objet d'une analyse d'impact qui doit identifier tous les composants concernés ainsi que les activités de revérification nécessaires.

7.5.2.6 Les tests d'intégration E/E/PES doivent consigner par écrit les informations suivantes:

a) la version de la spécification de test utilisée;

b) les critères d'acceptation des tests d'intégration;

c) la version des systèmes E/E/PE relatifs à la sécurité soumis aux tests;

d) les outils et les équipements utilisés ainsi que les données d'étalonnage;

e) les résultats de chaque test;

f) toute divergence entre les résultats prévus et réels;

g) l'analyse effectuée ainsi que les décisions prises quant à la poursuite du test ou l'émission d'une demande de modification dans le cas où des anomalies seraient observées.

7.5.2.7 Au cours de l'intégration E/E/PES, afin d'éviter les anomalies, un ensemble approprié de techniques et de mesures, conforme au tableau B.3 doit être utilisé.

7.6 Procédures d'exploitation et de maintenance E/E/PES

NOTE Cette phase est représentée dans la case 9.5 de la figure 2.

7.6.1 Objectif

L'objectif des prescriptions du présent paragraphe est de développer des procédures permettant de s'assurer que la sécurité fonctionnelle prescrite des systèmes E/E/PE relatifs à la sécurité est maintenue pendant l'exploitation et la maintenance.

7.6.2 Prescriptions

7.6.2.1 Les procédures d'exploitation et de maintenance E/E/PES doivent être rédigées et 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 composants à vie prédéfinie, par exemple les ventilateurs de refroidissement des batteries, etc.;

b) les actions et contraintes qui sont nécessaires (par exemple, pendant l'installation, le démarrage, le fonctionnement normal, les tests individuels de série, les perturbations prévisibles, les anomalies ou défaillances ainsi que l'arrêt) pour prévenir 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 taux de demandes sur les systèmes E/E/PE relatifs à la sécurité;

d) la documentation qu'il est nécessaire de maintenir, montrant les résultats des audits et tests effectués sur des systèmes E/E/PE relatifs à la sécurité;

e) les procédures de maintenance à suivre lorsque des anomalies ou défaillances ont lieu dans les systèmes E/E/PE relatifs à la sécurité, y compris
   – les procédures de diagnostic et de réparation des anomalies,
   – les procédures de revalidation,
   – les prescriptions relatives au compte rendu de maintenance;
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 A la fois pour des raisons de sécurité et d'économie, il peut être profitable d'intégrer les procédures d'exploitation et de maintenance E/E/PES aux procédures globales d'exploitation et de maintenance de l'EUC.

NOTE 2 Il convient que les procédures d'exploitation et de maintenance E/E/PES incluent les procédures de modification du logiciel (voir CEI 61508-3, 7.8).

7.6.2.2 Les procédures d'exploitation et de maintenance du système E/E/PE relatif 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 tests effectués sur des systèmes E/E/PE relatifs à la sécurité.

7.6.2.3 Les actions de maintenance périodique requises pour maintenir la sécurité fonctionnelle prescrite (telle que conçue) des systèmes E/E/PE relatifs à la sécurité doivent être déterminées par une méthode systématique. Cette méthode doit déterminer les défaillances non révélées de tous les composants 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;
– la maintenance basée sur la fiabilité.

NOTE 1 La prise en compte du facteur humain est un élément clé pour la détermination des actions requises et de l'(les) interface(s) appropriée(s) avec les systèmes E/E/PE relatifs à la sécurité.

NOTE 2 Des tests périodiques seront effectués selon la fréquence nécessaire pour réaliser la mesure cible de défaillances.

NOTE 3 La fréquence des tests périodiques, de l'intervalle entre tests de diagnostic et la durée de réparation qui en découle dépendent de plusieurs facteurs (voir annexe B de la CEI 61508-6), tel que

– la mesure cible des défaillances associée au niveau d'intégrité de sécurité;
– l'architecture;
– la couverture du diagnostic des tests de diagnostic;
– le taux de demande moyen.

NOTE 4 La fréquence des tests périodiques et l'intervalle entre tests de diagnostic sont susceptibles d'influer de manière capitale sur la réalisation de l'intégrité de sécurité du matériel. L'un des principaux justificatifs de l'analyse de fiabilité du matériel (voir 7.4.3.2.2) est de s'assurer que les fréquences des deux types de tests conviennent à l'intégrité de sécurité cible du matériel.

