IEC 61508-2

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

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

IEC 61508-2:2010

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

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61508-2

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XD

ICS 25.040.40

ISBN 978-2-88910-525-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

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

International Standard IEC 61508-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2000. This edition constitutes a technical revision.

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

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

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

FDIS	Report on voting
65A/549/FDIS	65A/573/RVD

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

This International Standard

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

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

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;
- a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5};
- a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}];

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

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

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;
- introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe. However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

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

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

1 Scope

1.1 This part of the IEC 61508 series

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

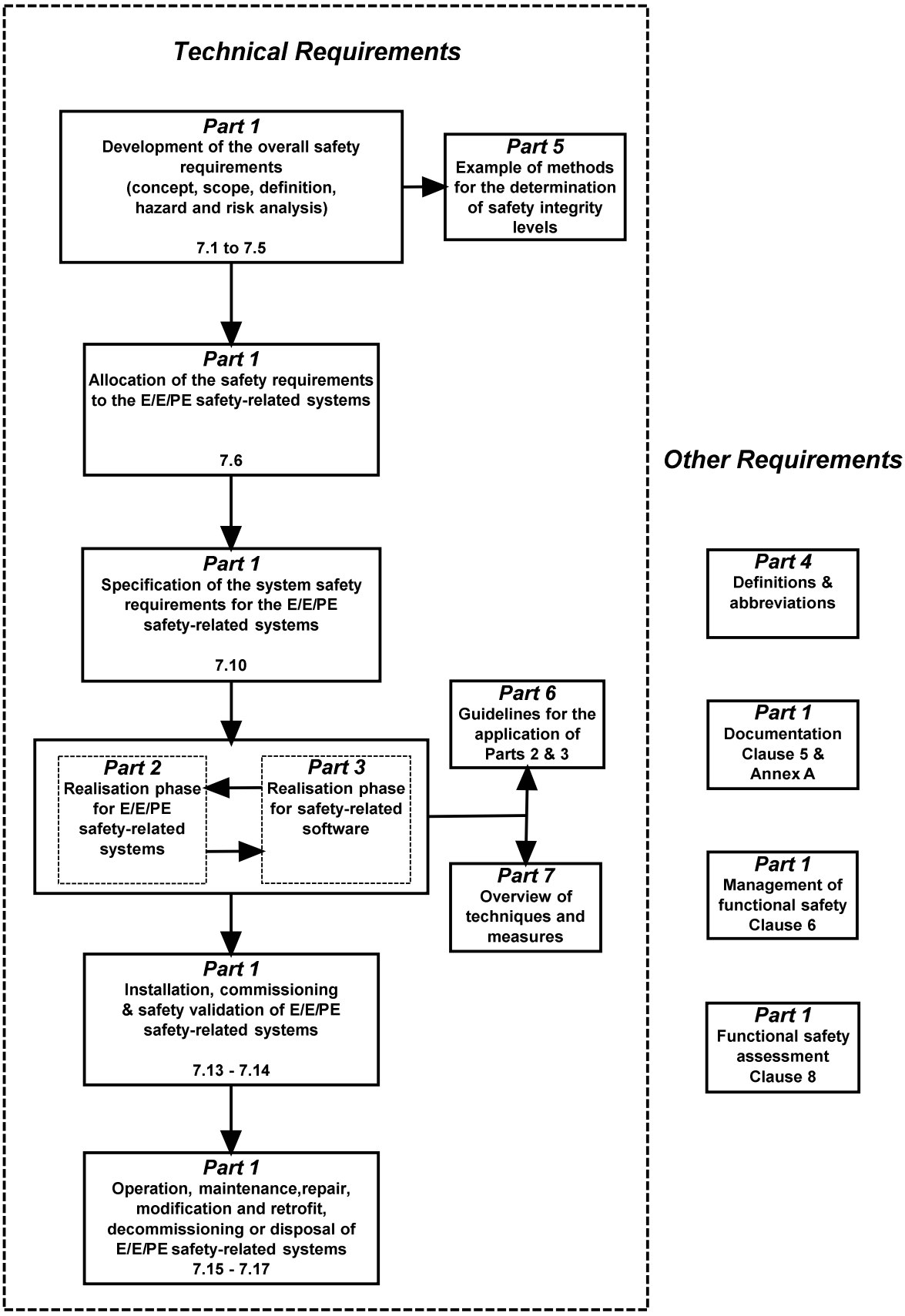


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Definitions and abbreviations

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

4 Conformance to this standard

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

5 Documentation

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

6 Management of functional safety

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

7 E/E/PE system safety lifecycle requirements

7.1 General

7.1.1 Objectives and requirements – general

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

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

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

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

7.1.2 Objectives

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

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

7.1.3 Requirements

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

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

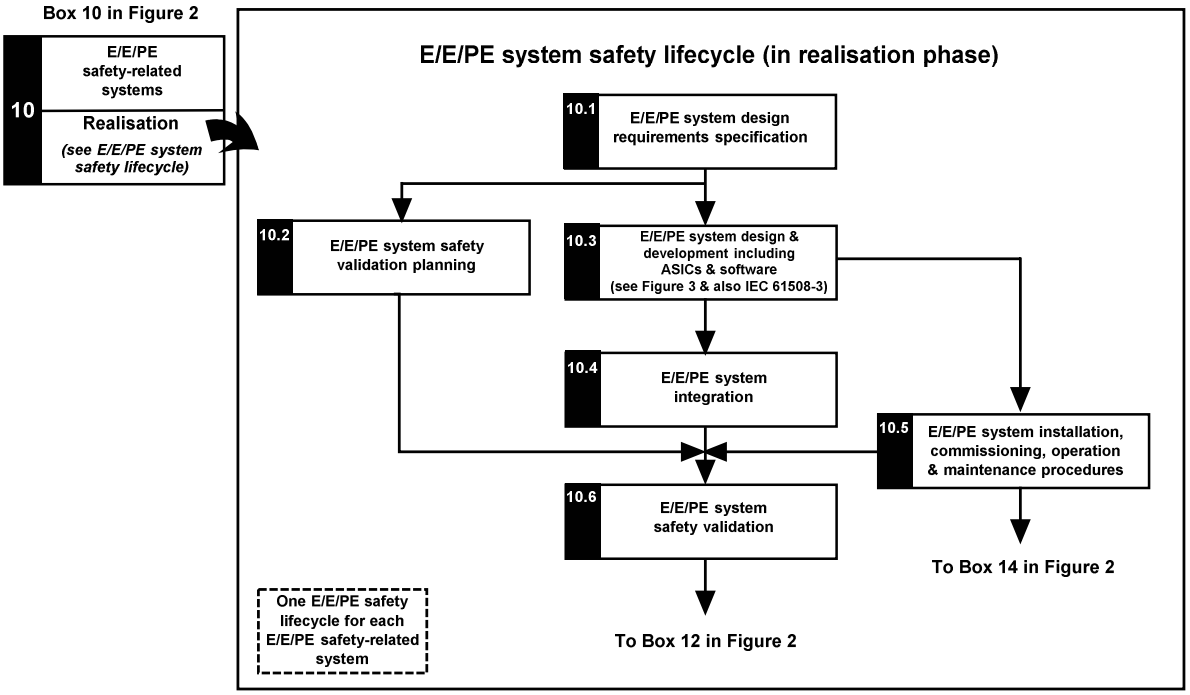
NOTE 2 There are significant similarities between the ASIC and the software design processes. IEC 61508-3 recommends the V-model for designing safety-related software. The V-model requires a clearly structured design process and a modular software structure for avoiding and controlling systematic faults.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

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

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

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

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



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

NOTE 2 This figure shows only those phases of the E/E/PE system safety lifecycle that are within the realisation phase of the overall safety lifecycle. The complete E/E/PE system safety lifecycle will also contain instances, specific to the E/E/PE safety-related system, of the subsequent phases of the overall safety lifecycle (Boxes 12 to 16 in Figure 2 of IEC 61508-1).