7.6.2.4 L'éventuel impact des procédures d'exploitation et de maintenance E/E/PES sur l'EUC doit être évalué.

7.6.2.5 Pour l'évitement des anomalies ou des défaillances au cours des procédures d'exploitation et de maintenance E/E/PES, un ensemble approprié de techniques et de mesures, conforme au tableau B.4, doit être utilisé.

7.7 Validation de sécurité E/E/PES

NOTE Cette phase est représentée dans la case 9.6 de la figure 2.

7.7.1 Objectif

L'objectif des prescriptions de ce paragraphe est de valider la conformité, à tous égards, des systèmes E/E/PE relatifs à la sécurité aux prescriptions de sécurité, en termes de fonctions de sécurité et d'intégrité de sécurité requises (voir 7.2).

7.7.2 Prescriptions

7.7.2.1 La validation de la sécurité E/E/PES 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 E/E/PES, l'activité de validation de sécurité E/E/PES est illustrée avant l'installation; cependant, dans certains cas, la validation de sécurité E/E/PES 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 prescriptions de validation du logiciel sont données dans la CEI 61508-3.

7.7.2.2 Tous les équipements de mesure de test utilisés pour la validation doivent être étalonnés en fonction d'un étalon lié à une norme nationale si elle est disponible ou selon une procédure bien acceptée. Le fonctionnement correct de tous les équipements de test doit être vérifié.

7.7.2.3 Chaque fonction de sécurité spécifiée dans les prescriptions de sécurité E/E/PES (voir 7.2) ainsi que les procédures d'exploitation et de maintenance E/E/PES doivent être validées par test et/ou analyse.

7.7.2.4 La documentation relative aux tests de validation de sécurité E/E/PES doit être élaborée et indiquer pour chaque fonction de sécurité

a) la version du plan de validation de sécurité E/E/PES utilisée;

b) la fonction de sécurité soumise à test (ou à l'analyse), ainsi que la référence spécifique à la prescription spécifiée lors de la planification de la validation de sécurité E/E/PES;

c) les outils et équipements utilisés ainsi que les données d'étalonnage;

d) les résultats de chaque test;

e) les divergences entre résultats prévus et 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, elles doivent être indiquées.

7.7.2.5 En cas de divergence (c'est-à-dire lorsque les résultats réels s'écartent des résultats prévus au-delà des tolérances), les résultats des tests de validation de sécurité E/E/PES doivent être consignés par écrit en indiquant

a) l'analyse effectuée; et

b) la décision prise quant à la poursuite du test ou l'émission d'une demande de modification et retour à une étape antérieure du test de validation.

7.7.2.6 Le fournisseur ou le développeur doit rendre disponible les résultats des tests de validation de sécurité E/E/PES au développeur de l'EUC et du système de commande de l'EUC de manière à leur permettre de satisfaire aux prescriptions pour la validation de sécurité globale de la CEI 61508-1.

7.7.2.7 Pour l'évitement des anomalies au cours de la validation de sécurité E/E/PES, un ensemble approprié de techniques et de mesures, conforme au tableau B.5 doit être utilisé.

7.8 Modification E/E/PES

7.8.1 Objectif

L'objectif des prescriptions de ce paragraphe est de s'assurer que l'intégrité de sécurité requise est maintenue après corrections, améliorations ou adaptations apportées aux systèmes E/E/PE relatifs à la sécurité.

7.8.2 Prescriptions

7.8.2.1 Pour chaque activité de modification E/E/PES, une documentation appropriée doit être établie et maintenue. La documentation doit comprendre

a) la spécification détaillée de la modification ou du changement;

b) une analyse d'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 éventuelles;

c) toutes approbations relatives aux modifications;

d) l'avancement des modifications;

e) les tests élémentaires des composants, y compris les données de revalidation;

f) l'historique de la gestion de configuration E/E/PES;

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 systémiers qui annoncent 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 de défauts dans le matériel ou le logiciel, et d'informer les utilisateurs du besoin de modifier dans le cas d'un défaut 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 vérifiés et revalidés.