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

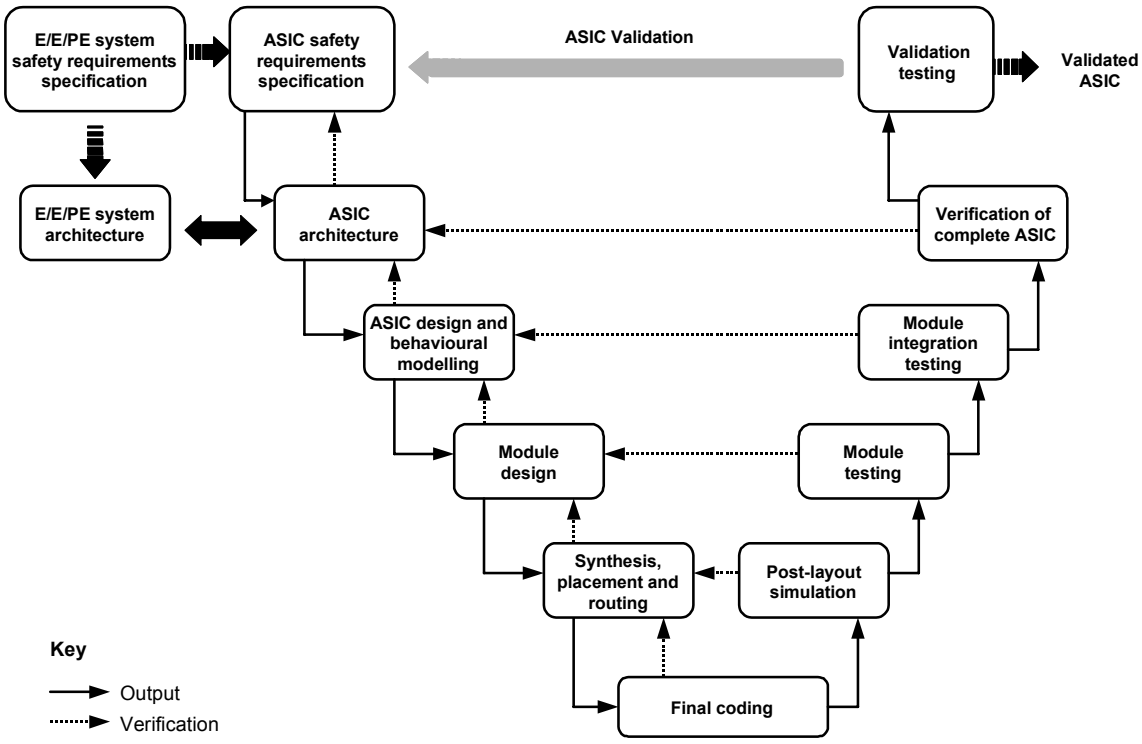


Figure 3 – ASIC development lifecycle (the V-Model)

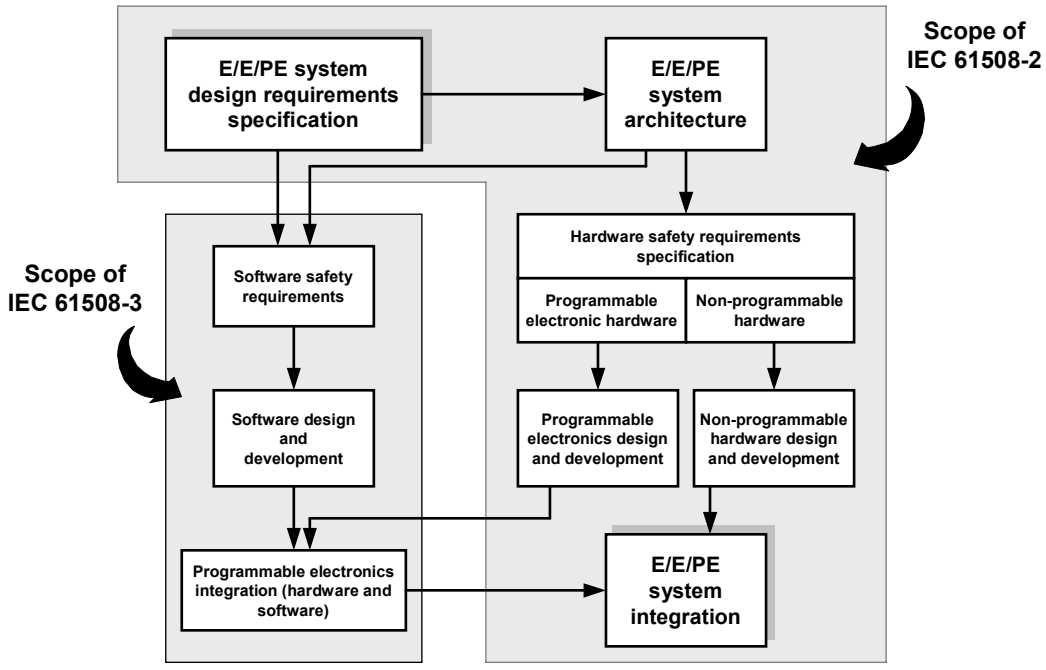


Figure 4 – Relationship between and scope of IEC 61508-2 and IEC 61508-3

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

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

Table 1 *(continued)*

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

7.2 E/E/PE system design requirements specification

NOTE This phase is Box 10.1 of Figure 2.

7.2.1 Objective

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

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

7.2.2 General

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

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

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

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

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

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

7.2.3 E/E/PE system design requirements specification

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

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

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

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

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

d) accuracy and stability requirements for measurements and controls;

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

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

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

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

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

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

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

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

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

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

NOTE 1 Information on the specific application cannot be understated (see 7.10.2.1 of IEC 61508-1). This is particularly important for maintenance, where the specified proof test interval should not be less than can be reasonably expected for the particular application. For example, the time between services that can be realistically attained for mass-produced items used by the public is likely to be greater than in a more controlled application.

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

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

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

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

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

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

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

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

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

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

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

7.3 E/E/PE system safety validation planning

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

7.3.1 Objective

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

7.3.2 Requirements

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

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

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

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

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

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

e) test evaluation procedures (with justifications);

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

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

g) policies for resolving validation failure.

7.4 E/E/PE system design and development

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

7.4.1 Objective

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

7.4.2 General requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) the method of achieving independence;

b) the justification of the method.

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

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

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

a) safety functions;

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

c) equipment and operator interfaces.

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

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

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

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

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

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

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

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

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

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

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

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

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

7.4.3 Synthesis of elements to achieve the required systematic capability

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.4.4 Hardware safety integrity architectural constraints

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

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

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

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

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

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

7.4.4.1 General requirements

7.4.4.1.1 With respect to the hardware fault tolerance requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.4.4.2 Route 1_H

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

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

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

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

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

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

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

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

2) the elements are of the same type; and

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

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

   b) determine the hardware fault tolerance of the subsystem;

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

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

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

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

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

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

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

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

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

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

i. For general application to any subsystem see 7.4.4.2.1.

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

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

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

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

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

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

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

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

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

i. For general application to any subsystem see 7.4.4.2.1.

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

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

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

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

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

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

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

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

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

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

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

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

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

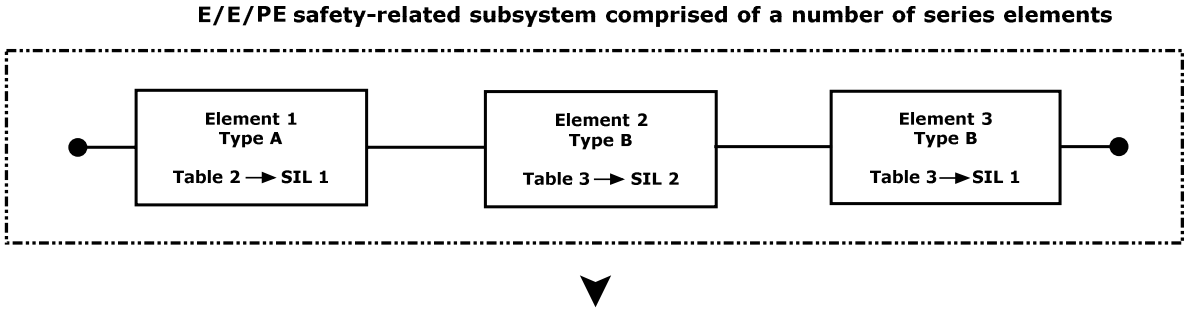


Figure 5 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements, see 7.4.4.2.3)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