NOTE Voir également 7.16.2.6 de la CEI 61508-1.

7.9 Vérification E/E/PES

7.9.1 Objectif

L'objectif des prescriptions de ce paragraphe est de tester et d'évaluer les résultats d'une phase donnée pour s'assurer du caractère correct et de la cohérence des résultats par rapport aux produits et normes fournis en données pour cette phase.

NOTE Pour plus de commodité, toutes les activités de vérification ont été regroupées en 7.9, mais elles sont en fait entreprises au cours de plusieurs phases.

7.9.2 Prescriptions

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 E/E/PES et doit être consignée par écrit.

7.9.2.2 La planification de la vérification E/E/PES doit se référer 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 E/E/PES doit spécifier les activités à entreprendre pour s'assurer du caractère correct et de 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 E/E/PES doit tenir compte des éléments suivants:

a) le choix des stratégies et techniques de vérification;

b) le choix et l'utilisation des équipements de test;

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 tests.

7.9.2.5 Au cours de chaque phase de conception et de développement, il doit être démontré que les prescriptions fonctionnelles et les prescriptions d'intégrité de sécurité sont remplies.

7.9.2.6 Le résultat de chaque activité de vérification doit être consigné par écrit et indiquer soit que le système E/E/PE relatif à la sécurité a passé avec succès la vérification, ou les raisons de l'échec. Les éléments suivants doivent être pris en compte:

a) les entités qui ne sont pas conformes à une ou plusieurs prescriptions pertinentes du cycle de vie de sécurité E/E/PES (voir 7.2);

b) les entités qui ne sont pas conformes à une ou plusieurs normes de conception applicables (voir 7.4);

c) les entités qui ne sont pas conformes à une ou plusieurs prescriptions de gestion de sécurité applicables (voir article 6).

7.9.2.7 Pour la vérification des prescriptions de sécurité E/E/PES, après établissement des prescriptions de sécurité E/E/PES (voir 7.2) et avant d'entamer la phase suivante (conception et développement), la vérification doit

a) déterminer l'adéquation des prescriptions de sécurité E/E/PES pour satisfaire aux prescriptions établies dans l'attribution des prescriptions de sécurité E/E/PES (voir la CEI 61508-1) pour la sécurité, la fonctionnalité et autres prescriptions spécifiées lors de la planification de la sécurité, et

b) vérifier les incompatibilités entre

   – les prescriptions de sécurité E/E/PES (7.2),

   – l'allocation des prescriptions de sécurité (CEI 61508-1),

   – les tests E/E/PES (voir 7.4), et

   – la documentation de l'utilisateur et toute autre documentation relative au système.

7.9.2.8 Pour la vérification de la conception et du développement E/E/PES, après achèvement de la conception et du développement E/E/PES (voir 7.4) et avant d'entamer la phase suivante (intégration), la vérification doit

a) s'assurer que les tests E/E/PES (voir 7.4) conviennent à la conception et au développement E/E/PES (voir 7.4);

b) s'assurer de la cohérence et de la complétude (jusqu'au niveau module inclus) de la conception et du développement E/E/PES (voir 7.4) par rapport aux prescriptions de sécurité E/E/PES (voir 7.2); et

c) vérifier les incompatibilités entre

   – les prescriptions de sécurité E/E/PES (7.2),

   – la conception et le développement E/E/PES (7.4), et

   – les tests E/E/PES (voir 7.4).

NOTE 1 Le tableau B.5 recommande des techniques de validation de la sécurité, d'analyse des défaillances et des techniques de test qui sont également applicables à la vérification.

NOTE 2 Le tableau A.1, qui donne les anomalies et défaillances qui doivent être détectées, est pris en compte pour vérifier que la couverture du diagnostic a été réalisée.

7.9.2.9 Pour la vérification de l'intégration E/E/PES, l'intégration des systèmes E/E/PE relatifs à la sécurité doit être vérifiée pour s'assurer de la conformité aux prescriptions de 7.5.

7.9.2.10 Les cas de tests ainsi que leurs résultats doivent être consignés par écrit.

8 Evaluation de la sécurité fonctionnelle

Les prescriptions 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 et limite la couverture de diagnostic maximale qu'il est admis d'annoncer 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, les défaillances systématiques, les défaillances environnementales et les défaillances opérationnelles. L'annexe B de la CEI 61508-6 et l'annexe A de la CEI 61508-7 fournissent plus d'informations quant aux architectures et 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 anomalies et défaillances est souvent difficile à déterminer;
– la caractérisation des défaillances passe d'aléatoire à systématique en fonction de la complexité du matériel et du logiciel 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:

– 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 de composants 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, une fois qu'elles sont apparues, un grand nombre de mesures est en général nécessaire. La structure de prescriptions fournie 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 E/E/PES (annexe B) et celles utilisées pour **maîtriser les 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 du diagnostic et la proportion de défaillances en sécurité sont déterminées sur la base du tableau A.1 conformément aux procédures détaillées à l'annexe C. Les tableaux A.2 à A.15 appuient les prescriptions du tableau A.1 en recommandant des techniques et des mesures de test de diagnostic ainsi que les niveaux maximaux de couverture de diagnostic qui peuvent être réalisés en utilisant ces techniques et mesures. Ces tableaux ne remplacent aucune des prescriptions de l'annexe C. Les tableaux A.2 à A.15 ne sont pas exhaustifs. D'autres mesures et techniques peuvent être utilisées, pourvu que la preuve permettant d'appuyer la couverture de diagnostic annoncée soit produite. Si une couverture de diagnostic élevée est annoncée, alors, à minima, il convient qu'au moins une technique permettant une couverture de diagnostic élevée soit utilisée, à partir de chacun de ces tableaux.

De la même manière, les tableaux A.16 à A.18 recommandent des techniques et des mesures pour chaque niveau d'intégrité de sécurité pour maîtriser des défaillances systématiques. Le tableau A.16 recommande des mesures globales pour maîtriser des défaillances systématiques (voir également la CEI 61508-3), le tableau A.17 recommande des mesures pour maîtriser des défaillances environnementales et le tableau A.18 recommande des mesures pour maîtriser des défaillances opérationnelles. La plupart de ces mesures de maîtrise peuvent être classées en fonction du tableau A.19.

Toutes les techniques et mesures développées dans ces tableaux sont décrites dans l'annexe A de la CEI 61508-7. Les techniques et mesures logicielles requises pour chaque niveau d'intégrité de sécurité sont données dans la CEI 61508-3. Les lignes directrices permettant de déterminer l'architecture d'un système E/E/PE relatif à la sécurité sont données dans l'annexe B de la CEI 61508-6.

Le fait de se conformer aux lignes directrices de la présente annexe ne garantit pas en soi l'intégrité de sécurité. Il est important de tenir compte des éléments suivants:

– la cohérence des techniques et mesures choisies ainsi que la manière dont elles se complètent; et
– les techniques et les mesures qui sont les mieux adaptées aux problèmes spécifiques rencontrés au cours du développement de chaque système particulier E/E/PE relatif à la sécurité.

A.2 Intégrité de sécurité du matériel

Le tableau A.1 fournit des prescriptions pour des anomalies ou des défaillances qui doivent être détectées par les techniques et mesures de maîtrise des défaillances du matériel afin de réaliser la couverture de diagnostic pertinente (voir également l'annexe C). Les tableaux A.2 à A.15 appuient les prescriptions du tableau A.1 en recommandant des techniques et des mesures de test de diagnostic ainsi que les niveaux maximaux de couverture de diagnostic qui peuvent être réalisés en utilisant ces techniques et mesures. Il est admis que ces tests soient appliqués de manière permanente ou périodique. Les tableaux ne remplacent aucune des prescriptions de 7.4. Les tableaux A.2 à A.15 ne sont pas exhaustifs. D'autres mesures et techniques peuvent être utilisées, pourvu que la preuve permettant d'appuyer la couverture de diagnostic soit produite.

NOTE 1 La présentation générale des techniques et mesures examinées dans ces tableaux est fournie à l'annexe A de la CEI 61508-7. Le paragraphe applicable est référencé dans la seconde colonne des tableaux A.2 à A.15.

NOTE 2 Les qualificatifs faible, moyen et élevé de la couverture du diagnostic sont quantifiés à 60 %, 90 % et 99 % respectivement.