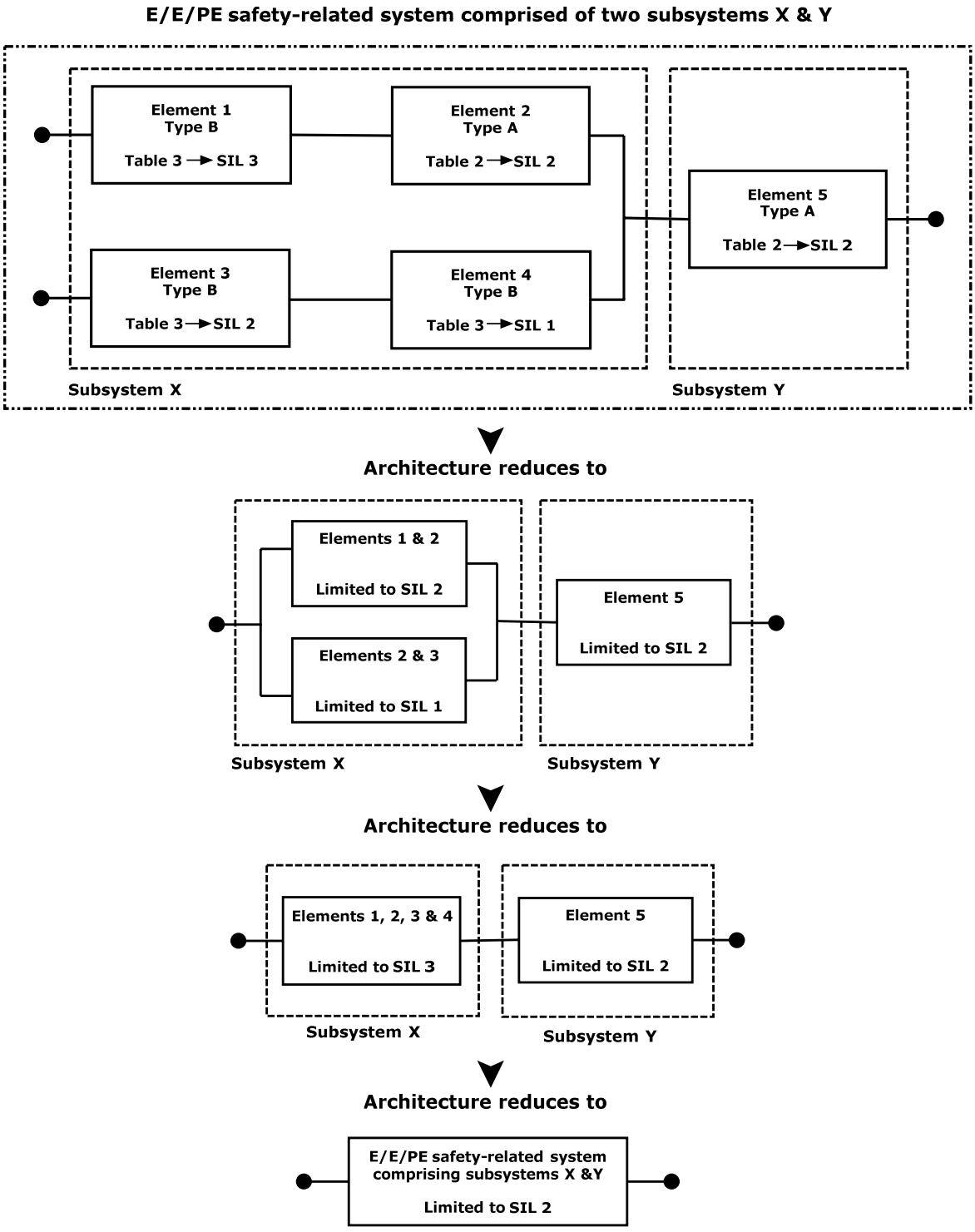
a) Combining elements 1 and 2: The hardware fault tolerance and safe failure fraction achieved by the combination of elements 1 and 2 (each separately meeting the requirements for SIL 3 and SIL 2 respectively) meets the requirements of SIL 2 (determined by element 2; see 7.4.4.2.3);

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

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

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

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



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

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

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

7.4.4.3 Route 2_H

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c) evaluated according to:

   i) the amount of field feedback; and,

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

   iii) the undertaking of specific tests;

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

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

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

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

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

7.4.5 Requirements for quantifying the effect of random hardware failures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

h) the repair times for detected failures;

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

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

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

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

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

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

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

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

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

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

7.4.5.4 The diagnostic test interval of any subsystem:

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

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

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

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

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

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

c) select and implement the applicable improvements;

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

7.4.6 Requirements for the avoidance of systematic faults

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

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

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

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

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

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

c) clear and precise documentation and communication of information;

d) verification and validation.

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

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

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

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

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

c) the pass/fail criteria.

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

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

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

7.4.7 Requirements for the control of systematic faults

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

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

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

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

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

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

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

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

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

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

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

7.4.8 Requirements for system behaviour on detection of a fault

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

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

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

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

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

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

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

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

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

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

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

7.4.9 Requirements for E/E/PE system implementation

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

m) the hardware fault tolerance of the element.

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

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

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

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

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

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

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

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

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

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

7.4.10 Requirements for proven in use elements

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

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

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

7.4.10.2 The documentary evidence required by 7.4.10.1 shall demonstrate that:

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

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

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

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

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

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

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

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

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

c) the statistical evidence.

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

a) the complexity of the element;

b) the systematic capability required for the element;

c) the novelty of design.

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

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

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

7.4.11 Additional requirements for data communications

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

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

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

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

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

Figure 7 (a) White channel

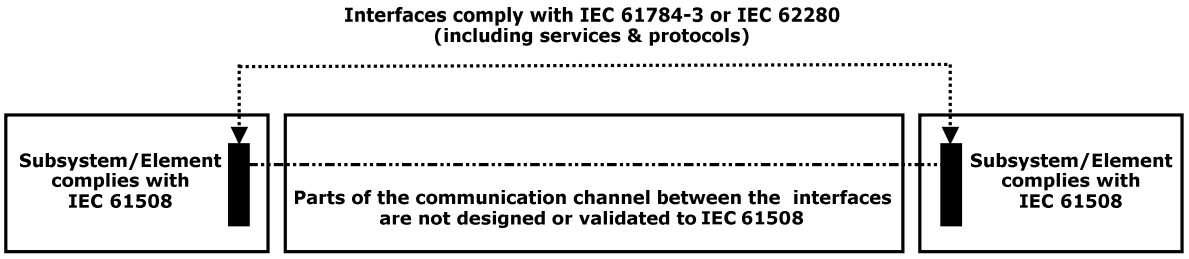


Figure 7 (b) Black channel

Figure 7 – Architectures for data communication

7.5 E/E/PE system integration

NOTE This phase is Box 10.4 of Figure 2.

7.5.1 Objective

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

7.5.2 Requirements

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

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

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

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

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

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

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

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

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

a) the version of the test specification used;

b) the criteria for acceptance of the integration tests;

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

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

e) the results of each test;

f) any discrepancy between expected and actual results;

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

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

7.6 E/E/PE system operation and maintenance procedures

NOTE This phase is Box 10.5 of Figure 2.

7.6.1 Objective

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

7.6.2 Requirements

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

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

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

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

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

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

   – procedures for fault diagnoses and repair;

   – procedures for revalidation;

   – maintenance reporting requirements;

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

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

   – procedures for reporting failures;

   – procedures for analysing failures;

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

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

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

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

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

– examination of fault trees;

– failure mode and effect analysis.

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

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

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

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

– the architecture;

– the diagnostic coverage of the diagnostic tests, and

– the expected demand rate.

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

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

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

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

7.7 E/E/PE system safety validation

NOTE This phase is Box 10.6 of Figure 2.

7.7.1 Objective

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

7.7.2 Requirements

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

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

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

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

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

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

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

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

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

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

d) the results of each test;

e) discrepancies between expected and actual results.

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

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

a) the analysis made; and

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

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

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

7.8 E/E/PE system modification

7.8.1 Objective

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

7.8.2 Requirements

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

a) the detailed specification of the modification or change;

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

c) all approvals for changes;

d) progress of changes;

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

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

g) deviation from normal operations and conditions;

h) necessary changes to system procedures;

i) necessary changes to documentation.

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

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

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

NOTE See also 7.16.2.6 of IEC 61508-1.

7.9 E/E/PE system verification

7.9.1 Objective

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

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

7.9.2 Requirements

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

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

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

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

a) the selection of verification strategies and techniques;

b) the selection and utilisation of the test equipment;

c) the selection and documentation of verification activities;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.9.2.10 Test cases and their results shall be documented.

8 Functional safety assessment

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

Annex A
(normative)

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

A.1 General

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

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

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

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

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

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

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

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

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

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

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

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

A.2 Hardware safety integrity

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

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

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

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

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

Table A.1 *(continued)*

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

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

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

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

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

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

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

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

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

Table A.2 – Electrical components

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

Table A.3 – Electronic components

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

Table A.4 – Processing units

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

Table A.5 – Invariable memory ranges

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

Table A.6 – Variable memory ranges

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

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

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

Table A.8 – Data paths (internal communication)

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

Table A.9 – Power supply

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

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

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

Table A.11 – Clock

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

Table A.12 – Communication and mass-storage

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

Table A.13 – Sensors

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

Table A.14 – Final elements (actuators)

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

A.3 Systematic safety integrity

The following tables give recommendations for techniques and measures to:

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

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

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

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

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

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

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

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

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

The required effectiveness is signified as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex B
(normative)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The required effectiveness is signified as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table B.6 *(continued)*

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

Table B.6 *(continued)*

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

Annex C
(normative)

Diagnostic coverage and safe failure fraction

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

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

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

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

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

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

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

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

b) Categorize each failure mode according to whether it leads (in the absence of diagnostic tests) to:

   – a safe failure; or

   – a dangerous failure;

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

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

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

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

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

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

h) Calculate safe failure fraction of the element as:

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

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

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

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

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

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

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

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

C.2 Determination of diagnostic coverage factors

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

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

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

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

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

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

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

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

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

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

Annex D
(normative)

Safety manual for compliant items

D.1 General

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

D.2 Contents

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

For every compliant item, the safety manual shall contain:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

j) the hardware fault tolerance;

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

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

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

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

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

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

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

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

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

Annex E
(normative)

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

E.1 General

This annex is referenced by 7.4.2.2 b).

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

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

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

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

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

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

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

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

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

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

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

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

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

– noise;

– disturbance propagation over the power supply lines;

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

– excessive current-draw resulting from short circuit.

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

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

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

– detecting power supply faults by means of voltage monitors;

– using partially increased voltage tolerance;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

E.3 β-factor

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

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

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

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

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

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

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

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

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

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

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

Annex F
(informative)

Techniques and measures for ASICs – avoidance of systematic failures

F.1 General

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

NOTE 1 This informative annex is referenced by 7.4.6.7.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

F.2 Guidelines: Techniques and measures

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

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

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

The recommended effectiveness is signified as follows.

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

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

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

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

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

Table F.1 *(continued)*

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

Table F.1 *(continued)*

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

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

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

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

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

Table F.2 *(continued)*

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

Table F.2 *(continued)*

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

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

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

Bibliography

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

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

[3] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

[4] IEC 61508-5: 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity* levels

[5] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[6] IEC 60601 (all parts), *Medical electrical equipment*

[7] IEC 61165, *Application of Markov techniques*

[8] IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

[9] IEC 61164, *Reliability growth – Statistical test and estimation methods*

[10] IEC 62308, *Equipment reliability – Reliability assessment methods*

[11] IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

[12] ISO 14224, *Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data for equipment*

[13] IEC 60050-191, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

[14] ISO 9000*, Quality management systems – Fundamentals and vocabulary*

[15] IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

[16] IEEE 352:1987, *IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch