IEC 61508-6

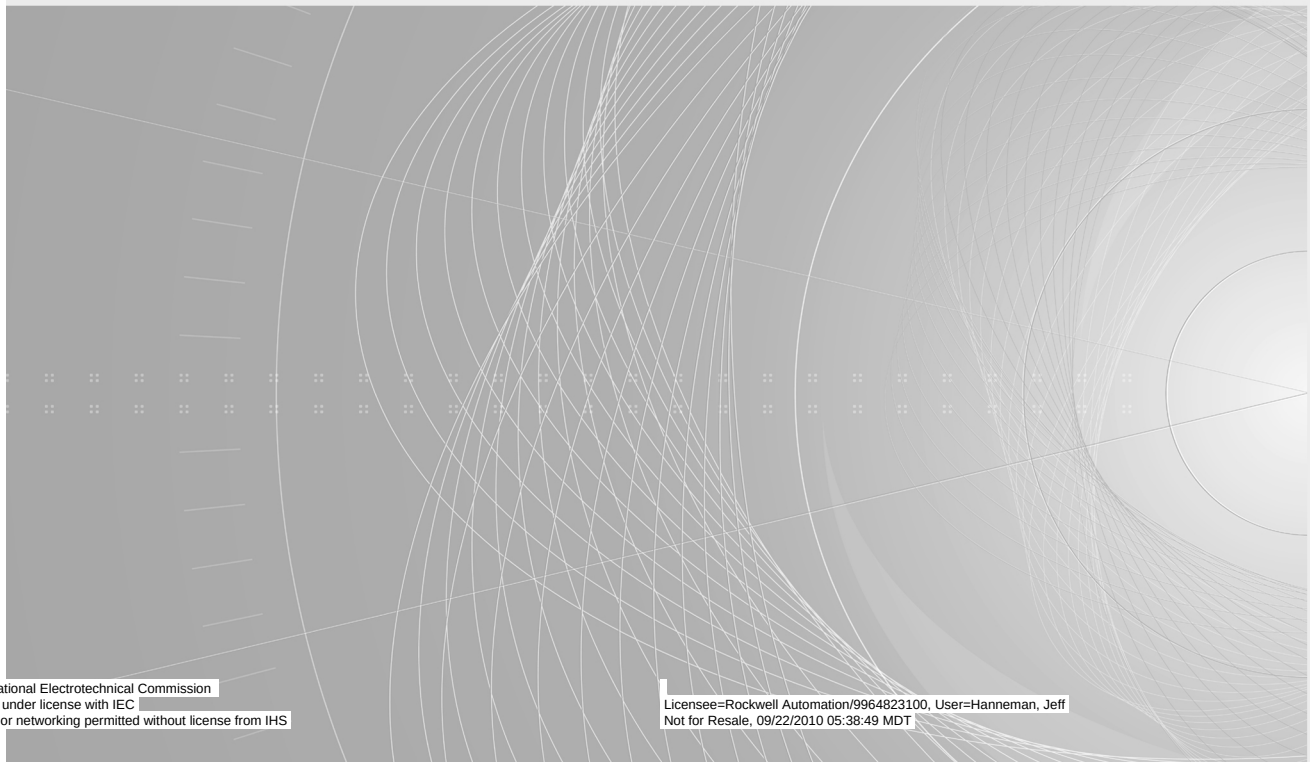
Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –
Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3



IEC 61508-6:2010

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 It also gives information on projects, withdrawn and replaced publications.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 61508-6

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –
Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XE

ICS 25.040.40

ISBN 978-2-88910-529-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

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 61508-6 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.

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

FDIS	Report on voting
65A/553/FDIS	65A/577/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 stability 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.

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;

– sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in
  – a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5};
  – a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}];

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

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

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

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

Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

1 Scope

1.1 This part of IEC 61508 contains information and guidelines on IEC 61508-2 and IEC 61508-3.

- Annex A gives a brief overview of the requirements of IEC 61508-2 and IEC 61508-3 and sets out the functional steps in their application.
- Annex B gives an example technique for calculating the probabilities of hardware failure and should be read in conjunction with 7.4.3 and Annex C of IEC 61508-2 and Annex D.
- Annex C gives a worked example of calculating diagnostic coverage and should be read in conjunction with Annex C of IEC 61508-2.
- Annex D gives a methodology for quantifying the effect of hardware-related common cause failures on the probability of failure.
- Annex E gives worked examples of the application of the software safety integrity tables specified in Annex A of IEC 61508-3 for safety integrity levels 2 and 3.

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

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.

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

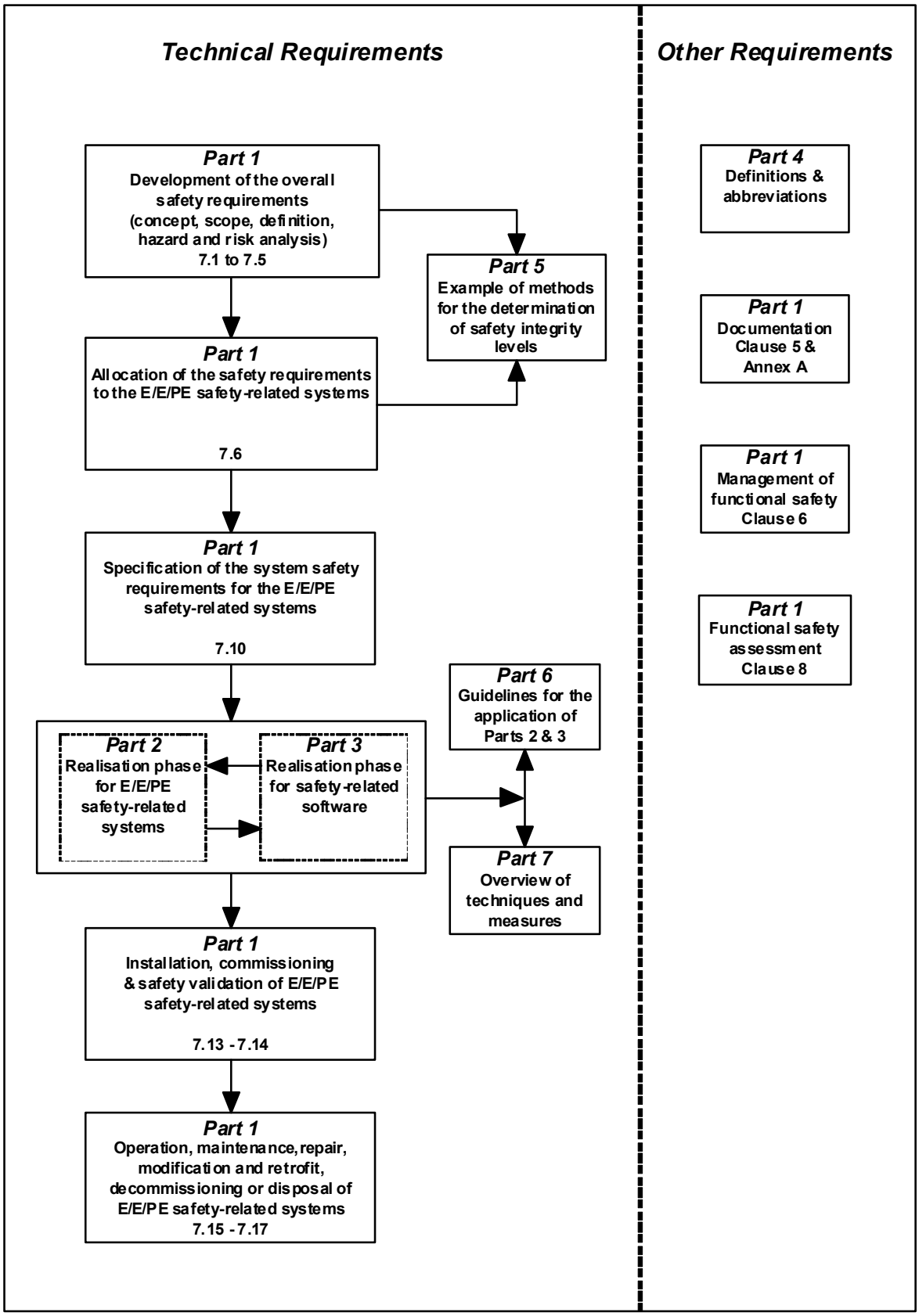


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

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

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

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

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

3 Definitions and abbreviations

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

Annex A
(informative)

Application of IEC 61508-2 and of IEC 61508-3

A.1 General

Machinery, process plant and other equipment may, in the case of malfunction (for example by failures of electrical, electronic and/or programmable electronic devices), present risks to people and the environment from hazardous events such as fires, explosions, radiation overdoses, machinery traps, etc. Failures can arise from either physical faults in the device (for example causing random hardware failures), or from systematic faults (for example human errors made in the specification and design of a system cause systematic failure under some particular combination of inputs), or from some environmental condition.

IEC 61508-1 provides an overall framework based on a risk approach for the prevention and/or control of failures in electro-mechanical, electronic, or programmable electronic devices.

The overall goal is to ensure that plant and equipment can be safely automated. A key objective of this standard is to prevent:

– failures of control systems triggering other events, which in turn could lead to danger (for example fire, release of toxic materials, repeat stroke of a machine, etc.); and

– undetected failures in protection systems (for example in an emergency shut-down system), making the systems unavailable when needed for a safety action.

IEC 61508-1 requires that a hazard and risk analysis at the process/machine level is carried out to determine the amount of risk reduction necessary to meet the risk criteria for the application. Risk is based on the assessment of both the consequence (or severity) and the frequency (or probability) of the hazardous event.

IEC 61508-1 further requires that the amount of risk reduction established by the risk analysis is used to determine if one or more safety-related systems[1] are required and what safety functions (each with a specified safety integrity)[2] they are needed for.

IEC 61508-2 and IEC 61508-3 take the safety functions and safety integrity requirements allocated to any system, designated as a E/E/PE safety-related system, by the application of IEC 61508-1 and establish requirements for safety lifecycle activities which:

– are to be applied during the specification, design and modification of the hardware and software; and

– focus on means for preventing and/or controlling random hardware and systematic failures (the E/E/PE system and software safety lifecycles)[3].

---

1 Systems necessary for functional safety and containing one or more electrical (electro-mechanical), electronic or programmable electronic (E/E/PE) devices are *designated* as E/E/PE safety-related systems and include all equipment necessary to carry out the required safety function (see 3.5.1 of IEC 61508-4).

2 Safety integrity is specified as one of four discrete levels. Safety integrity level 4 is the highest and safety integrity level 1 the lowest (see 3.5.4 and 3.5.8 of IEC 61508-4).

3 To enable the requirements of this standard to be clearly structured, a decision was made to order the requirements using a development process model in which each stage follows in a defined order with little iteration (sometimes referred to as a waterfall model). However, it is stressed that any lifecycle approach can be used provided a statement of equivalence is given in the safety plan for the project (see Clause 7 of IEC 61508-1).

IEC 61508-2 and IEC 61508-3 do not give guidance on which level of safety integrity is appropriate for a given required tolerable risk. This decision depends upon many factors, including the nature of the application, the extent to which other systems carry out safety functions and social and economic factors (see IEC 61508-1 and IEC 61508-5).

The requirements of IEC 61508-2 and IEC 61508-3 include:

– the application of measures and techniques[4], which are graded against the safety integrity level, for the avoidance of systematic failures[5] by preventative methods; and

– the control of systematic failures (including software failures) and random hardware failures by design features such as fault detection, redundancy and architectural features (for example diversity).

In IEC 61508-2, assurance that the safety integrity target has been satisfied for dangerous random hardware failures is based on:

– hardware fault tolerance requirements (see Tables 2 and 3 of IEC 61508-2); and

– the diagnostic coverage and frequency of proof tests of subsystems and components, by carrying out a reliability analysis using appropriate data.

In both IEC 61508-2 and IEC 61508-3, assurance that the safety integrity target has been satisfied for systematic failures is gained by:

– the correct application of safety management procedures;

– the use of competent staff;

– the application of the specified safety lifecycle activities, including the specified techniques and measures[6]; and

– an independent functional safety assessment[7].

The overall goal is to ensure that remaining systematic faults, commensurate with the safety integrity level, do not cause a failure of the E/E/PE safety-related system.

IEC 61508-2 has been developed to provide requirements for achieving safety integrity in the hardware[8] of the E/E/PE safety-related systems including sensors and final elements. Techniques and measures against both random hardware failures and systematic hardware failures are required. These involve an appropriate combination of fault avoidance and failure control measures as indicated above. Where manual action is needed for functional safety, requirements are given for the operator interface. Also diagnostic test techniques and measures, based on software and hardware (for example diversity), to detect random hardware failures are specified in IEC 61508-2.

IEC 61508-3 has been developed to provide requirements for achieving safety integrity for the software – both embedded (including diagnostic fault detection services) and application software. IEC 61508-3 requires a combination of fault avoidance (quality assurance) and fault tolerance approaches (software architecture), as there is no known way to prove the absence of faults in reasonably complex safety-related software, especially the absence of specification and design faults. IEC 61508-3 requires the adoption of such software

---

4 The required techniques and measures for each safety integrity level are shown in the tables in Annexes A and B of IEC 61508-2 and IEC 61508-3.

5 Systematic failures cannot usually be quantified. Causes include: specification and design faults in hardware and software; failure to take account of the environment (for example temperature); and operation-related faults (for example poor interface).

6 Alternative measures to those specified in the standard are acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

7 Independent assessment does not always imply third party assessment (see Clause 8 of IEC 61508-1).

8 Including fixed built-in software or software equivalents (also called firmware), such as application-specific integrated circuits.

engineering principles as: top down design; modularity; verification of each phase of the development lifecycle; verified software modules and software module libraries; and clear documentation to facilitate verification and validation. The different levels of software require different levels of assurance that these and related principles have been correctly applied.

The developer of the software may or may not be separate from the organization developing the whole E/E/PE system. In either case, close cooperation is needed, particularly in developing the architecture of the programmable electronics where trade-offs between hardware and software architectures need to be considered for their safety impact (see Figure 4 of IEC 61508-2).

A.2 Functional steps in the application of IEC 61508-2

The functional steps in the application of IEC 61508-2 are shown in Figures A.1 and A.2. The functional steps in the application of IEC 61508-3 are shown in Figure A.3.

Functional steps for IEC 61508-2 (see Figures A.1 and A.2) are as follows:

a) Obtain the allocation of safety requirements (see IEC 61508-1). Update the safety planning as appropriate during E/E/PE safety-related system development.

b) Determine the requirements for E/E/PE safety-related systems, including the safety integrity requirements, for each safety function (see 7.2 of IEC 61508-2). Allocate requirements to software and pass to software supplier and/or developer for the application of IEC 61508-3.

NOTE 1 The possibility of coincident failures in the EUC control system and E/E/PE safety-related system(s) needs to be considered at this stage (see A.5.4 of IEC 61508-5). These may result from failures of components having a common cause due to for example similar environmental influences. The existence of such failures could lead to a higher than expected residual risk unless properly addressed.

c) Start the phase of planning for E/E/PE safety-related system safety validation (see 7.3 of IEC 61508-2).

d) Specify the architecture (configuration) for the E/E/PE safety-related logic subsystem, sensors and final elements. Review with the software supplier/developer the hardware and software architecture and the safety implications of the trade-offs between the hardware and software (see Figure 4 of IEC 61508-2). Iterate if required.

e) Develop a model for the hardware architecture for the E/E/PE safety-related system. Develop this model by examining each safety function separately and determine the subsystem (component) to be used to carry out this function.

f) Establish the system parameters for each of the subsystems (components) used in the E/E/PE safety-related system. For each of the subsystems (elements), determine the following:

   – the proof test interval for failures which are not automatically revealed;
   – the mean time to restoration;
   – the diagnostic coverage (see Annex C of IEC 61508-2);
   – the probability of failure;
   – the required architectural constraints; for Route 1_H see 7.4.4.2 and Annex C of IEC 61508-2 and for Route 2_H see 7.4.4.3 of IEC 61508-2.

g) Create a reliability model for each of the safety functions that the E/E/PE safety-related system is required to carry out.

NOTE 2 A reliability model is a mathematical formula which shows the relationship between reliability and relevant parameters relating to equipment and conditions of use.

h) Calculate a reliability prediction for each safety function using an appropriate technique. Compare the result with the target failure measure determined in b) above and the requirements of Route 1_H (see 7.4.4.2 of IEC 61508-2) or Route 2_H (see 7.4.4.3 of

IEC 61508-2). If the predicted reliability does not meet the target failure measure and/or does not meet the requirements of Route 1_H or Route 2_H , then change

- where possible, one or more of the subsystem parameters (go back to f) above); and/or
- the hardware architecture (go back to d) above).

NOTE 3 A number of modelling methods are available and the analyst should choose which is the most appropriate (see Annex B for guidance on some methods that could be used).

i) Implement the design of the E/E/PE safety-related system. Select measures and techniques to control systematic hardware failures, failures caused by environmental influences and operational failures (see Annex A of IEC 61508-2).

j) Integrate the verified software (see IEC 61508-3) onto the target hardware (see 7.5 of IEC 61508-2 and Annex B of IEC 61508-2) and, in parallel, develop the procedures for users and maintenance staff to follow when operating the system (see 7.6 of IEC 61508-2 and Annex B of IEC 61508-2). Include software aspects (see A.3 f)).

k) Together with the software developer (see 7.7 of IEC 61508-3), validate the E/E/PE system (see 7.7 of IEC 61508-2 and Annex B of IEC 61508-2).

l) Hand over the hardware and results of the E/E/PE safety-related system safety validation to the system engineers for further integration into the overall system.

m) If maintenance/modification of the E/E/PE safety related system is required during operational life then re-activate IEC 61508-2 as appropriate (see 7.8 of IEC 61508-2).

A number of activities run across the E/E/PE safety related system safety lifecycle. These include verification (see 7.9 of IEC 61508-2) and functional safety assessment (see Clause 8 of IEC 61508-1).

In applying the above steps the E/E/PE safety related system safety techniques and measures appropriate to the required safety integrity level are selected. To aid in this selection, tables have been formulated, ranking the various techniques/measures against the four safety integrity levels (see Annex B of IEC 61508-2). Cross-referenced to the tables is an overview of each technique and measure with references to further sources of information (see Annexes A and B of IEC 61508-7).

Annex B provides one possible technique for calculating the probabilities of hardware failure for E/E/PE safety-related systems.

NOTE 4 In applying the above steps, alternative measures to those specified in the standard are acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

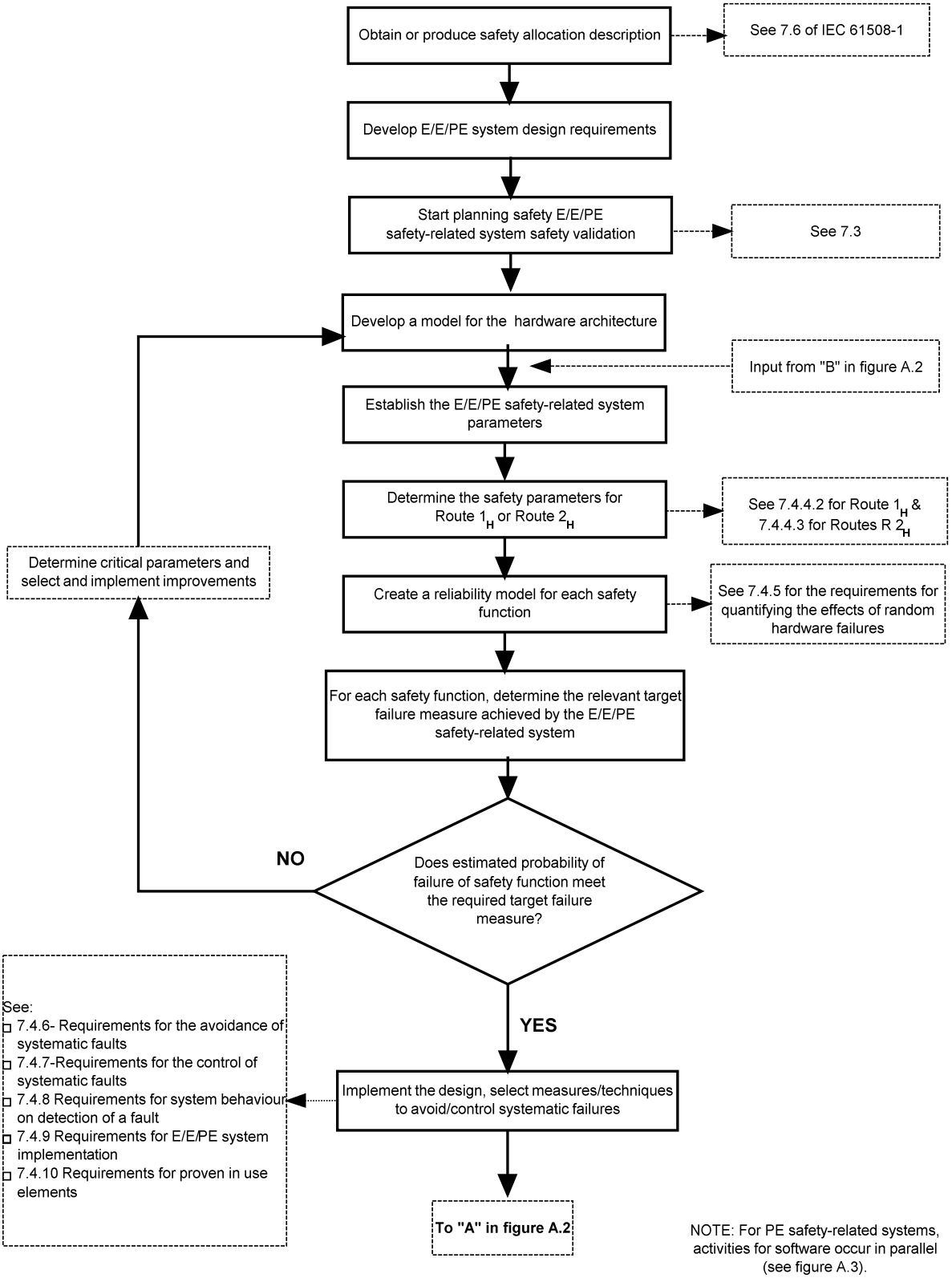


Figure A.1 – Application of IEC 61508-2

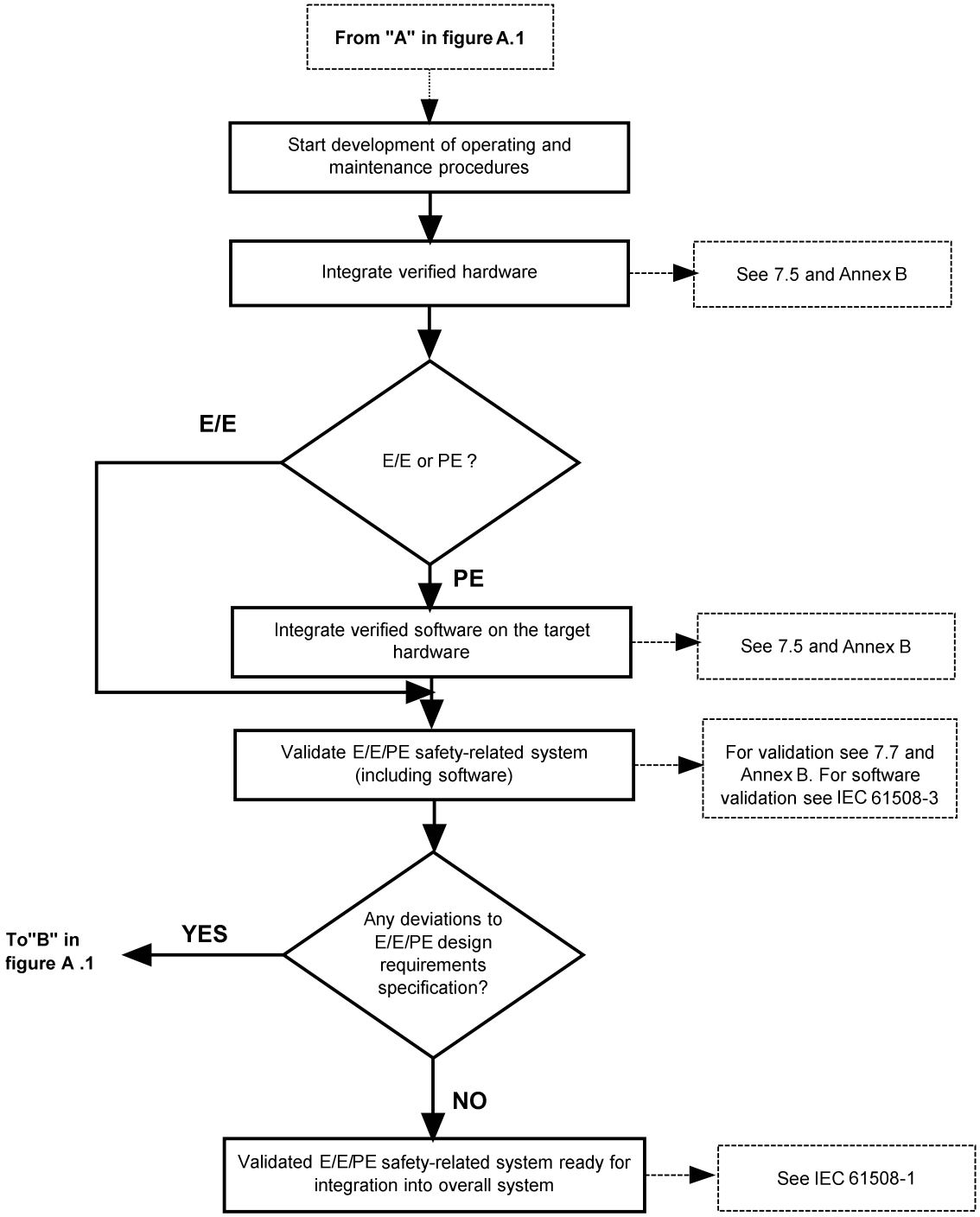


Figure A.2 – Application of IEC 61508-2 (Figure A.1 *continued*)

A.3 Functional steps in the application of IEC 61508-3

Functional steps for IEC 61508-3 (see Figure A.3) are as follows.

a) Obtain the requirements for the E/E/PE safety-related systems and relevant parts of the safety planning (see 7.3 of IEC 61508-2). Update the safety planning as appropriate during software development.

NOTE 1 Earlier lifecycle phases have already:

- specified the required safety functions and their associated safety integrity levels (see 7.4 and 7.5 of IEC 61508-1);
- allocated the safety functions to designated E/E/PE safety-related systems (see 7.6 of IEC 61508-1); and
- allocated functions to software within each E/E/PE safety-related system (see 7.2 of IEC 61508-2).

b) Determine the software architecture for all safety functions allocated to software (see 7.4 of IEC 61508-3 and Annex A of IEC 61508-3).

c) Review with the E/E/PE safety-related system's supplier/developer, the software and hardware architecture and the safety implications of the trade-offs between the software and hardware (see Figure 4 of IEC 61508-2). Iterate if required.

d) Start the planning for software safety verification and validation (see 7.3 and 7.9 of IEC 61508-3).

e) Design, develop and verify/test the software according to the:

- software safety planning;
- software safety integrity level; and
- software safety lifecycle.

f) Complete the final software verification activity and integrate the verified software onto the target hardware (see 7.5 of IEC 61508-3), and in parallel develop the software aspects of the procedures for users and maintenance staff to follow when operating the system (see 7.6 of IEC 61508-3, and A.2 k)).

g) Together with the hardware developer (see 7.7 of IEC 61508-2), validate the software in the integrated E/E/PE safety-related systems (see 7.7 of IEC 61508-3).

h) Hand over the results of the software safety validation to the system engineers for further integration into the overall system.

i) If modification of the E/E/PE safety-related system software is required during operational life then re-activate this IEC 61508-3 phase as appropriate (see 7.8 of IEC 61508-3).

A number of activities run across the software safety lifecycle. These include verification (see 7.9 of IEC 61508-3) and functional safety assessment (see Clause 8 of IEC 61508-3).

In applying the above steps, software safety techniques and measures appropriate to the required safety integrity are selected. To aid in this selection, tables have been formulated ranking the various techniques/measures against the four safety integrity levels (see Annex A of IEC 61508-3). Cross-referenced to the tables is an overview of each technique and measure with references to further sources of information (see Annex C of IEC 61508-7).

Worked examples in the application of the safety integrity tables are given in Annex E, and IEC 61508-7 includes a probabilistic approach to determining software safety integrity for pre-developed software (see Annex D of IEC 61508-7).

NOTE 2 In applying the above steps, alternative measures to those specified in the standard are acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

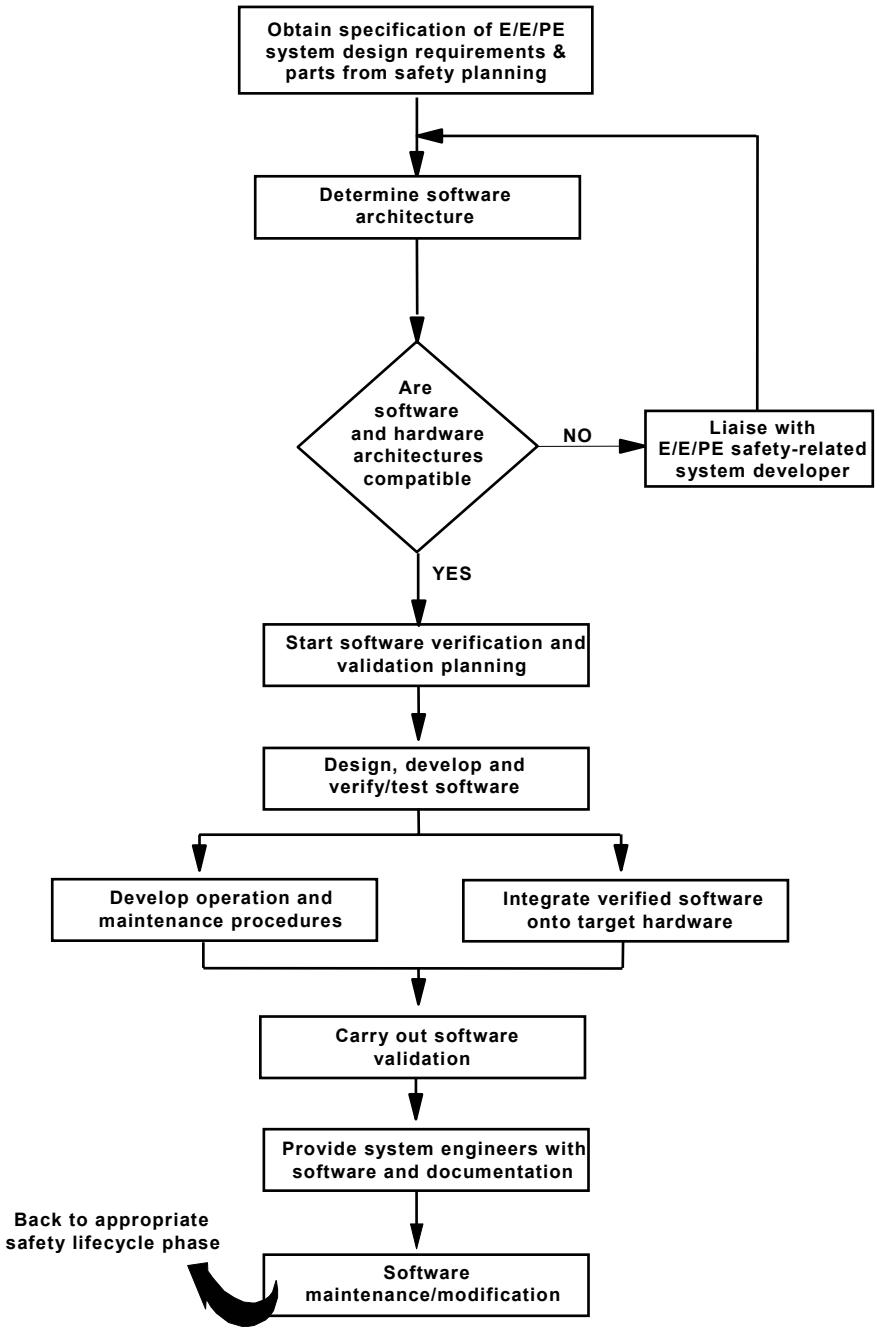


Figure A.3 – Application of IEC 61508-3

Annex B
(informative)

Example of technique for evaluating probabilities of hardware failure

B.1 General

This annex provides possible techniques for calculating the probabilities of hardware failure for E/E/PE safety-related systems installed in accordance with IEC 61508-1, IEC 61508-2 and IEC 61508-3. The information provided is informative in nature and should not be interpreted as the only evaluation techniques that might be used. It does, however, provide both a relatively simple approach for assessing the capability of E/E/PE safety-related systems and guidelines to use alternative techniques derived from the classical reliability calculations techniques.

NOTE 1 System architectures stated in this part are provided by way of examples and should not be considered exhaustive as there are many other architectures that may be used.

NOTE 2 See ISA-TR84.00.02-2002 [17] in the Bibliography.

A number of reliability techniques are more or less straightforwardly usable for the analysis of hardware safety integrity of E/E/PE safety-related systems. Classically, they are sorted according to the two following point of views:

– static (Boolean) versus dynamic (states/transitions) models;

– analytical versus Monte Carlo simulation calculations.

Boolean models encompass all models describing the static logical links between the elementary failures and the whole system failure. Reliability Block Diagrams (RBD) (see C.6.4 of IEC 61508-7 and IEC 61078 [4]) and Fault Trees (FT) (see B.6.6.5 and B.6.6.9 of IEC 61508-7) and IEC 61025 [18] belong to Boolean models.

States/transitions models encompass all models describing how the system behaves (jumps from states to states) according to arising events (failures, repairs, tests, etc.). Markovian (see B.6.6.6 of IEC 61508-7 and IEC 61165 [5]), Petri nets (see B.2.3.3 and B.6.6.10 of IEC 61508-7 and IEC 62551 [19]) and formal language models belong to states/transitions models. Two Markovian approaches are investigated: a simplified approach based on specific formulae (B.3) and a general approach allowing direct calculations on Markov graphs (B.5.2). For non Markovian safety systems, Monte Carlo simulations can be used instead. With present time personal computers this is achievable even for SIL 4 calculations. Subclauses B.5.3 and B.5.4 of this annex provides guidelines about handling Monte Carlo simulations (see B.6.6.8 of IEC 61508-7) on behavioural models based on Petri nets and formal languages modelling.

The simplified approach which is presented first is based on RBD graphical representations and specific Markovian formulae obtained from Taylor's developments and slightly conservative underlying hypotheses described in B.3.1.

All these methods can be used for the majority of safety related systems and, when deciding which technique to use on any particular application, it is very important that the user of a particular technique is competent in using the technique and this may be more important than the technique which is actually used. It is the responsibility of the analyst to verify that the underling hypotheses of any particular method are satisfied or any adjustments are required to obtain an adequate realist conservative result. In case of poor reliability data or dominant common cause failure, it may be sufficient to use the simplest model / techniques. Whether the loss of accuracy is significant can only be determined in the particular circumstances.

If software programmes are used to perform the calculations then the practitioner shall have an understanding of the formulae/techniques used by the software package to ensure its use is suitable for the specific application. The practitioner should also verify the software package by checking its output with some manual calculated test cases.

Where a failure of the EUC control system places a demand on the E/E/PE safety-related system, then the probability of a hazardous event occurring also depends on the probability of failure of the EUC control system. In that situation, it is necessary to consider the possibility of co-incident failure of components in the EUC control system and the E/E/PE safety-related system due to common cause failure mechanisms. The existence of such failures could lead to a higher than expected residual risk unless properly addressed.

B.2 Considerations about basic probabilistic calculations

B.2.1 Introduction

The reliability block diagram (RBD) on Figure B.1 is representing a safety loop made of three sensors (A, B, C), one logic solver (D), two final elements (E, F), and common cause failures (CCF).

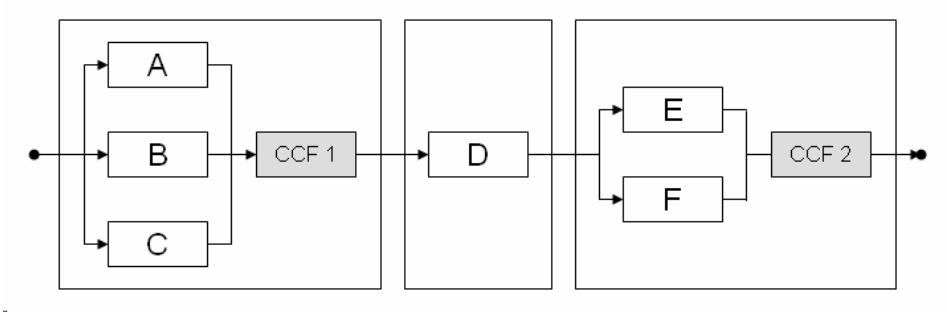


Figure B.1 – Reliability Block Diagram of a whole safety loop

This facilitates the identification of five failure combinations leading to the E/E/PE safety-related system failure. Each of them is a so-called minimal cut set:

– (A, B, C) is a triple failure;

– (E, F) is a double failure;

– (D) (CCF1) (CCF2) are single failures.

B.2.2 Low demand E/E/PE safety-related system

When a E/E/PE safety-related system is used in low demand mode, the standard requires that its PFD_{avg} (i.e. its average unavailability) be assessed. This is simply the ratio $MDT(T)/T$ where $MDT(T)$ is the mean down time over the period [0, T] of the E/E/PE safety-related system.

For safety system the probability of failure is, normally, very low and the probability to have two minimal cut sets at the same time is negligible. Therefore, the sum of the mean down times due to each cut sets gives a conservative estimate of the mean down time of the whole system. From Figure B.1 we find:

$$MDT \approx MDT^{ABC} + MDT^{D} + MDT^{EF}$$

Dividing by T gives:

$$PFD_{avg} \approx PFD_{avg}^{ABC} + PFD_{avg}^{D} + PFD_{avg}^{EF}$$

Therefore, for parts in series, PFD_{avg} calculations are very similar to those performed with ordinary probabilities when they are very small compared to 1.

However for parallel parts where multiple failure are required before the loss of the function like (E, F), it is clear that MDT^{EF} may not be calculated straightforwardly from MDT^{E} and MDT^{F}: The (E,F) system's *MDT* has to be calculated as

$$MDT^{EF} = \int_0^T PFD^E(t) PFD^F(t) dt$$

Therefore, ordinary probabilistic calculations (additions and multiplications) are no longer valid for PFD_{avg} calculations (integrals) of parts in parallel. PFD_{avg} has not the same properties as a genuine probability and its assimilation with a genuine probability is likely to lead to non conservative results. In particular, it is not possible to obtain the PFD_{avg} of an E/E/PE safety-related system just by combining in a conventional way the $PFD_{avg,i}$ of its components. As this is sometimes encouraged by commercial Boolean software packages, analysts should be vigilant to avoid such non conservative calculations which are undesirable when dealing with safety.

EXAMPLE For a redundant (1oo2) channel with a dangerous undetected failure rate λ_{DU} with a proof test interval τ, an incorrect probability model calculation could give $(\lambda_{DU}.\tau)^2/4$ when the actual result is $(\lambda_{DU}.\tau)^2/3$.

Calculations may be performed analytically or by using Monte Carlo simulation. This annex describes how to do that by using conventional reliability models based on Boolean (RBD or Fault-trees) or, states/transitions models (Markov, Petri nets, etc.).

B.2.3 Continuous or high demand mode E/E/PE safety-related system

B.2.3.1 General *PFH* formula

When an E/E/PE safety-related system is used in continuous or high demand mode, the standard requires the calculation of its *PFH* (i.e. its average frequency of dangerous failure). This is the average of the so called unconditional failure intensity (also called failure frequency) *w(t)* over the period of interest:

$$PFH(T) = \frac{1}{T}\int_0^T w(t) dt$$

Where the E/E/PE safety-related system is working in continuous mode and is the ultimate safety barrier, then the overall safety-related system failure will lead directly to a potentially hazardous situation. Hence for failures that cause the loss of the overall safety function no overall safety-related system repair can be considered in the calculations. However, if the failure of the overall safety-related system does not lead directly to the potential hazard due to some other safety barrier or equipment failure then it may be possible to consider the detection and repair of the safety-related system in its risk reduction calculation.

B.2.3.2 Un-reliability case (e.g. single barrier working in continuous mode)

This case is relevant when E/E/PE safety-related system working in continuous mode is the ultimate safety barrier. Therefore a potential hazard can occur as soon as it is failing. No overall system failures are acceptable over the period of interest.

In this case the *PFH* may be calculated by using the unreliability over the period of interest:

$$F(T):\ PFH(T) = \frac{1 - \exp\left[-\int_0^T \Lambda(t)dt\right]}{T} = \frac{F(T)}{T}$$

The overall system failure rate, $\Lambda(t)$, may be time dependent or constant.

When it is time dependant, we have: $PFH(T) = \frac{1 - \exp(-\Lambda_{avg}.T)}{T} \approx \Lambda_{avg}$

When the system is made of components completely and quickly repairable with constant failure and repair rates (e.g. dangerous detected failures), $\Lambda(t)$ reaches quickly an asymptotic constant value Λ_{as} and, when $PFH(T) << 1.$, we have:

$$PFH(T) = \frac{1 - \exp(-\Lambda_{as}.T)}{T} \approx \Lambda_{as} = \frac{1}{MTTF}$$

Λ_{as} exists only when the E/E/PE safety-related system working in continuous mode comprises only safe and DD failures (i.e. quickly detected and repaired). No repair of failures that can directly cause the overall failure of the safety function can be considered. For a redundant configuration where it is relevant to consider proof tests, then the asymptotic failure rate is not relevant and the previous equations have to be used. It is the job of the analyst to verify which case is relevant.

B.2.3.3 Unavailability case (e.g. multiple safety barriers)

When the E/E/PE safety-related system working in continuous mode is not the ultimate barrier, its failures only increase the demand frequency on other safety barriers, or when it is working in the high demand mode, such that it is possible to detect (automatically or manually) and repair a fault that could cause the direct loss of the safety function within the expected demand period. In this case its overall failures can be repaired and *PFH* may be calculated from the availability, *A(t),* and from the conditional failure intensity, $\Lambda_V(t)$, of the system.

Again, when the system is made of components completely and quickly repairable (i.e. when, in any degraded situation, there is an high probability to come back quickly to a good working state), $\Lambda_V(t)$ reaches quickly its asymptotic value, Λ_{vas}, which, in addition, is also a good approximation of the true asymptotic overall system failure rate, $\Lambda_{as,}$ introduced in B.2.3.2.

This leads to the following approximations:

$$PFH = \frac{1}{MUT + MDT} = \frac{1}{MTBF} \approx \frac{1}{MUT} \approx \frac{1}{MTTF}$$

where

MUT is the acronym for Mean Up Time;

MDT is the acronym for Mean Down Time;

MTBF is the acronym for Mean Time Between Failure; and

MTTF is the acronym for Mean Time To Failure.

B.2.3.4 Failure rate considerations

Several formulae above use the overall system failure rate $\Lambda(t)$. Its evaluation is not so easy and some reminders are needed.

Series structures are very simple to handle as failure rates can be added. From Figure B.1, we can write $\Lambda(t) = \Lambda^{abc}(t) + \lambda^{CCF1}(t) + \lambda^{d}(t) + \Lambda^{ef}(t) + \lambda^{CCF2}(t)$ where $\Lambda(t)$ is the overall failure rate of the E/E/PE safety-related system and $\Lambda^{abc}(t)$, $\lambda^{CCF1}(t)$, $\lambda^{d}(t)$, $\Lambda^{ef}(t)$ and $\lambda^{CCF2}(t)$ the failure rates of the five minimal cut sets.

For parallel structures this is not so simple because there are no simple relationships with individual components failure rates. For example, let us consider cut set (E, F):

1) When E and F cannot be immediately be restored (e.g. DU failures), $\Lambda^{ef}(t)$ varies continuously from 0 to λ (failure rate of E or F). An asymptotic value is reached when one of the two components is likely to have failed. This is a very slow process as this arises when t becomes larger than $1/\lambda$. This asymptotic value will be never reached in actual life if E and F are periodically proof tested with a test interval $\tau << 1/\lambda$.
2) When E and F are restored in a relatively short period of time (e.g. DD failures), $\Lambda^{ef}(t)$ goes very fast to an asymptotic value $\Lambda^{ef}_{As} = 2\lambda^2/\mu$ which can be used as an equivalent constant failure rate. It is reached when t becomes greater than two or three times the larger *MTTR* of the components. It is a particular case of the completely and quickly repairable systems discussed above.

Therefore, in the general case, evaluating the overall system failure rates imply more complex calculations than the more simple series structure.

B.3 Reliability block diagram approach, assuming constant failure rate

B.3.1 Underlying hypothesis

The calculations are based on the following assumptions:

– the resulting average probability of failure on demand for the system is less than 10^{-1}, or the resultant average frequency of dangerous failure for the system is less than 10^{-5} h^{-1}

NOTE 1 This assumption means that the E/E/PE safety-related system is within the scope of IEC 61508 series and within the SIL 1 band (see Tables 2 and 3 of IEC 61508-1).

– component failure rates are constant over the life of the system;

– the sensor (input) subsystem comprises the actual sensor(s) and any other components and wiring, up to but not including the component(s) where the signals are first combined by voting or other processing (for example for two sensor channels, the configuration would be as shown in Figure B.2);

– the logic subsystem comprises the component(s) where the signals are first combined, and all other components up to and including where final signal(s) are presented to the final element subsystem;

– the final element (output) subsystem comprises all the components and wiring which process the final signal(s) from the logic subsystem including the final actuating component(s);

– the hardware failure rates used as inputs to the calculations and tables are for a single channel of the subsystem (for example, if 2oo3 sensors are used, the failure rate is for a single sensor and the effect of 2oo3 is calculated separately);

– the channels in a voted group all have the same failure rates and diagnostic coverage;

– the overall hardware failure rate of a channel of the subsystem is the sum of the dangerous failure rate and safe failure rate for that channel, which are assumed to be equal;

NOTE 2 This assumption affects the safe failure fraction (see Annex C of IEC 61508-2), but the safe failure fraction does not affect the calculated values for probability of failure given in this annex.

– for each safety function, there is perfect proof testing and repair (i.e. all failures that remain undetected are detected by the proof test), but for the effects of a non-perfect proof test see B.3.2.5;

– the proof test interval is at least an order of magnitude greater than the MRT;

– for each subsystem there is a single proof test interval and MRT;

– the expected interval between demands is at least an order of magnitude greater than the proof test interval;

– for all subsystems operating in low demand mode of operation, and for 1oo2, 1oo2D,1oo3 and 2oo3, voted groups operating in high demand or continuous mode of operation, the fraction of failures specified by the diagnostic coverage is both detected and repaired within the MTTR used to determine hardware safety integrity requirements;

EXAMPLE If a MTTR of 8 h is assumed, this includes the diagnostic test interval which is typically less than 1 h, the remainder being the MRT.

NOTE 3 For 1oo2, 1oo2D, 1oo3 and 2oo3 voted groups, it is assumed that any repair is on-line. Configuring an E/E/PE safety-related system, so that on any detected fault the EUC is put into a safe state, improves the average probability of failure on demand. The degree of improvement depends on the diagnostic coverage.

– for 1oo1 and 2oo2 voted groups operating in high demand or continuous mode of operation, the E/E/PE safety-related system always achieves a safe state after detecting a dangerous fault; to achieve this, the expected interval between demands is at least an order of magnitude greater than the diagnostic test intervals, or the sum of the diagnostic test intervals and the time to achieve a safe state is less than the process safety time;

NOTE 4 For process safety time see 3.6.20 of IEC 61508-4.

– when a power supply failure removes power from a de-energize-to-trip E/E/PE safety-related system and initiates a system trip to a safe state, the power supply does not affect the average probability of failure on demand of the E/E/PE safety-related system; if the system is energized to trip, or the power supply has failure modes that can cause unsafe operation of the E/E/PE safety-related system, the power supply should be included in the evaluation;

– where the term channel is used, it is limited to only that part of the system under discussion, which is usually either the sensor, logic or final element subsystem;

– the abbreviated terms are described in Table B.1.

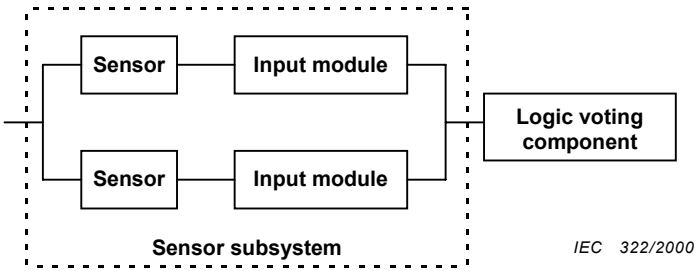


Figure B.2 – Example configuration for two sensor channels

Table B.1 – Terms and their ranges used in this annex
(applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and 2oo3)

Abbre-viation	Term (units)	Parameter ranges in Tables B.2 to B.5 and B.10 to B.13
T_1	Proof test interval (hour)	One month (730 h)[1] Three months (2 190 h)[1] Six months (4 380 h) One year (8 760 h) Two years (17 520 h)[2] Ten years (87 600 h)[2]
MTTR	Mean time to restoration (hour)	8 h NOTE MTTR = MRT = 8 hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT.
MRT	Mean repair time (hour)	8 h NOTE MTTR = MRT = 8 hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT
DC	Diagnostic coverage (expressed as a fraction in the equations and as a percentage elsewhere)	0 % 60 % 90 % 99 %
β	The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere) (Tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta_D$)	2 % 10 % 20 %
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere) (Tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta_D$)	1 % 5 % 10 %
λ_{DU}	Dangerous Undetected failure rate (per hour) of a channel in a subsystem	$0{,}05 \times 10^{-6}$ $0{,}25 \times 10^{-6}$ $0{,}5 \times 10^{-6}$ $2{,}5 \times 10^{-6}$ 5×10^{-6} 25×10^{-6}
PFD_G	Average probability of failure on demand for the group of voted channels (If the sensor, logic or final element subsystem comprises of only one voted group, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively)	
PFD_S	Average probability of failure on demand for the sensor subsystem	
PFD_L	Average probability of failure on demand for the logic subsystem	

Abbre-viation	Term (units)	Parameter ranges in Tables B.2 to B.5 and B.10 to B.13
PFD_{FE}	Average probability of failure on demand for the final element subsystem	
PFD_{SYS}	Average probability of failure on demand of a safety function for the E/E/PE safety-related system	
PFH_G	Average frequency of dangerous failure for the group of voted channels (if the sensor, logic or final element subsystem comprises of only one voted group, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively)	
PFH_S	Average frequency of dangerous failure for the sensor subsystem	
PFH_L	Average frequency of dangerous failure for the logic subsystem	
PFH_{FE}	Average frequency of dangerous failure for the final element subsystem	
PFH_{SYS}	Average frequency of dangerous failure of a safety function for the E/E/PE safety-related system	
λ	Total failure rate (per hour) of a channel in a subsystem	
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal to 0,5 λ (assumes 50 % dangerous failures and 50 % safe failures)	
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)	
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)	
λ_{SD}	Detected safe failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected safe failure rates within the channel of the subsystem)	
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem)	
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)	
t_{CE}'	Channel equivalent mean down time (hour) for 1oo2D architecture (this is the combined down time for all the components in the channel of the subsystem)	
t_{GE}'	Voted group equivalent mean down time (hour) for 1oo2D architecture (this is the combined down time for all the channels in the voted group)	
T_2	Interval between demands (h)	
K	Fraction of the success of the autotest circuit in the 1oo2D system	
PTC	Proof Test Coverage	
[1] High demand or continuous mode only.		
[2] Low demand mode only.		

B.3.2 Average probability of failure on demand (for low demand mode of operation)

B.3.2.1 Procedure for calculations

The average probability of failure on demand of a safety function for the E/E/PE safety-related system is determined by calculating and combining the average probability of failure on demand for all the subsystems which together implement the safety function. Since in this annex the probabilities are small, this can be expressed by the following (see Figure B.3):

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

where

PFD_{SYS} is the average probability of failure on demand of a safety function for the E/E/PE safety-related system;

PFD_S is the average probability of failure on demand for the sensor subsystem;

PFD_L is the average probability of failure on demand for the logic subsystem; and

PFD_{FE} is the average probability of failure on demand for the final element subsystem.

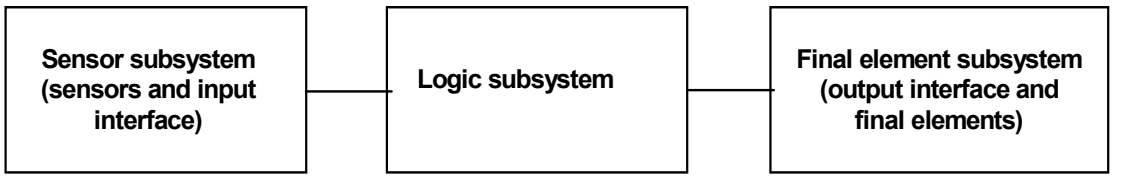


Figure B.3 – Subsystem structure

To determine the average probability of failure on demand for each of the subsystems, the following procedure should be adhered to for each subsystem in turn.

a) Draw the block diagram showing the sensor subsystem (input) components, logic subsystem components or final element subsystem (output) components. For example, sensor subsystem components may be sensors, barriers, input conditioning circuits; logic subsystem components may be processors and scanning devices; and final element subsystem components may be output conditioning circuits, barriers and actuators. Represent each subsystem as one or more 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 or 2oo3 voted groups.

b) Refer to the relevant table from Tables B.2 to B.5 which are for six-month, one-year, two-year and 10-year proof test intervals. These tables also assume an 8 h mean time to restoration for each failure once it has been revealed.

c) For each voted group in the subsystem, select from the relevant table of Tables B.2 to B.5:

   – architecture (for example, 2oo3);

   – diagnostic coverage of each channel (for example, 60 %);

   – the dangerous failure rate (per hour), λ_D, of each channel (for example, $2{,}5 \times 10^{-06}$);

   – the common cause failure β-factors, β and β_D, for the interaction between the channels in the voted group (for example, 2 % and 1 % respectively).

NOTE 1 It is assumed that every channel in the voted group has the same diagnostic coverage and failure rate (see Table B.1).

NOTE 2 It is assumed in Tables B.2 to B.5 (and in Tables B.10 to B.13) that the β-factor in the absence of diagnostic tests (also used for undetected dangerous failures in the presence of diagnostic tests), β, is 2 times the β-factor for failures detected by the diagnostic tests, β_D.

d) Obtain, from the relevant table from Tables B.2 to B.5, the average probability of failure on demand for the voted group.

e) If the safety function depends on more than one voted group of sensors or actuators, the combined average probability of failure on demand of the sensor or final element subsystem, PFD_S or PFD_{FE}, is given in the following equations, where PFD_{Gi} and PFD_{Gj} is the average probability of failure on demand for each voted group of sensors and final elements respectively:

$$PFD_S = \sum_i PFD_{Gi}$$

$$PFD_{FE} = \sum_j PFD_{Gj}$$

The formula used in all the equations for both *PFD* and system failure rate are all a function of component failure rate and mean down time (*MDT*). Where there are a number of elements in the system and it is required to calculate the combined elements overall *PFD* or system failure rate, then it is often necessary to use a single value for the *MDT* in the equations. However each element may have different failure detection mechanisms with different *MDT* and different elements may have different *MDT* values for the same failure mechanisms, in which case it is necessary to calculate a single value for the *MDT* which can represent all the elements in the path. This can be accomplished by considering the total paths overall failure rate then proportioning the individual *MDT's* equivalent to their failure rate contribution to the total failure rate under consideration.

As an example, if there are two elements in series but one with a proof test, T_1, and the other with a proof test, T_2, then the equivalent single value for the *MDT* is:

$$\lambda_T = \lambda_1 + \lambda_2$$

and

$$MDT_E = \frac{\lambda_1}{\lambda_T}\left(\frac{T_1}{2}\right) + \frac{\lambda_2}{\lambda_T}\left(\frac{T_2}{2}\right)$$

B.3.2.2 Architectures for low demand mode of operation

NOTE 1 This subclause should be read sequentially, since equations which are valid for several architectures are only stated where they are first used.

NOTE 2 The equations are based on the assumptions listed in B.3.1.

NOTE 3 The following examples are typical configurations and are not intended to be an exhaustive.

B.3.2.2.1 1oo1

This architecture consists of a single channel, where any dangerous failure leads to a failure of the safety function when a demand arises.

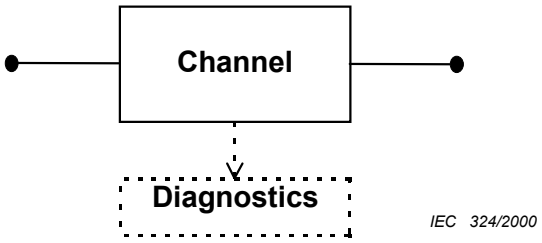


Figure B.4 – 1oo1 physical block diagram

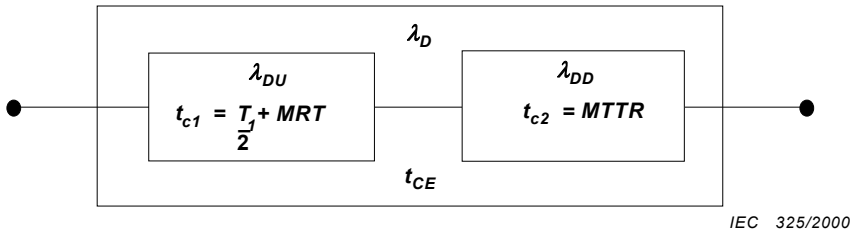


Figure B.5 – 1oo1 reliability block diagram

Figures B.4 and B.5 contain the relevant block diagrams. The dangerous failure rate for the channel is given by

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

Figure B.5 shows that the channel can be considered to comprise of two components, one with a dangerous failure rate λ_{DU} resulting from undetected failures and the other with a dangerous failure rate λ_{DD} resulting from detected failures. It is possible to calculate the channel equivalent mean down time t_{CE}, adding the individual down times from both components, t_{c1} and t_{c2}, in direct proportion to each component's contribution to the probability of failure of the channel:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

For every architecture, the detected dangerous failure rate and the undetected dangerous failure rate are given by

$$\lambda_{DU} = \lambda_D(1 - DC); \quad \lambda_{DD} = \lambda_D DC$$

For a channel with down time t_{CE} resulting from dangerous failures

$$PFD = 1 - e^{-\lambda_D t_{CE}}$$
$$\approx \lambda_D t_{CE} \qquad \text{since } \lambda_D t_{CE} << 1$$

Hence, for a 1oo1 architecture, the average probability of failure on demand is

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

B.3.2.2.2 1oo2

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be a dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

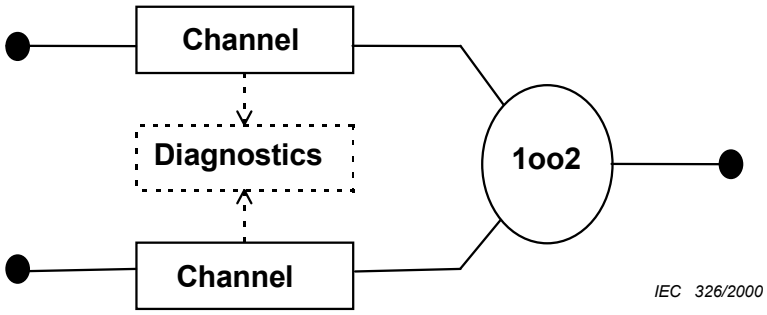


Figure B.6 – 1oo2 physical block diagram

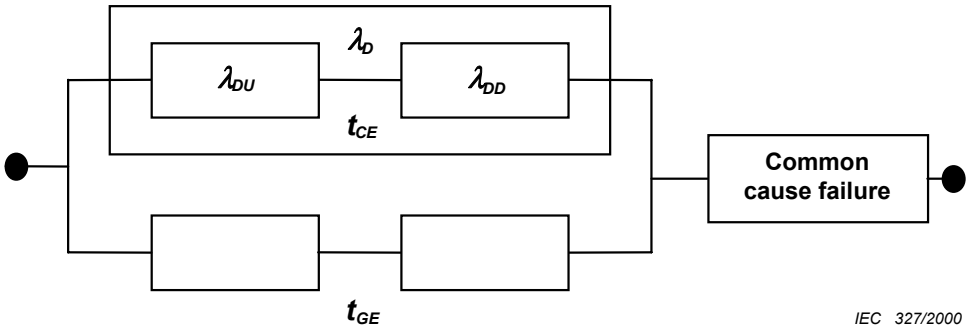


Figure B.7 – 1oo2 reliability block diagram

Figures B.6 and B.7 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1, but now it is necessary to also calculate the system equivalent down time t_{GE}, which is given by

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

The average probability of failure on demand for the architecture is

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

B.3.2.2.3 2oo2

This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

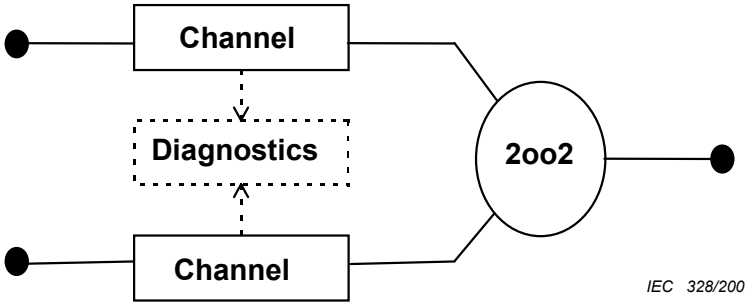


Figure B.8 – 2oo2 physical block diagram

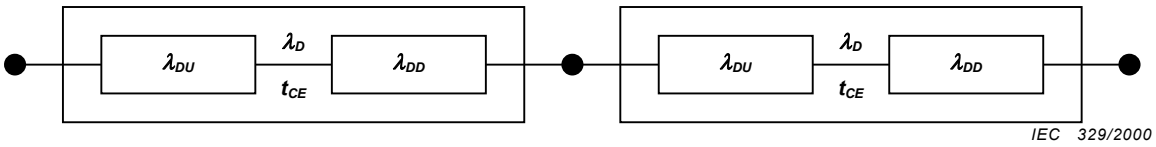


Figure B.9 – 2oo2 reliability block diagram

Figures B.8 and B.9 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1, and the average probability of failure on demand for the architecture is

$$PFD_G = 2\lambda_D t_{CE}$$

B.3.2.2.4 1oo2D

This architecture consists of two channels connected in parallel. During normal operation, both channels need to demand the safety function before it can take place. In addition, if the diagnostic tests in either channel detect a fault then the output voting is adapted so that the overall output state then follows that given by the other channel. If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated to either channel, then the output goes to the safe state. In order to detect a discrepancy between the channels, either channel can determine the state of the other channel via a means independent of the other channel. The channel comparison / switch over mechanism may not be 100 % efficient therefore K represents the efficiency of this inter-channel comparison / switch mechanism, i.e. the output may remain on the 2oo2 voting even with one channel detected as faulty.

NOTE The parameter K will need to be determined by an FMEA.

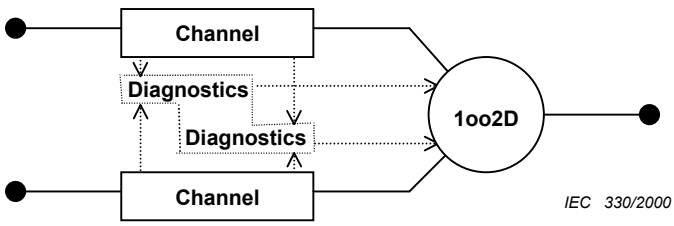


Figure B.10 – 1oo2D physical block diagram

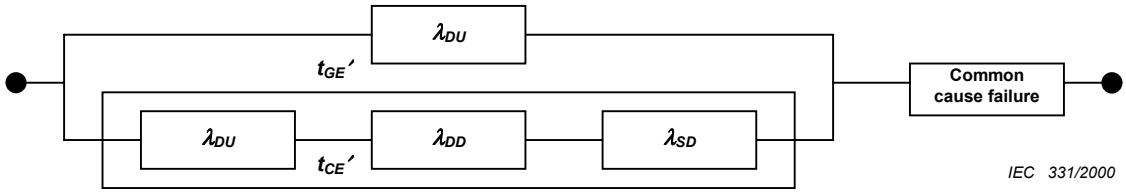


Figure B.11 – 1oo2D reliability block diagram

The detected safe failure rate for every channel is given by

$$\lambda_{SD} = \lambda_S DC$$

Figures B.10 and B.11 contain the relevant block diagrams. The values of the equivalent mean down times differ from those given for the other architectures in B.3.2.2 and hence are labelled t_{CE}' and t_{GE}'. Their values are given by

$$t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + (\lambda_{DD} + \lambda_{SD})}$$

$$t_{GE}' = \frac{T_1}{3} + MRT$$

The average probability of failure on demand for the architecture is

$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}'\,t_{GE}' + 2(1-K)\lambda_{DD}t_{CE}' + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

B.3.2.2.5 2oo3

This architecture consists of three channels connected in parallel with a majority voting arrangement for the output signals, such that the output state is not changed if only one channel gives a different result which disagrees with the other two channels.

It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

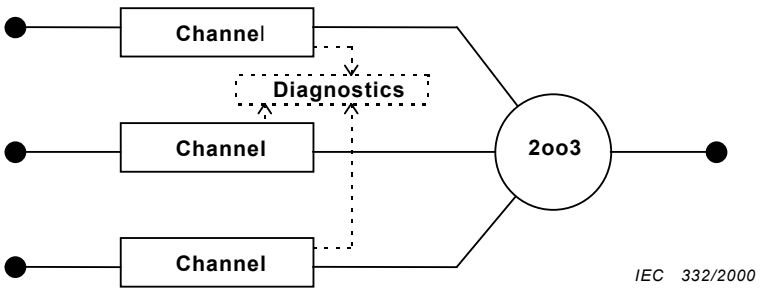


Figure B.12 – 2oo3 physical block diagram

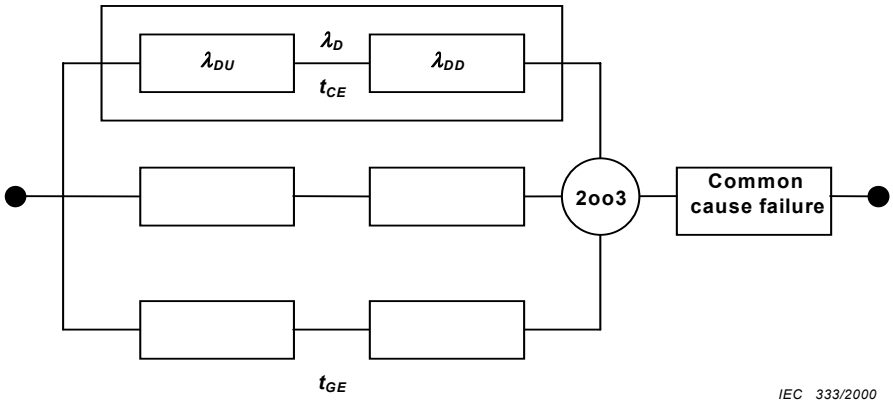


Figure B.13 – 2oo3 reliability block diagram

Figures B.12 and B.13 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1 and the value of t_{GE} is as given in B.3.2.2.2. The average probability of failure on demand for the architecture is

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

B.3.2.2.6 1oo3

This architecture consists of three channels connected in parallel with a voting arrangement for the output signals, such that the output state follows 1oo3 voting.

It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

The reliability diagram will be the same as for the 2oo3 case but with voting 1oo3. The value of t_{CE} is as given in B.3.2.2.1 and the value of t_{GE} is as given in B.3.2.2.2. The average probability of failure on demand for the architecture is

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

Where

IEC 332/2000

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

B.3.2.3 Detailed tables for low demand mode of operation

Table B.2 – Average probability of failure on demand for a proof test interval of six months and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see Note 2)	**0 %**	1,1E-04			5,5E-04			1,1E-03		
	60 %	4,4E-05			2,2E-04			4,4E-04		
	90 %	1,1E-05			5,7E-05			1,1E-04		
	99 %	1,5E-06			7,5E-06			1,5E-05		
1oo2	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo2 (see Note 2)	**0 %**	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,3E-05			1,1E-04			2,3E-04		
	99 %	3,0E-06			1,5E-05			3,0E-05		
1oo2D (see Note 3)	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	1,4E-06	4,9E-06	9,3E-06	7,1E-06	2,5E-05	4,7E-05	1,4E-05	5,0E-05	9,3E-05
	90 %	4,3E-07	1,3E-06	2,4E-06	2,2E-06	6,6E-06	1,2E-05	4,3E-06	1,3E-05	2,4E-05
	99 %	6,0E-08	1,5E-07	2,6E-07	3,0E-07	7,4E-07	1,3E-06	6,0E-07	1,5E-06	2,6E-06
2oo3	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,6E-05	1,1E-04	2,7E-05	1,1E-04	2,2E-04
	60 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo3	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see Note 2)	**0 %**	5,5E-03			1,1E-02			5,5E-02		
	60 %	2,2E-03			4,4E-03			2,2E-02		
	90 %	5,7E-04			1,1E-03			5,7E-03		
	99 %	7,5E-05			1,5E-04			7,5E-04		
1oo2	**0 %**	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	90 %	1,2E-05	5,6E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04	1,5E-04	6,0E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,4E-05	6,6E-05	1,3E-04
2oo2 (see Note 2)	**0 %**	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,3E-03			1,1E-02		
	99 %	1,5E-04			3,0E-04			1,5E-03		
1oo2D (see Note 3)	**0 %**	1,5E-04	5,8E-04	1,1E-03	3,8E-04	1,2E-03	2,3E-03	5,0E-03	9,0E-03	1,4E-02
	60 %	7,7E-05	2,5E-04	4,7E-04	1,7E-04	5,2E-04	9,5E-04	1,3E-03	3,0E-03	5,1E-03
	90 %	2,2E-05	6,6E-05	1,2E-04	4,5E-05	1,3E-04	2,4E-04	2,6E-04	6,9E-04	1,2E-03
	99 %	3,0E-06	7,4E-06	1,3E-05	6,0E-06	1,5E-05	2,6E-05	3,0E-05	7,4E-05	1,3E-04
2oo3	**0 %**	2,3E-04	6,5E-04	1,2E-03	6,8E-04	1,5E-03	2,5E-03	1,3E-02	1,5E-02	1,9E-02
	60 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,3E-03	3,9E-03	5,9E-03
	90 %	1,2E-05	5,7E-05	1,1E-04	2,7E-05	1,2E-04	2,3E-04	2,4E-04	6,8E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,7E-06	1,3E-05	2,6E-05	1,5E-05	6,7E-05	1,3E-04
1oo3	**0 %**	1,1E-04	5,5E-04	1,1E-03	2,2E-04	1,1E-03	2,2E-03	1,4E-03	5,7E-03	1,1E-02
	60 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	90 %	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.3 – Average probability of failure on demand for a proof test interval of one year and mean time to restoration of 8 h

Architecture	*DC*	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	**0 %**	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,2E-05			1,1E-04			2,2E-04		
	99 %	2,6E-06			1,3E-05			2,6E-05		
1oo2	**0 %**	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,0E-06	4,4E-05	8,8E-05	1,9E-05	8,9E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
2oo2 (see Note 2)	**0 %**	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,5E-05			2,2E-04			4,5E-04		
	99 %	5,2E-06			2,6E-05			5,2E-05		
1oo2D (see Note 3)	**0 %**	4,5E-06	2,2E-05	4,4E-05	2,4E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	2,8E-06	9,8E-06	1,9E-05	1,4E-05	4,9E-05	9,3E-05	2,9E-05	9,9E-05	1,9E-04
	90 %	8,5E-07	2,6E-06	4,8E-06	4,3E-06	1,3E-05	2,4E-05	8,5E-06	2,6E-05	4,8E-05
	99 %	1,0E-07	2,8E-07	5,0E-07	5,2E-07	1,4E-06	2,5E-06	1,0E-06	2,8E-06	5,0E-06
2oo3	**0 %**	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,2E-05	2,4E-04	4,5E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,5E-06	4,5E-05	8,8E-05	2,1E-05	9,1E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo3	**0 %**	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	8,8E-06	4,4E-05	8,8E-05	1,8E-05	8,8E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06

Architecture	*DC*	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	**0 %**	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,2E-03			1,1E-02		
	99 %	1,3E-04			2,6E-04			1,3E-03		
1oo2	**0 %**	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60 %	1,1E-04	4,6E-04	9,0E-04	2,8E-04	9,7E-04	1,8E-03	3,4E-03	6,6E-03	1,1E-02
	90 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,9E-06	2,4E-05	4,8E-05	2,6E-05	1,2E-04	2,4E-04
2oo2 (see Note 2)	**0 %**	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,5E-03			2,2E-02		
	99 %	2,6E-04			5,2E-04			2,6E-03		
1oo2D (see Note 3)	**0 %**	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,9E-03	1,8E-02	2,5E-02	3,4E-02
	60 %	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03	3,9E-03	7,1E-03	1,1E-02
	90 %	4,4E-05	1,3E-04	2,4E-04	9,1E-05	2,7E-04	4,8E-04	5,8E-04	1,4E-03	2,5E-03
	99 %	5,2E-06	1,4E-05	2,5E-05	1,0E-05	2,8E-05	5,0E-05	5,4E-05	1,4E-04	2,5E-04
2oo3	**0 %**	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,8E-03	5,6E-03	4,8E-02	5,0E-02	5,3E-02
	60 %	1,6E-04	5,1E-04	9,4E-04	4,8E-04	1,1E-03	2,0E-03	8,4E-03	1,1E-02	1,5E-02
	90 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
	99 %	2,5E-06	1,2E-05	2,4E-05	5,1E-06	2,4E-05	4,8E-05	3,1E-05	1,3E-04	2,5E-04
1oo3	**0 %**	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,7E-03	1,3E-02	2,3E-02
	60 %	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03	1,0E-03	4,5E-03	8,9E-03
	90 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,8E-06	2,4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.4 – Average probability of failure on demand for a proof test interval of two years and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	**0 %**	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,4E-05			2,2E-04			4,4E-04		
	99 %	4,8E-06			2,4E-05			4,8E-05		
1oo2	**0 %**	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,9E-05	8,9E-05	1,8E-04	3,9E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
2oo2 (see Note 2)	**0 %**	8,8E-04			4,4E-03			8,8E-03		
	60 %	3,5E-04			1,8E-03			3,5E-03		
	90 %	8,8E-05			4,4E-04			8,8E-04		
	99 %	9,6E-06			4,8E-05			9,6E-05		
1oo2D (see Note 3)	**0 %**	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	9,0E-04
	60 %	5,7E-06	2,0E-05	3,7E-05	2,9E-05	9,9E-05	1,9E-04	6,0E-05	2,0E-04	3,7E-04
	90 %	1,7E-06	5,2E-06	9,6E-06	8,5E-06	2,6E-05	4,8E-05	1,7E-05	5,2E-05	9,6E-05
	99 %	1,9E-07	5,4E-07	9,8E-07	9,5E-07	2,7E-06	4,9E-06	1,9E-06	5,4E-06	9,8E-06
2oo3	**0 %**	9,5E-06	4,4E-05	8,8E-05	6,2E-05	2,3E-04	4,5E-04	1,6E-04	5,0E-04	9,3E-04
	60 %	3,6E-06	1,8E-05	3,5E-05	2,1E-05	9,0E-05	1,8E-04	4,7E-05	1,9E-04	3,6E-04
	90 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,3E-07	4,6E-06	9,2E-06
1oo3	**0 %**	8,8E-06	4,4E-05	8,8E-05	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,8E-05	8,8E-05	1,8E-04	3,5E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	**0 %**	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,4E-03			2,2E-02		
	99 %	2,4E-04			4,8E-04			2,4E-03		
1oo2	**0 %**	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60 %	2,8E-04	9,7E-04	1,8E-03	7,5E-04	2,1E-03	3,8E-03	1,2E-02	1,8E-02	2,5E-02
	90 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	99 %	4,7E-06	2,3E-05	4,6E-05	9,5E-06	4,6E-05	9,2E-05	5,4E-05	2,4E-04	4,6E-04
2oo2 (see Note 2)	**0 %**	4,4E-02			8,8E-02			>1E-01		
	60 %	1,8E-02			3,5E-02			>1E-01		
	90 %	4,4E-03			8,8E-03			4,4E-02		
	99 %	4,8E-04			9,6E-04			4,8E-03		
1oo2D (see Note 3)	**0 %**	1,1E-03	2,7E-03	4,8E-03	3,4E-03	6,6E-03	1,1E-02	6,7E-02	7,7E-02	9,0E-02
	60 %	3,8E-04	1,1E-03	1,9E-03	9,6E-04	2,3E-03	4,0E-03	1,3E-02	1,9E-02	2,6E-02
	90 %	9,0E-05	2,6E-04	4,8E-04	1,9E-04	5,4E-04	9,8E-04	1,5E-03	3,2E-03	5,3E-03
	99 %	9,6E-06	2,7E-05	4,9E-05	1,9E-05	5,4E-05	9,8E-05	1,0E-04	2,8E-04	5,0E-04
2oo3	**0 %**	2,3E-03	3,7E-03	5,6E-03	8,3E-03	1,1E-02	1,4E-02	1,9E-01	1,8E-01	1,7E-01
	60 %	4,8E-04	1,1E-03	2,0E-03	1,6E-03	2,8E-03	4,4E-03	3,2E-02	3,5E-02	4,0E-02
	90 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,4E-03	4,0E-03	6,0E-03
	99 %	4,8E-06	2,3E-05	4,6E-05	1,0E-05	4,7E-05	9,2E-05	6,9E-05	2,5E-04	4,8E-04
1oo3	**0 %**	4,6E-04	2,2E-03	4,4E-03	1,0E-03	4,5E-03	8,9E-03	2,4E-02	3,7E-02	5,5E-02
	60 %	1,8E-04	8,8E-04	1,8E-03	3,6E-04	1,8E-03	3,5E-03	3,1E-03	9,9E-03	1,8E-02
	90 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	99 %	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.5 – Average probability of failure on demand for a proof test interval of ten years and a mean time to restoration of 8 h

Architecture	*DC*	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	**0 %**	2,2E-03			1,1E-02			2,2E-02		
	60 %	8,8E-04			4,4E-03			8,8E-03		
	90 %	2,2E-04			1,1E-03			2,2E-03		
	99 %	2,2E-05			1,1E-04			2,2E-04		
1oo2	**0 %**	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	1,9E-05	8,9E-05	1,8E-04	1,1E-04	4,6E-04	9,0E-04	2,7E-04	9,6E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
2oo2 (see Note 2)	**0 %**	4,4E-03			2,2E-02			4,4E-02		
	60 %	1,8E-03			8,8E-03			1,8E-02		
	90 %	4,4E-04			2,2E-03			4,4E-03		
	99 %	4,5E-05			2,2E-04			4,5E-04		
1oo2D (see Note 3)	**0 %**	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	2,9E-05	9,9E-05	1,9E-04	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03
	90 %	8,4E-06	2,6E-05	4,8E-05	4,3E-05	1,3E-04	2,4E-04	9,0E-05	2,6E-04	4,8E-04
	99 %	8,9E-07	2,6E-06	4,8E-06	4,5E-06	1,3E-05	2,4E-05	8,9E-06	2,6E-05	4,8E-05
2oo3	**0 %**	6,2E-05	2,3E-04	4,5E-04	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,7E-03	5,6E-03
	60 %	2,1E-05	9,0E-05	1,8E-04	1,6E-04	5,0E-04	9,3E-04	4,7E-04	1,1E-03	2,0E-03
	90 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,3E-05	2,4E-04	4,5E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
1oo3	**0 %**	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03
	60 %	1,8E-05	8,8E-05	1,8E-04	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05

Architecture	*DC*	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	**0 %**	>1E-01			>1E-01			>1E-01		
	60 %	4,4E-02			8,8E-02			>1E-01		
	90 %	1,1E-02			2,2E-02			>1E-01		
	99 %	1,1E-03			2,2E-03			1,1E-02		
1oo2	**0 %**	1,8E-02	2,4E-02	3,2E-02	6,6E-02	7,4E-02	8,5E-02	>1E-01	>1E-01	>1E-01
	60 %	3,4E-03	6,6E-03	1,1E-02	1,2E-02	1,8E-02	2,5E-02	>1E-01	>1E-01	>1E-01
	90 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,8E-03	4,9E-03	1,8E-02	2,5E-02	3,5E-02
	99 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
2oo2 (see Note 2)	**0 %**	>1E-01			>1E-01			>1E-01		
	60 %	8,8E-02			>1E-01			>1E-01		
	90 %	2,2E-02			4,4E-02			>1E-01		
	99 %	2,2E-03			4,5E-03			2,2E-02		
1oo2D (see Note 3)	**0 %**	1,8E-02	2,5E-02	3,3E-02	6,6E-02	7,7E-02	9,0E-02	1,6E+00	1,5E+00	1,4E+00
	60 %	3,9E-03	7,1E-03	1,1E-02	1,3E-02	1,9E-02	2,6E-02	2,6E-01	2,7E-01	2,8E-01
	90 %	5,7E-04	1,4E-03	2,5E-03	1,5E-03	3,1E-03	5,2E-03	2,0E-02	2,7E-02	3,5E-02
	99 %	4,6E-05	1,3E-04	2,4E-04	9,5E-05	2,7E-04	4,9E-04	6,0E-04	1,5E-03	2,5E-03
2oo3	**0 %**	4,8E-02	5,0E-02	5,3E-02	1,9E-01	1,8E-01	1,7E-01	4,6E+00	4,0E+00	3,3E+00
	60 %	8,3E-03	1,1E-02	1,4E-02	3,2E-02	3,5E-02	4,0E-02	7,6E-01	7,1E-01	6,6E-01
	90 %	6,9E-04	1,5E-03	2,6E-03	2,3E-03	3,9E-03	5,9E-03	4,9E-02	5,4E-02	6,0E-02
	99 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
1oo3	**0 %**	4,7E-03	1,3E-02	2,3E-02	2,4E-02	3,7E-02	5,5E-02	2,5E+00	2,0E+00	1,6E+00
	60 %	1,0E-03	4,5E-03	8,9E-03	3,0E-03	9,8E-03	1,8E-02	1,7E-01	1,8E-01	1,9E-01
	90 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,8E-03	1,3E-02	2,4E-02
	99 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

B.3.2.4 Example for low demand mode of operation

Consider a safety function requiring a SIL 2 system. Suppose that the initial assessment for the system architecture, based on previous practice, is for one group of three analogue pressure sensors, voting 2oo3. The logic subsystem is a redundant 1oo2D configured PE system driving a single shut-down valve plus a single vent valve. Both the shut-down and vent valves need to operate in order to achieve the safety function. The architecture is shown in Figure B.14. For the initial assessment, a proof test period of one year is assumed.

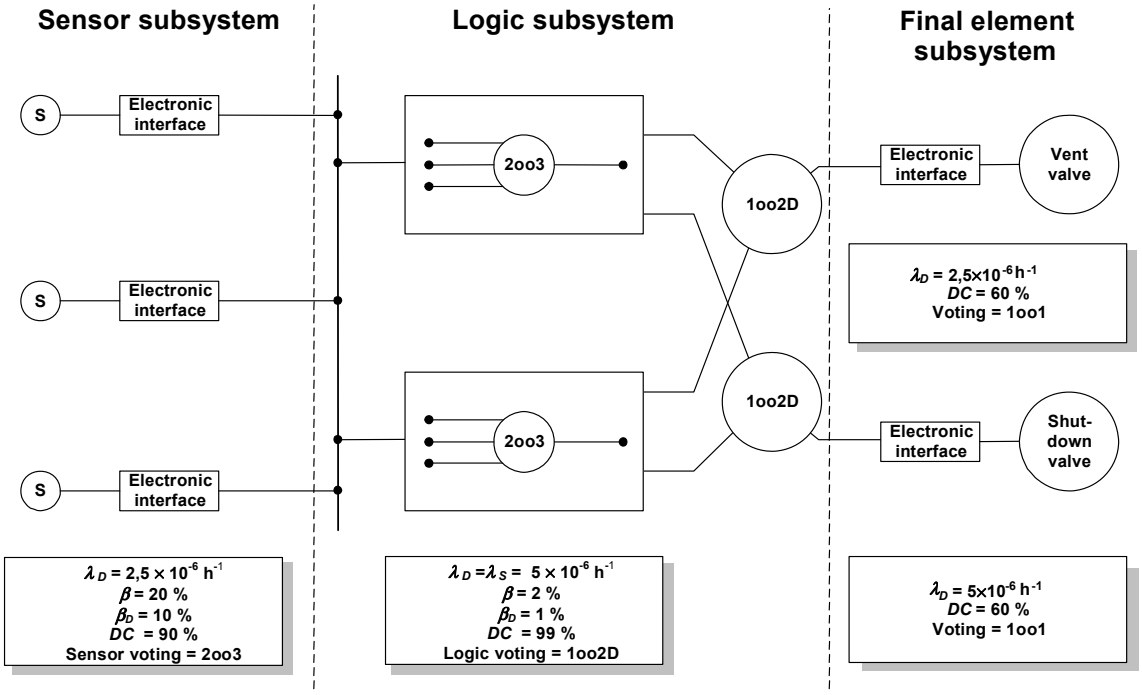


Figure B.14 – Architecture of an example for low demand mode of operation

Table B.6 – Average probability of failure on demand for the sensor subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*)

Architecture	*DC*	λ_D = 2,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0 %	6,8E-04	1,5E-03	2,5E-03
	60 %	1,6E-04	5,1E-04	9,4E-04
	90 %	2,7E-05	1,2E-04	2,3E-04
	99 %	2,5E-06	1,2E-05	2,4E-05
NOTE This table is abstracted from Table B.3.				

Table B.7 – Average probability of failure on demand for the logic subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*)

Architecture	*DC*	λ_D = 0,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2D	0 %	1,1E-03	2,7E-03	4,8E-03
	60 %	2,0E-04	9,0E-04	1,8E-03
	90 %	4,5E-05	2,2E-04	4,4E-04
	99 %	4,8E-06	2,4E-05	4,8E-05
NOTE This table is abstracted from Table B.3.				

Table B.8 – Average probability of failure on demand for the final element subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*)

Architecture	*DC*	λ_D = 2,5E-06	λ_D = 0,5E-05
1oo1	0 %	1,1E-02	2,2E-02
	60 %	4,4E-03	8,8E-03
	90 %	1,1E-03	2,2E-03
	99 %	1,3E-04	2,6E-04
NOTE This table is abstracted from Table B.3.			

From Tables B.6 to B.8 the following values are derived.

For the sensor subsystem,

$PFD_S = 2{,}3 \times 10^{-4}$

For the logic subsystem,

$PFD_L = 4{,}8 \times 10^{-6}$

For the final element subsystem,

$PFD_{FE} = 4{,}4 \times 10^{-3} + 8{,}8 \times 10^{-3}$

$= 1{,}3 \times 10^{-2}$

Therefore, for the safety function,

$PFD_{SYS} = 2{,}3 \times 10^{-4} + 4{,}8 \times 10^{-6} + 1{,}3 \times 10^{-2}$

$= 1{,}3 \times 10^{-2}$

$\equiv$ **safety integrity level 1**

To improve the system to meet safety integrity level 2, one of the following could be done:

a) change the proof test interval to six months

$PFD_S = 1{,}1 \times 10^{-4}$

$PFD_L = 2{,}6 \times 10^{-6}$

$PFD_{FE} = 2{,}2 \times 10^{-3} + 4{,}4 \times 10^{-3}$

$= 6{,}6 \times 10^{-3}$

$PFD_{SYS} = 6{,}7 \times 10^{-3}$

≡ **safety integrity level 2**

b) change the 1oo1 shutdown valve (which is the output device with the lower reliability) to 1oo2 (assuming β = 10 % and β_D = 5 %)

PFD_S = $2{,}3 \times 10^{-4}$

PFD_L = $4{,}8 \times 10^{-6}$

PFD_{FE} = $4{,}4 \times 10^{-3} + 9{,}7 \times 10^{-4}$

= $5{,}4 \times 10^{-3}$

PFD_{SYS} = $5{,}6 \times 10^{-3}$

≡ **safety integrity level 2**

B.3.2.5 Effects of a non-perfect proof test

Faults in the safety system that are not detected by either diagnostic tests or proof tests may be found by other methods arising from events such as a hazardous event requiring operation of the safety function or during an overhaul of the equipment. If the faults are not detected by such methods it should be assumed that the faults will remain for the life of the equipment. Consider a normal proof test period of T_1 where the fraction of faults detected when a proof test is performed is designated as PTC (proof test coverage) and the fraction of the faults not detected when a proof test is performed is designated as (1-PCT). These latter faults which are not detected at the proof test will only be revealed when a demand is made on the safety-related system at demand period T_2. Therefore, the proof test period (T_1) and the demand period (T_2) govern the effective down time..

An example of this is given below for a 1oo2 architecture. T_2 is the time between demands on the system:

$$t_{CE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$t_{GE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE}t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}(PTC)\left(\frac{T_1}{2} + MRT\right) +$$

$$\beta\lambda_{DU}(1-PTC)\left(\frac{T_2}{2} + MRT\right)$$

Table B.9 below gives the numeric results of a 1oo2 system with a 100 % one-year proof test (T_1 = 1 year) compared against a 90 % proof test where the demand period T_2 is assumed to be 10 years. This example has been calculated assuming a failure rate of $0{,}5 \times 10^{-5}$ per hour, a β value of 10 % and a β_D value of 5 %.

Table B.9 – Example for a non-perfect proof test

Architecture	*DC*	λ_D = 0,5E-05	
		100 % proof test	90 % proof test
		β = 10 % β_D = 5 %	β = 10 % β_D = 5 %
1oo2	0 %	2,7E-03	6,0E-03
	60 %	9,7E-04	2,0E-03
	90 %	2,3E-04	4,4E-04
	99 %	2,4E-05	4,4E-05

B.3.3 Average frequency of dangerous failure (for high demand or continuous mode of operation)

B.3.3.1 Procedure for calculations

The method for calculating the probability of failure of a safety function for an E/E/PE safety-related system operating in high demand or continuous mode of operation is identical with that for calculating for a low demand mode of operation (see B.2.1), except that average probability of failure on demand (PFD_{SYS}) is replaced with average frequency of dangerous failure (PFH_{SYS}).

The overall probability of a dangerous failure of a safety function for the E/E/PE safety-related system, PFH_{SYS}, is determined by calculating the dangerous failure rates for all the sub-systems which together provide the safety function and adding together these individual values. Since in this annex the probabilities are small, this can be expressed by the following:

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE}$$

where

PFH_{SYS} is the average frequency of dangerous failure of a safety function for the E/E/PE safety-related system;

PFH_S is the average frequency of dangerous failure for the sensor subsystem;

PFH_L is the average frequency of dangerous failure for the logic subsystem; and

PFH_{FE} is the average frequency of dangerous failure for the final element subsystem.

B.3.3.2 Architectures for high demand or continuous mode of operation

NOTE 1 This subclause should be read sequentially, since equations which are valid for several architectures are only stated where they are first used. See also B.3.2.2.

NOTE 2 The calculations are based on the assumptions listed in B.3.1.

B.3.3.2.1 1oo1

Figures B.4 and B.5 show the relevant block diagrams.

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\lambda_{DU} = \lambda_D(1 - DC); \qquad \lambda_{DD} = \lambda_D DC$$

If it is assumed that the safety system puts the EUC into a safe state on detection of any failure, for a 1oo1 architecture the following is obtained

$$PFH_G = \lambda_{DU}$$

B.3.3.2.2 1oo2

Figures B.6 and B.7 show the relevant block diagrams. The value of t_{CE} is as given in B.3.3.2.1. If it is assumed that the safety system puts the EUC into a safe state once there is detection of a failure in both channels and taking a conservative approach, the following is obtained

$$PFH_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})(1 - \beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU}$$

B.3.3.2.3 2oo2

Figures B.8 and B.9 show the relevant block diagrams. If it is assumed that each channel is put into a safe state on detection of any fault, for a 2oo2 architecture, the following is obtained

$$PFH_G = 2\lambda_{DU}$$

B.3.3.2.4 1oo2D

Figures B.10 and B.11 show the relevant block diagrams.

$$\lambda_{SD} = \frac{\lambda}{2} DC$$

$$t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$PFH_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}' + 2(1-K)\lambda_{DD} + \beta\lambda_{DU}$$

B.3.3.2.5 2oo3

Figures B.12 and B.13 show the relevant block diagrams. The value of t_{CE} is as given in B.3.3.2.1. If it is assumed that the safety system puts the EUC into a safe state once there is detection of a failure in any two channels and taking a conservative approach, the following is obtained

$$PFH_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU}$$

B.3.3.2.6 1oo3

Figures B.12 and B.13 show the relevant block diagrams. The value of t_{CE} and t_{GE} is as given in B.3.3.2.1. and B.3.2.2.2. If it is assumed that the safety system puts the EUC into a safe state once there is detection of a failure in the tree channels and taking a conservative approach, the following is obtained

$$PFH_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2(1-\beta)\lambda_{DU}t_{CE}t_{GE} + \beta\lambda_{DU}$$

B.3.3.3 Detailed tables for high demand or continuous mode of operation

Table B.10 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one month and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	**0 %**	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	**0 %**	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	2.1E-08	1.0E-07	2.0E-07	4.3E-08	2.0E-07	4.0E-07	2.7E-07	1.1E-06	2.1E-06
	90 %	5.1E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.5E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	**0 %**	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	8.1E-08	1.6E-07	2.6E-07	1.6E-07	3.2E-07	5.2E-07	8.7E-07	1.7E-06	2.7E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	**0 %**	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.5E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90 %	5.2E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07	6.6E-08	2.6E-07	5.1E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08
1oo3	**0 %**	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.1E-07	2.5E-06	5.0E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.11 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of three month and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	**0 %**	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	**0 %**	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90 %	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07	6.4E-08	2.6E-07	5.1E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.2E-09	2.5E-08	5.0E-08
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	**0 %**	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	8.2E-08	1.6E-07	2.6E-07	1.7E-07	3.3E-07	5.3E-07	1.0E-06	1.8E-06	2.8E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	**0 %**	9.0E-08	2.8E-07	5.3E-07	2.6E-07	6.3E-07	1.1E-06	4.5E-06	5.9E-06	7.6E-06
	60 %	2.6E-08	1.1E-07	2.0E-07	6.6E-08	2.2E-07	4.2E-07	8.5E-07	1.6E-06	2.5E-06
	90 %	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07	9.3E-08	2.9E-07	5.3E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.7E-09	2.6E-08	5.1E-08
1oo3	**0 %**	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.5E-07	2.5E-06	5.0E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.12 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of six month and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.2E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	**0 %**	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07
	60 %	4.1E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.5E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	**0 %**	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	2.4E-08	1.0E-07	2.0E-07	5.7E-08	2.1E-07	4.1E-07	6.3E-07	1.4E-06	2.3E-06
	90 %	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07	7.8E-08	2.7E-07	5.2E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	**0 %**	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	8.4E-08	1.6E-07	2.6E-07	1.8E-07	3.3E-07	5.3E-07	1.2E-06	2.0E-06	2.9E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.8E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	**0 %**	1.3E-07	3.2E-07	5.5E-07	4.2E-07	7.7E-07	1.2E-06	8.4E-06	9.2E-06	1.0E-05
	60 %	3.3E-08	1.1E-07	2.1E-07	9.1E-08	2.4E-07	4.4E-07	1.5E-06	2.1E-06	2.9E-06
	90 %	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07	1.3E-07	3.2E-07	5.6E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	6.1E-09	2.6E-08	5.1E-08
1oo3	**0 %**	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	7.1E-07	2.7E-06	5.1E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.1E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.13 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one year and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	**0 %**	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.1E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	**0 %**	1.1E-09	5.1E-09	1.0E-08	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.5E-08	1.0E-07
	60 %	4.1E-10	2.0E-09	4.0E-09	2.3E-09	1.0E-08	2.0E-08	5.0E-09	2.1E-08	4.1E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	**0 %**	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	2.9E-08	1.1E-07	2.1E-07	7.4E-08	2.3E-07	4.2E-07	1.1E-06	1.7E-06	2.6E-06
	90 %	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07	1.0E-07	3.0E-07	5.4E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.6E-09	2.6E-08	5.0E-08
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	**0 %**	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	8.9E-08	1.7E-07	2.7E-07	1.9E-07	3.5E-07	5.4E-07	1.7E-06	2.3E-06	3.2E-06
	90 %	9.6E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	1.0E-06	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	**0 %**	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-06	1.4E-06	1.6E-05	1.6E-05	1.6E-05
	60 %	4.6E-08	1.2E-07	2.2E-07	1.4E-07	2.9E-07	4.7E-07	2.8E-06	3.2E-06	3.8E-06
	90 %	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.6E-08	1.0E-07	2.1E-07	3.9E-07	6.2E-07
	99 %	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08	6.9E-09	2.7E-08	5.1E-08
1oo3	**0 %**	5.1E-08	2.5E-07	5.0E-07	1.1E-07	5.1E-07	1.0E-06	1.4E-06	3.2E-06	5.5E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.6E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.1E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

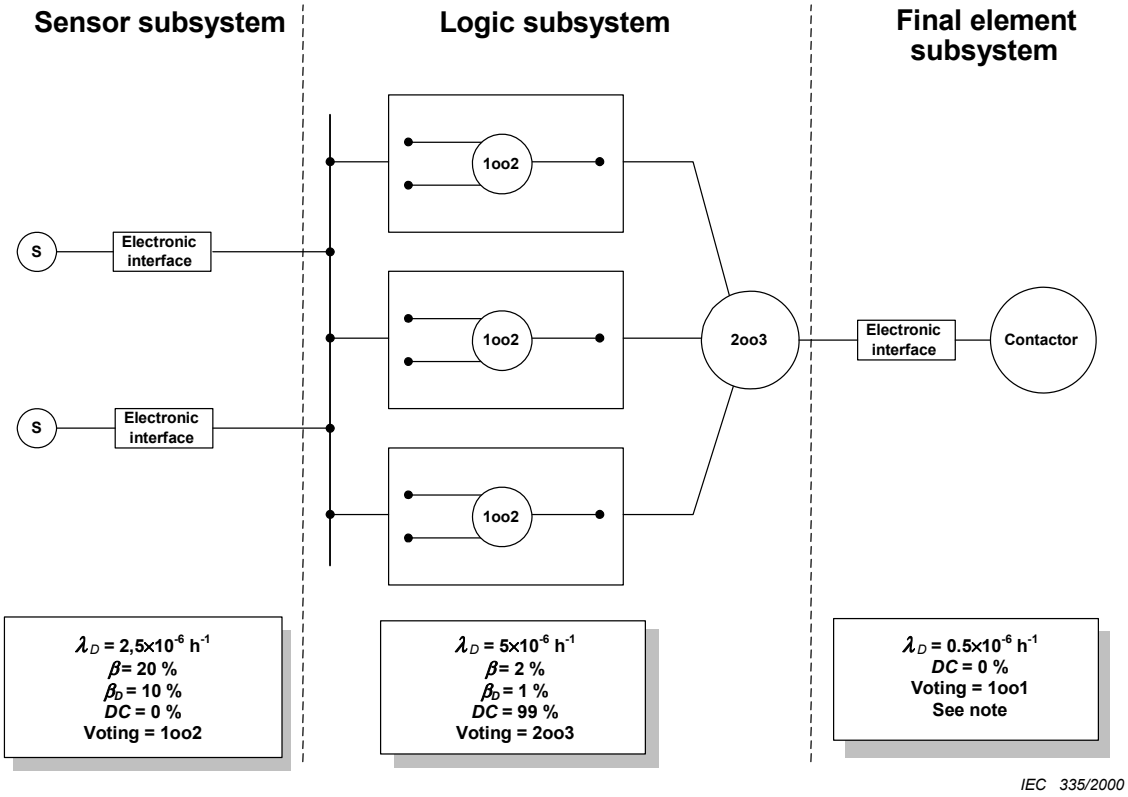
NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

B.3.3.4 Example for high demand or continuous mode of operation

Consider a safety function requiring a SIL 2 system. Suppose that the initial assessment for the system architecture, based on previous practice, is for one group of two sensors, voting 1oo2. The logic subsystem is a redundant 2oo3 configured PE system driving a single shutdown contactor. This is shown in Figure B.15 For the initial assessment, a proof test period of six months is assumed.



NOTE The final element subsystem has an overall safe failure fraction greater than 60 %.

Figure B.15 – Architecture of an example for high demand or continuous mode of operation

Table B.14 – Average frequency of a dangerous failure for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*)

Architecture	*DC*	λ_D =2,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2	0 %	7,6E-08	2,7E-07	5,2E-07
	60 %	2,4E-08	1,0E-07	2,0E-07
	90 %	5,3E-09	2,5E-08	5,0E-08
	99 %	5,0E-10	2,5E-09	5,0E-09
NOTE This table is abstracted from Table B.12.				

Table B.15 – Average frequency of a dangerous failure for the logic subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*)

Architecture	*DC*	λ_D = 0,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0 %	4,2E-07	7,7E-07	1,2E-06
	60 %	9,1E-08	2,4E-07	4,4E-07
	90 %	1,3E-08	5,3E-08	1,0E-07
	99 %	1,0E-09	5,0E-09	1,0E-08
NOTE This table is abstracted from Table B.12.				

Table B.16 – Average frequency of a dangerous failure for the final element subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*)

Architecture	*DC*	λ_D = 0,5E-06
1oo1	0 %	5,0E-07
	60 %	2,0E-07
	90 %	5,0E-08
	99 %	5,0E-09
NOTE This table is abstracted from Table B.12.		

From Tables B.14 to B.16 the following values are derived.

For the sensor subsystem,

$PFH_S = 5{,}2 \times 10^{-7}$ / h

For the logic subsystem,

$PFH_L = 1{,}0 \times 10^{-9}$/ h

For the final element subsystem,

$PFH_{FE} = 5{,}0 \times 10^{-7}$ / h

Therefore, for the safety function,

$PFH_{SYS} = 5{,}2 \times 10^{-7} + 1{,}0 \times 10^{-9} + 5{,}0 \times 10^{-7}$

$= 1{,}02 \times 10^{-6}$ / h

≡ **safety integrity level 1**

To improve the system to meet safety integrity level 2, one of the following could be done:

a) change the input sensor type and mounting to improve the defences against common cause failure, thus improving β from 20 % to 10 % and β_D from 10 % to 5 %;

$PFH_S = 2{,}7 \times 10^{-7}$ / h

$PFH_L = 1{,}0 \times 10^{-9}$ / h

$PFH_{FE} = 5{,}0 \times 10^{-7}$ / h

$PFH_{SYS} = 7{,}7 \times 10^{-7}$ / h

≡ **safety integrity level 2**

b) change the single output device to two devices in 1oo2 (β = 10 % and β_D = 5 %).

PFH_S = $5{,}2 \times 10^{-7}$ / h

PFH_L = $1{,}0 \times 10^{-9}$ / h

PFH_{FE} = $5{,}1 \times 10^{-8}$ / h

PFH_{SYS} = $5{,}7 \times 10^{-7}$ / h

≡ **safety integrity level 2**

B.4 Boolean approach

B.4.1 General

The Boolean approach encompasses the techniques representing the logical function linking the individual component failures to the overall system failure. The main Boolean models used in the reliability field are Reliability Block Diagrams (RBD), Fault Trees (FT), Event Trees and Cause Consequence Diagrams. Only the first two methods are considered here. The aim of all these methods is to represent the logical structure of the system. However, its behaviour over time is not included in these model techniques. Therefore, care has to be taken when considering behavioural features (e.g. time dependent features such as periodic proof tests) when undertaking the calculations. The first approach for using Boolean models is to split the graphical representation from the calculations. This has been described in the previous section where RBD are used to model the structure and Markovian calculations used to assess *PFD* or *PFH*. Further considerations are now discussed for probabilistic calculations on RBD and FT.

This approach is limited to components behaving reasonably independently from each other.

B.4.2 Reliability block diagram model

A lot of examples of RBD have been previously given and Figure B.1 represents, for example, a whole safety loop made of three sensors (A, B, C) working in 1oo3, one logic solver (D) and two terminal elements (E, F) working in 1oo2.

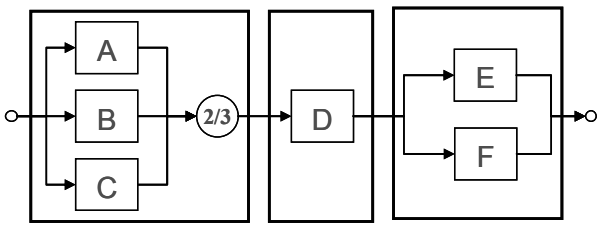


Figure B.16 – Reliability block diagram of a simple whole loop with sensors organised into 2oo3 logic

Figure B.16 shows a similar loop with sensors working in 2oo3. The main interest of such graphical representation is threefold: it remains very close to the physical structure of the system under study, it is widely used by engineers and it is a good support for discussion.

The main shortcoming is that RBD is more a method of representation than a method of analysis in itself.

For more details on RBD see C.6.4 of IEC 61508-7 and IEC 61078.

B.4.3 Fault tree model

Fault trees have exactly the same properties as RBD but in addition they constitute an effective deductive (top-down) method of analysis helping reliability engineers to develop

models step by step from the top event (unwanted or undesirable event) to the individual components failures.

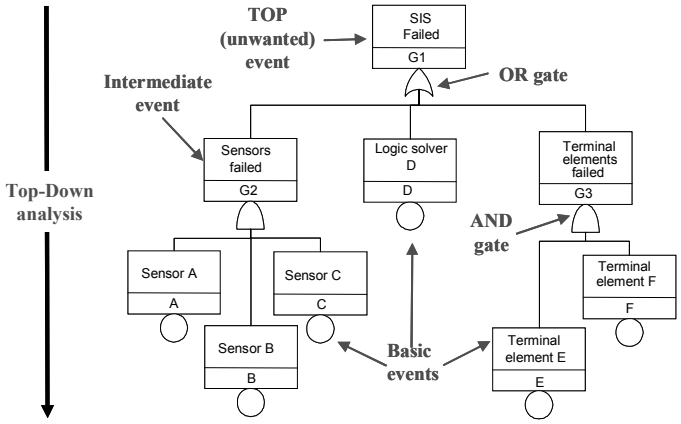


Figure B.17 – Simple fault tree equivalent to the reliability block diagram presented on Figure B.1

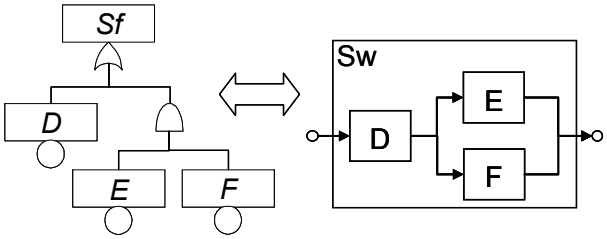
Figure B.17 shows a fault tree which is perfectly equivalent to the RBD presented on Figure B.1 but where the steps of the top-down analysis are identified (for example: E/E/PE safety-related system failed => Sensor failed => sensor A failed). In FT, the elements in series are linked by "OR gates" and element in parallel (i.e. redundant) are linked by "AND gates".

For more details on FT see B.6.6.5 and B.6.6.9 of IEC 61508-7 and IEC 61025.

B.4.4 *PFD* calculations

B.4.4.1 General overview

RBD and FT representing exactly the same things, the calculations may be handled exactly in the same way. Figure B.18 shows small equivalent FT and RBD which will be used to show the main principles of the calculations.



NOTE In this figure, italic letters are used for failed items and non-italic letters for working items.

Figure B.18 – Equivalence fault tree / reliability block diagram

The small FT represents the logical function $Sf = D \cup (E \cap F)$ where *Sf* is the failure of the system and *D, E, F* the failures of the individual components. The small RBD represents the logical function $Sw = D \cap (E \cup F)$ where Sw is the good functioning of the system and D, E, F the good functioning of the individual components. Then *Sf* = NOT Sw, and *Sf* and Sw represent exactly the same information (i.e. the logical function and its dual).

The primary use of FT and RBD is identifying the combinations of the various component failures leading to the overall system failure. They are the minimal cut sets so-called because they indicate where to cut the RBD in order that a signal sent at the input does not reach the output. In this case, there are two cut sets: the single failure (*D*) and the double failure (*E, F*).

Applying basic probabilistic mathematics on logical functions lead straightforwardly to the probability of failure P_{Sf} of the system and we obtain

$$P_{Sf} = P(D) + P(E \cap F) - P(D \cap E \cap F)$$

If the components are independent this formula becomes:

$$P_{Sf} = P_D + P_E P_F - P_D P_E P_F$$

where

P_i is the probability that component i is failed.

This formula is time independent and reflects only the logical structure of the system.

Therefore both RDB and FT are basically static, i.e. time independent models.

Nevertheless, if the probability of failure of each individual component at time *t* is independent of what happens on the other component over *[0, t]* the above formula remains valid at any time and we can write:

$$P_{Sf}(t) = P_D(t) + P_E(t)P_F(t) - P_D(t)P_E(t)P_F(t)$$

The analyst should verify if the required approximations are acceptable or not and finally, the instantaneous unavailability $U_{Sf}(t)$ of the system is obtained:

$$U_{Sf}(t) = U_D(t) + U_E(t)U_F(t) - U_D(t)U_E(t)U_F(t)$$

The conclusion is that fault trees or reliability block diagrams allow calculating directly the instantaneous unavailability $U_{Sf}(t)$ of E/E/PE safety-related systems and that additional calculations are needed and according to B.2.2:

$$PFD_{avg}(T) = \frac{1}{T} MDT(T) = \frac{1}{T}\int_0^T U_{Sf}(t)dt$$

This principle may be applied to minimal cut sets:

– single failure (*D*): $PFD^D(\tau) = \frac{1}{\tau}\int_0^\tau \lambda_D t.dt = \lambda_D \tau / 2$

– double failure (*E, F*): $PFD^{EF}(\tau) = \frac{1}{\tau}\int_0^\tau \lambda_E.\lambda_F.t^2 dt = \lambda_E \lambda_F \tau^2 / 3$

B.4.4.2 Calculations based on fault trees or reliability block diagram tools

The formula $U_{Sf}(t) = U_D(t) + U_E(t)U_F(t) - U_D(t)U_E(t)U_F(t)$ described above is only a particular case of the so-called Poincaré formula. More generally if $Sf = \bigcup_i C_i$ where (C_i) represents the minimal cut sets of the system:

$$P(\bigcup_{i-1}^{n} C_i) = \sum_{j=1}^{n} P(C_j) - \sum_{j=1}^{n}\sum_{i=1}^{j-1} P(C_j \bigcap C_i) + \sum_{j=3}^{n}\sum_{i=2}^{j-1}\sum_{k=1}^{j-1} P(C_j \bigcap C_i \bigcap C_k) - \ldots .$$

The number of minimal cut sets increases exponentially when the number of individual components increases. Then the Poincaré formula leads to a combinatory explosion of terms very quickly intractable by hand. Fortunately this problem has been analysed over the last forty years and numerous algorithms have been developed to manage such calculations. At the present time the last developments and the most powerful ones are based on the so-called Binary Decision Diagrams (BDD) which are derived from a sophisticated Shannon decomposition of the logical function.

A lot of commercial software packages mainly based on fault tree models are used daily by reliability engineers in various industry fields (nuclear, petroleum, aeronautics, automotive, etc.). They can be used for PFD_{avg} calculation but analysts have to be very cautious because some of them implement wrong PFD_{avg} calculations. The main mistake encountered is the conventional combination of the $PFD_{avg,i}$ of individual components (generally obtained simply by $\lambda_i \tau/2$) to produce a result which is supposed to be the whole system PFD_{avg}. As shown above this is wrong and non conservative.

Anyway, fault tree software packages may be used to calculate the instantaneous system unavailability $U_{Sf}(t)$ from the instantaneous unavailabilities of its components $U_i(t)$. Then the average of $U_{Sf}(t)$ may be done over the period of interest to evaluate the PFD_{avg}. Depending on the software in use this can be done by the software itself or by side calculations.

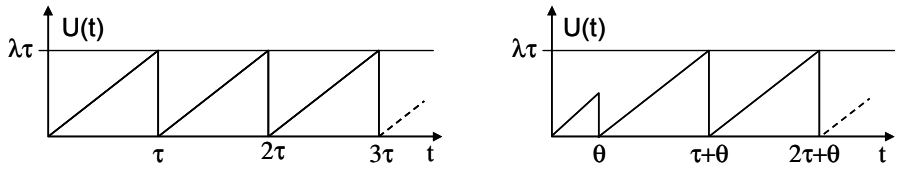


Figure B.19 – Instantaneous unavailability *U(t)* of single periodically tested components

The ideal case previously described is presented on the left of Figure B.19:

$$U_i(t) = \lambda \zeta \text{ and } \zeta = t \text{ modulo } \tau.$$

This is a so called saw-tooth curve increasing linearly from 0 to $\lambda\tau$ and restarting from 0 after a test or a repair (which are considered to be instantaneous as the EUC is stopped during them).

When several components are used in redundant structures, the tests may be staggered as shown on the right of Figure B.19 where the first test interval is different from the others. That has no impact on the PFD_{avg} or on maximum value which are equal to $\lambda\tau/2$ and $\lambda\tau$ in both cases.

Of course in less ideal cases these curves may be more complicated than that. Guidelines will be given in B.5.2 to design more accurate saw tooth curves but for the purpose of this chapter the curves presented on Figure B.19 are sufficient.

This can be applied to the small fault tree presented on Figure B.18 as illustrated in Figure B.20 (where DU means Dangerous Undetected and CCF means Common Cause Failure) . We have considered that the system was made of two redundant components (E and F) and that (D) is a common cause failure on these components. The calculation has been achieved with the following figures:

$$\lambda_{DU} = 3{,}5 \times 10^{-6}/\text{h},\ \tau = 4\ 380 \text{ h and } \beta = 1\ \%$$

A small β factor has been chosen to ensure that CCF does not dominate the result at the top and to gain a better understanding on how that works.

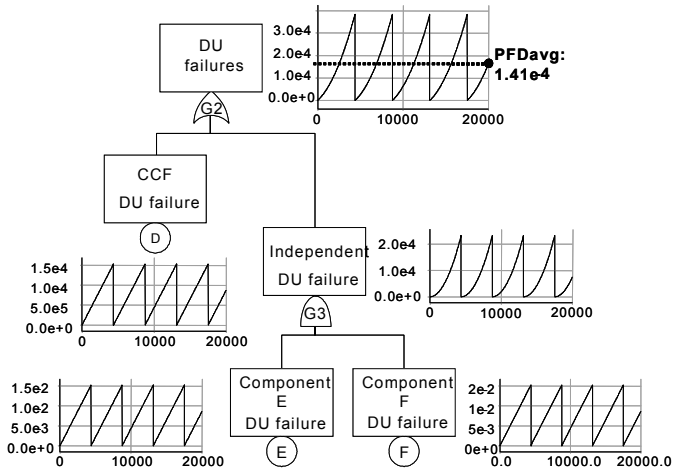


Figure B.20 – Principle of PFD_{avg} calculations when using fault trees

It is easy to recognize the kind of saw-tooth curves presented on the left hand side of Figure B.19 as inputs for *D, E* and *F*. The CCF (*D*) is tested each time *E* or *F* are tested. Then, as *E* and *F* are tested at the same time every 6 months, the CCF (*D*) is also tested every 6 months.

By using one of the algorithms developed for fault tree calculations, it is easy to draw the saw-tooth curves at outputs of all logical gates. The PFD_{avg} is calculated by averaging the result obtained for the top event. This can be performed by Fault Tree software itself or by manual calculations. $PFD_{avg} = 1{,}4 \times 10^{-4}$ is obtained and according to this standard, this meets the target failure measure for SIL 3 for a low demand mode of operation.

As shown on Figure B.20, the graphs are smooth between tests. Therefore there are no difficulties to evaluate the average, provided the instant of tests are identified and taken under consideration.

It is interesting to notice that as soon as redundancy is implemented, the saw-tooth curves at top event level are no longer linear between tests (i.e. the overall system failure rate is no longer constant).

It is also interesting to measure the impact on the PFD_{avg} of staggering the tests of the redundant components instead of performing them at the same time. This is illustrated in Figure B.21 where the tests of the component F have been staggered from those of component E by 3 months.

This has several important effects:

– CCF are now tested every 3 months (i.e. each time E is tested and each time F is tested). This proof test frequency is the double as the previous case.

– the top event saw-tooth curve has also a proof test frequency double than the one applied before.

– the saw tooth curve is less spread around its average than in the previous case.

– the PFD_{avg} has decreased to $8{,}3 \times 10^{-5}$: with this new test policy the system is SIL 4.

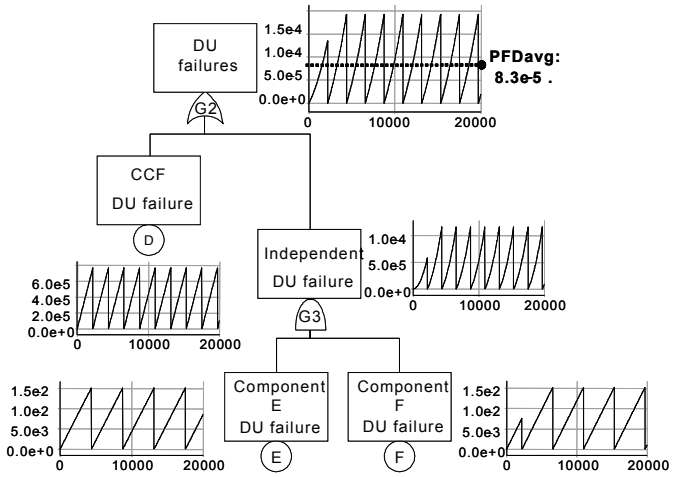


Figure B.21 – Effect of staggering the tests

If the tests are staggered and adequate procedures implemented this will increase the likelihood of detecting CCFs and is an effective method of reducing the CCF for systems operating in a low demand mode of operation. Here it has been improved from SIL 3 to SIL 4 (from hardware failures point of view and if other requirements of the IEC 61508 series are met).

Figure B.22 represents the saw-tooth curve obtained when adding a component G (λ_{DU} = 7 × 10^{-9}/h and never tested) and a component H (λ_{DU} = 4 × 10^{-8}/h tested every 2 years) in series with the system modelled on Figure B.20.

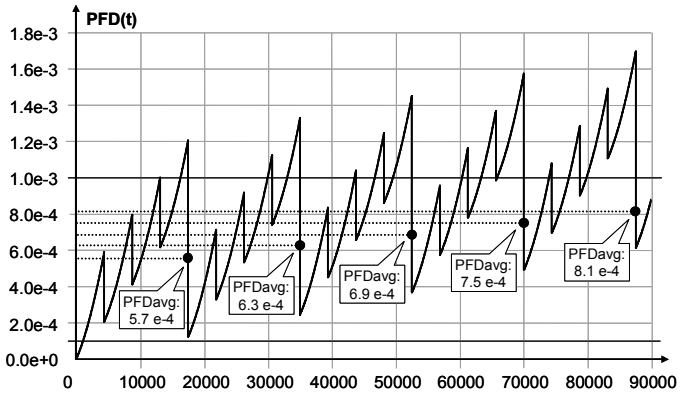


Figure B.22 – Example of complex testing pattern

The impact of the component G never tested is twofold: *PFD(t)* never goes back to zero after the test performed every two years and PFD_{avg} increases continuously (black circles corresponding to the PFD_{avg} over the period covered by the related dotted line).

Even if the elementary saw-tooth curves (like those presented on Figure B.19) are very simple, the results at the top event level may be rather complicated but this does not raise particular difficulties.

This clause aims only to illustrate the principle of the calculation by using Boolean models. Subclause B.5.2 related to the Markovian approaches, will give some guidelines to design more sophisticated input saw-tooth curves for elementary components.

It can be concluded that, when the individual components are reasonably independent there is no problem to handle PFD_{avg} calculations for E/E/PE safety-related systems by using

classical Boolean techniques. This is not so simple from theoretical point of view and the analyst doing the study should have acquired a sound knowledge of the probabilistic calculations to identify and discard the wrong PFD_{avg} implementations sometimes encountered. Provided these precautions are taken, any fault tree software package may be used for above calculations.

Boolean techniques may be also used for *PFH* calculations but the theoretical developments are beyond the purpose of this informative annex.

B.5 States/transition approaches

B.5.1 General

Boolean models are basically time-independent and the introduction of time is possible only in specific particular cases. This is rather artificial and a good knowledge of probabilistic calculations is needed to avoid mistakes. Therefore other probabilistic models, dynamic in nature may be used instead. In the reliability field they are fundamentally based on the next approach in two steps:

– identification of all the states of the system under study;

– analysis of the jumps (transitions) of the system from states to states, according to events arising and along its life.

This is why they are gathered in the category of states/transitions models.

The general approach actually consists in building a kind of automaton behaving like the system under study when events (failures, repairs, tests, etc.) are arising. As per this standard, E/E/PE safety-related systems have only discrete states, this is equivalent to building a so-called finite state automaton. Those models are dynamic in nature and may be implemented in various manners: graphic representations, specific formal languages or common programming languages. This annex presents two of them which are very different but complementary:

– Markov model which has been developed at the very beginning of the last century. It is rather well known and handled analytically;

– Petri net model which has been developed in the sixties. It is less well known (but more and more used because of its flexibility) and handled by Monte Carlo simulation.

Both are based on graphical drawings very helpful for users. Other techniques based on formal languages modelling will be very quickly analysed at the end of this clause.

B.5.2 Markovian approach

B.5.2.1 Principle of modelling

The Markovian approach is the elder of all the dynamic approaches used in the reliability field. Markov processes are split between those which are "amnesic" (homogeneous Markov processes where all transition rates are constant) and the others (semi Markov processes). As the future of a homogeneous Markov process does not depend on its past, analytical calculations are relatively straightforward. This is more difficult for semi Markov processes for which Monte Carlo simulation can be used. In this part of the IEC 61508 series, only homogeneous Markov processes are considered and the term "Markov processes" is used for the sake of simplicity (see C.6.4 of IEC 61508-7 and IEC 61165).

The fundamental basic formula of Markov processes is the following:

$$P_i(t+dt) = \sum_{k \neq i} P_k(t)\lambda_{ki}dt + P_i(t)(1 - \sum_{k \neq i} \lambda_{ik}dt)$$

In this formula, λ_{ki} is the transition rate (e.g. failure or repair rate) from state *i* to state *k*. It is self explaining: the probability to be in state *i* at *t+dt* is the probability to jump toward *i* (when in another state *k*) or to remain in state *i* (if already in this state) between *t* and *t* + *dt*.

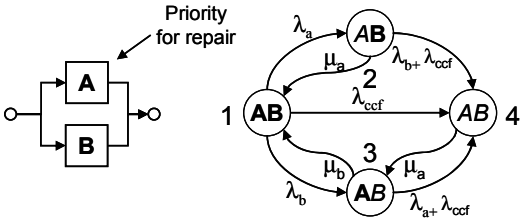


Figure B.23 – Markov graph modelling the behaviour of a two component system

There is a straightforward relationship between the above equation and a graphical representation like Figure B.23 which models a system made of two components with a single repair team (component A having priority to be repaired) and a common cause failure. In this figure **A** indicates that A is working and *A* that it has failed. As the detection times must be considered μ_a and μ_b in Figure B.23 are the restoration rates of the components (i.e. μ_a=*1/MTTR*$_a$ and μ_b=*1/MTTR*$_b$).

For example the probability to be in state 4 is simply calculated as follows:

$$P_4(t+dt) = [P_1(t)\lambda_{ccf} + P_2(t)(\lambda_b + \lambda_{ccf}) + P_3(t)(\lambda_a + \lambda_{ccf})]dt + P_4(t)(1-\mu_a dt)$$

This leads to a vectorial differential equation,

$d\vec{P}(t)/dt = [M]\vec{P}(t)$, which is conventionally solved by:

$$\vec{P}(t) = e^{t[M]}\vec{P}(0)$$

where

[*M*] is the Markovian matrix containing the transition rates and $\vec{P}(0)$ the vector of the initial conditions (generally a column vector with 1 for the perfect state an 0 for the others).

Even if an exponential of a matrix has not exactly the same properties of an ordinary exponential, it is possible to write:

$$\vec{P}(t) = e^{(t-t1)[M]}e^{t1[M]}\vec{P}(0) = e^{(t-t1)[M]}\vec{P}(t1)$$

This demonstrates the basic property of Markov processes: the knowledge of the probabilities of the states at a given instant *t1* summarizes all the past and is enough to calculate how the system evolves in the future from *t1*. This is very useful for *PFD* calculations.

Efficient algorithms have been developed and implemented in software packages a long time ago in order to solve above equations. Then, when using this approach, the analyst can focus only on the building of the models and not on the underlying mathematics even if, anyway, he has to understand at least what is described in this appendix.

Figure B.24 shows the principle of *PFD* calculations:

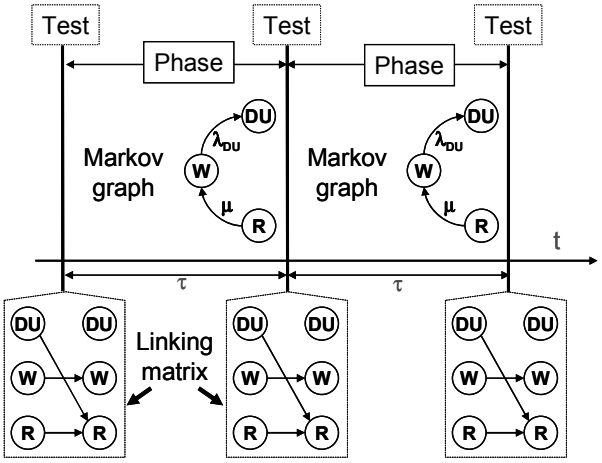


Figure B.24 – Principle of the multiphase Markovian modelling

PFD calculations are related to E/E/PE safety-related systems working in low demand mode and periodically (proof) tested. For such systems repairs are initiated only when tests are performed. The tests are singular points along the time but this is not a problem as a multi phase Markovian approach may be used to deal with.

For example, a simple system made of one periodically tested single component has three states as shown on Figure B.24: working (W), dangerous failure undetected (DU) and under repair (R).

Between tests its behaviour is modelled by the Markovian process on the upper part of Figure B.24: it can fail (W→ DU) or under repair (R→ W). As no repair may be started within a test interval, there is no transition from DU to R. Because the diagnostic of the failure has been performed before entering state R, μ is the repair rate of the component (i.e. μ=1/*MRT*) in Figure B.24.

When a test is performed (see linking matrix on Figure B.14), a repair is started if a failure has occurred (DU→ R), the component remains working if it was in a good functioning state (W→ W) and in the very hypothetical case that a repair started at the previous test is not finished, remains under repair (R→ R). A linking matrix [*L*] may by used to calculate the initial conditions at the beginning of state *i+1* from the probabilities of the states at the end of test *i*. This gives the following equation:

$$\begin{bmatrix} P_{DU}(0) \\ P_w(0) \\ P_R(0) \end{bmatrix}_{i+1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} P_{DU}(\tau) \\ P_w(\tau) \\ P_R(\tau) \end{bmatrix}_i \equiv \vec{P}_{i+1}(0) = [L]\vec{P}_i(\tau)$$

Replacing $\vec{P}_i(\tau)$ by its value, leads to an equation of recurrence which allows to calculate the initial conditions at the beginning of each test intervals:

$$\vec{P}_{i+1}(0) = [L]e^{t[M]}\vec{P}_i(0)$$

This can be used to calculate the probabilities at any time $t = i\tau + \zeta$. For example, within test interval *i,* the following is obtained:

$$\vec{P}(t) = \vec{P}_i(\zeta) = e^{\zeta[M]}\vec{P}_i(0), \quad (i-1)\tau \le t < i\tau, \quad \zeta = t \bmod \tau$$

Obtaining the instantaneous unavailability is straightforward by summing the probabilities of the states where the system is unavailable. A line vector (q_k) is helpful to express that:

$$U(t) = \sum_{k=1}^{n} q_k P_k(t)$$

where q_k = 1 if the system is unavailable in state k, and q_k = 0 otherwise.

For the simple model, $PFD(t) = U(t) = P_{DU}(t) + P_R(t)$ is obtained and the look of the saw-tooth curve obtained with this model is illustrated on Figure B.25.

The PFD_{avg} is calculated in the way previously described through the *MDT* which in turn is easy to calculate from the Mean Cumulated Times spent in the states:

$$\vec{MCT}(T) = \int_0^T \vec{P}(t)dt$$

Like for $\vec{P}(t)$, efficient algorithms are well known to perform this calculation over *[0, T]* to finally obtain: $PFD_{avg}(T) = \frac{1}{T}\sum_{k=1}^{n} q_k MCT_k(T)$

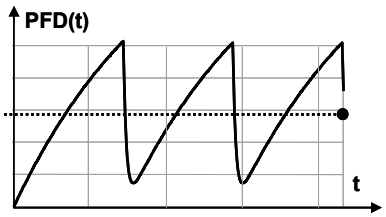


Figure B.25 – Saw-tooth curve obtained by multiphase Markovian approach

Applying this formula on the model presented on Figure B.24 leads to:

$$PFD_{avg}(T) = \frac{1}{T}\left[MCT_{DU}(T) + MCT_R(T)\right]$$

This may be reduced to the first term if the EUC is shut down during the repair.

The black circle on Figure B.25 is the PFD_{avg} of the saw-tooth curve over the whole period of calculation.

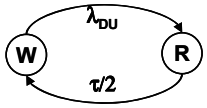


Figure B.26 – Approximated Markovian model

Note that the above calculations are often performed by using the approximated model presented on Figure B.26 where the state DU and R have been merged and where $\tau/2$ (i.e. the mean time to detect the failure) has been used as equivalent restoration time. This is valid only if the Markovian equations have been previously solved by another way in order to find this equivalence. This approximation is only applicable if the repair time is negligible. Also, the method may be very difficult for large complex systems.

The simple model of Figure B.24 may be easily improved for more realistic components. On Figure B.27, the linking matrix models a component which has both a probability, γ,to be failed due to the test (i.e. a genuine on demand failure) and a probability, σ, that the failure was not discovered by the test (by human error).

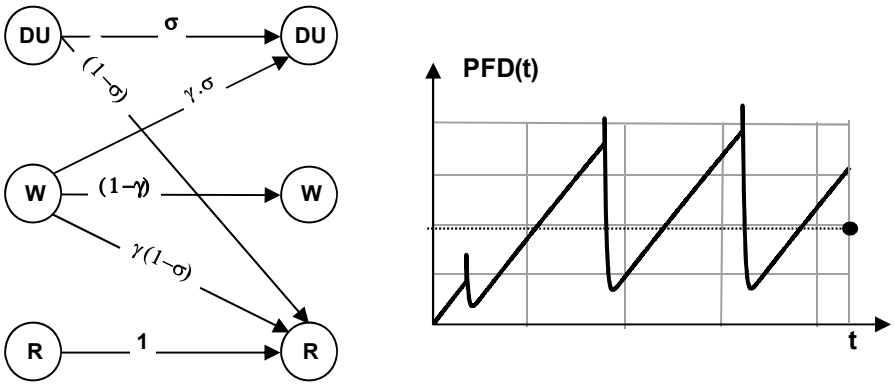


Figure B.27 – Impact of failures due to the demand itself

The look of the saw-tooth curve has changed and the jumps observed for each test correspond to the probability of on demand failure γ. Again the black circle presents the PFD_{avg}.

When a (redundant) component is disconnected to be tested, it becomes unavailable during the whole performance of the test and this contributes to its PFD_{avg}. Therefore, the test duration, π,shall be considered and an additional phase introduced between test intervals. This is shown on Figure B.28 where states R and W are modelled in this phase only for the sake of the completeness.

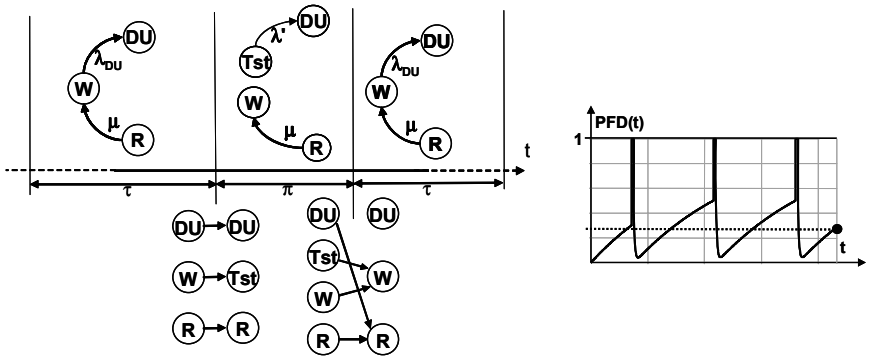


Figure B.28 – Modelling of the impact of test duration

In this Markov model, the system is unavailable in states R, DU and Tst. This is more complicated than before but the principle of calculation remains exactly the same. The behaviour of the saw-tooth curve is shown on the right. The system is unavailable during the test durations and this may be the top contribution to PFD_{avg}.

On the previous Markov graphs, only the dangerous undetected failures have been considered but the dangerous detected failure may be represented as well. The difference is that repair starts at once as it is represented on Figure B.29. Therefore μ_{DD} is the restoration rate of the component (μ_{DD} =*1/MTTR*)when μ_{DU} is its repair rate (μ_{DU}=1*/MRT)*.

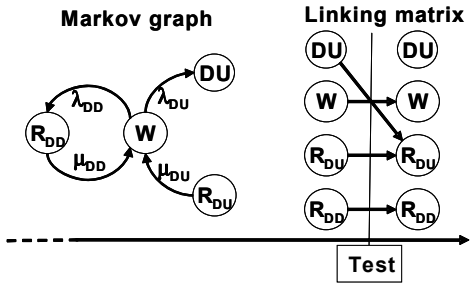


Figure B.29 – Multiphase Markovian model with both DD and DU failures

Safe failures should be represented if needed but the Markov graphs presented here are chosen to be as simple as possible.

The main problem with Markov graphs is that the number of states increases exponentially when the number of components of the system under study increases. Therefore building Markov graphs and performing above calculations without drastic approximations becomes very quickly intractable by hand.

Using an efficient Markovian software package helps to cope with calculation difficulties. There are a lot of such packages available even if they are not necessarily usable directly for PFD_{avg} calculation purpose: most of them perform instantaneous unavailability calculations but only some of them calculate the mean cumulated times spent in the states and only a few allow multiphase modelling. Anyway, there are no real difficulties to adapt them to PFD_{avg} calculations.

Concerning the modelling itself and when dependencies between components are light, Markovian and Boolean approaches can be mixed:

– Markov models are used to establish the instantaneous unavailabilities of each of the components;

– fault trees or reliability block diagrams are used to combine the individual unavailabilities to calculate the instantaneous unavailability *PFD(t)* of the whole system;

– PFD_{avg} is obtained by averaging *PFD(t)*.

This mixed approach has been described in Clause B.4 and saw-tooth curves like those on Figures B.25, B.27 and B.28 may be used as input to fault trees.

When dependencies between components cannot be neglected, some tools are available to build automatically the Markov graphs. They are based on models of a higher level than Markov models (e.g. Petri nets, formal language). Due to the combinatory explosion of the number of states, can still lead to difficulties.

This combined approach is very efficient for modelling complex systems.

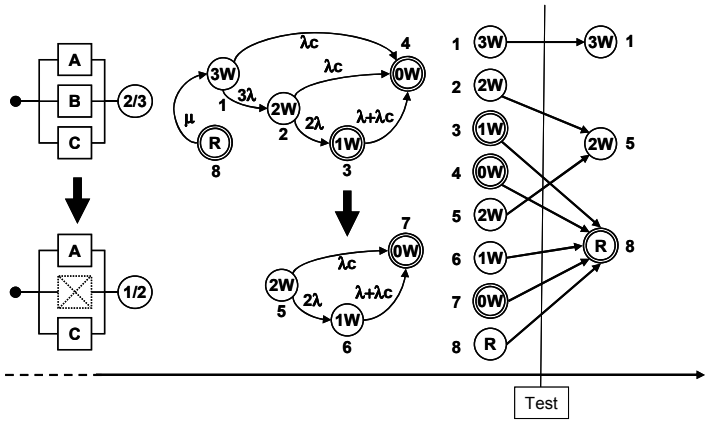


Figure B.30 – Changing logic (2oo3 to 1oo2) instead of repairing first failure

The system modelled in Figure B.30 is made of three components tested at the same time and working in 2oo3. When a failure is detected, the logic is changed from 2oo3 to 1oo2 as a 1oo2 logic is better than a 2oo3 logic from safety point of view (but worse from spurious failure point of view). It is only when a second failure is detected that the repair occurs and this consists in replacing all the three elements by three new ones. This introduces systemic constraints and it is not possible to build the behaviour of the whole system just by combining the independent behaviours of its components.

B.5.2.2 Principle of *PFH* calculations

For *PFH* calculations, the same type of multiphase Markovian modelling can be used for DU failures detected by proof tests. In order to simplify, only the principle of *PFH* calculations for DD failures which only need conventional (monophase) Markov models is shown. Of course, for E/E/PE safety-related systems working in continuous mode and having DU failures detected by periodical proof tests, the multiphase Markovian approach should be used. This does not change the principle considered hereafter.

Figure B.31 presents two Markov graphs modelling the same system made of two redundant components with a common cause failure. On the left hand side, the components (A and B) are repairable. On the right hand side, they are not repairable.

On both graphs state 4 (*AB*) is absorbing. The system remains failed after an overall failure and *P(t) = P1(t) + P2(t) + P3(t)* is the probability that no failure has occurred over *[0, t]*. Then, *R(t) = P(t)* is the reliability of the system and *F(t) = 1 - R(t) = P4(t)* is its unreliability.

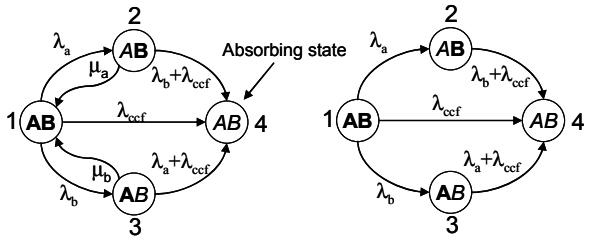


Figure B.31 – "Reliability" Markov graphs with an absorbing state

As discussed in B.2.3., this reliability model is adequate for dealing with the situation when the failure of the E/E/PE safety-related system leads immediately to a dangerous situation. Again μ_a and μ_b are the restoration rates of the components (i.e. μ_a=1/*MTTR*$_a$ and μ_b=1/*MTTR*$_b$)

Such a reliability Markov graph provides the *PFH* directly by *PFH* = *F(T)/T*. For example from Figure B.31 $PFH(T) = P4(T)/T$ (provided *P4(T)* << 1), is directly obtained.

Such a reliability Markov graph also allows the *MTTF* of the system to be calculated by the following formula:

$$MTTF = \lim_{t \to \infty} \sum_{k=1}^{n} a_k MCT_k(t)$$

In this formula $MCT_k(t)$ is the mean cumulated time spent in state *k,* and a_k = 1 if *k* is a good working state and a_k = 0 otherwise.

An upper bound is obtained by:

$$PFH \approx 1/MTTF$$

Efficient algorithms have been developed and almost all the Markovian software packages may be used for *F(T)* and *MTTF* calculations.

The above *PFH* estimations are valid in any case even if there is no overall system constant failure rate (as for the graph on the right hand side of Figure B.31). The only constraint is to use a reliability Markov graph with one (or several) absorbing state(s). Of course this holds when using a multiphase model.

When all the states are completely and quickly repairable, the overall system failure rate $\Lambda(t)$ converge quickly toward an asymptotic value Λ_{as} = 1/*MTTF*. In such graphs, except the perfect and the absorbing states, all states are quasi instantaneous (because the *MTTRs* of the components are short compared to their *MTTF*). This allows evaluating directly the overall system constant failure rates of each scenario starting from the perfect state and leading to the absorbing state. The Markov graph on the left hand side of Figure B.31 models such a completely and quickly repairable system. That is:

– $1 \rightarrow 4$: $\Lambda_{14} = \lambda_{ccf}$

– $1 \rightarrow 2 \rightarrow 4$: $\Lambda_{124} = \lambda_a . (\lambda_b + \lambda_{ccf})/[(\lambda_b + \lambda_{ccf}) + \mu_a] \approx \lambda_a . (\lambda_b + \lambda_{ccf})/\mu_a$

– $1 \rightarrow 3 \rightarrow 4$: $\Lambda_{134} = \lambda_b . (\lambda_a + \lambda_{ccf})/[(\lambda_a + \lambda_{ccf}) + \mu_b] \approx \lambda_b . (\lambda_a + \lambda_{ccf})/\mu_b$

For the scenario $1 \rightarrow 3 \rightarrow 4$ in above formulae, λ_b is the transition rate governing the jump out of the perfect state, and $(\lambda_a + \lambda_{ccf})/\mu_b$ is the probability to jump to 4 rather to come back to 1 when in state 3.

Finally: $\Lambda_{as} = \Lambda_{12} + \Lambda_{124} + \Lambda_{134} = 1/\text{MTTF}$

This can be easily generalized to complex Markov graphs but this is valid only for completely and quickly repairable systems, i.e. DD failures.

The Markov graph on the right hand side of Figure B.31 is not completely and quickly repairable. Therefore applying above calculation would lead to wrong results.

When the E/E/PE safety-related system working in continuous mode is used in conjunction with other safety barriers, its availability shall be considered. This is what is represented on both graphs of Figure B.32 below: there is no absorbing state and the system is repaired after an overall failure. *P(t) = P1(t) + P2(t) + P3(t)* is the probability that the system is working at *t*. Then, *A(t) = P(t)* is its availability and *U(t)* = 1 - *A(t) = P4(t)* its unavailability.

This case is very different from the example represented in Figure B.31 and *R(t)* and *A(t)* should be used correctly, as should *U(T)* and *F(T)* if correct results are to be obtained.

In case of DD failures, the simplest way to handle this problem is to calculate the upper bound of *PFH* through *MDT* and *MUT* as explained in B.2.3.

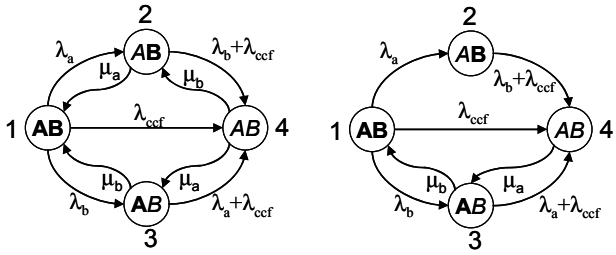


Figure B.32 – "Availability" Markov graphs without absorbing states

An interesting property of availability Markov graphs is that they reach an asymptotic equilibrium when the probability to enter a given state is equal to the probability to get out of it. Noted by:

– $P_{i,as} = \lim_{t\to\infty} P_i(t)$ the asymptotic value of $P_i(t)$

– $\lambda_i = \sum_{j\neq i} \lambda_{ij}$ the transition rate from *i* to any other state

Each time the system visits state *i*, the mean time in this state is $Mst_i = 1/\lambda_i$.

This allows calculating $MUT = \sum_i (1-q_i) P_{i,as} Mst_i$ and $MDT = \sum_i q_i P_{i,as} Mst_i$

where

q_i = 0, if *i* is a working state, and 1 otherwise.

Finally the following is obtained: $PFH = 1/(MUT + MDT) = 1/\sum_i P_{i,as} Mst_i = 1/\sum_i \frac{P_{i,as}}{\lambda_i}$

It should be noted that the number of failures observed over *[0, T]* is given by: $n = T/\sum_i \frac{P_{i,as}}{\lambda_i}$.

As most of the Markovian software packages are able to find the asymptotic probabilities there are no particular difficulties to achieve above calculations.

When the period under interest is too short for allowing the convergence of the Markov process, *PFH* may be calculated with: $w(t) = \sum_{i\neq f} \lambda_{if} P_i(t)$.

This gives: $PFH(T) = \sum_{i\neq f} \lambda_{if} \frac{\int_0^T P_i(t)dt}{T} = \frac{\sum_{i\neq f} \lambda_{if} MCT_i(T)}{T}$

There is again no difficulty to perform these calculations with a Markov software package providing the cumulated time in each of the states.

In the case of completely and quickly repairable systems (DD failures) the Vesely rate $\Lambda_v(t)$ converges very quickly toward an asymptotic value, Λ_{as}, which is a good approximation of the overall system constant failure rate of the system. Therefore in this case, the *PFH* may be calculated in the same way as in the reliability case.

In case of DU failures, this is more complicated due to the multiphase modelling. The above formula may be generalized to: $PFH(T) = \dfrac{\sum_{\varphi=1}^{n} \sum_{i \neq f} \lambda_{if} MCT_i(T_\varphi)}{\sum_{\varphi=1}^{n} T_\varphi}$

In this formula, T_φ is the duration of phase φ.

Multiphase Markovian processes generally reach equilibrium when the probability to jump out off a given state is equal to the probability to enter in it. The asymptotic values have nothing to do with those which are described above but they can be used in the above formula.

In conclusion, it can be said that the Markovian approach provides a lot of possibilities to calculate the *PFH* of an E/E/PE safety-related system working in continuous mode. Nevertheless, a good understanding of the underlying mathematics is needed to use them properly.

B.5.3 Petri nets and Monte Carlo simulation approach

B.5.3.1 Principle of modelling

An efficient way of modelling dynamic systems is to build a finite state automaton behaving as close as possible as the E/E/PE safety-related systems under study. Petri nets (see B.2.3.3 and B.6.6.10 of IEC 61508-7) have been proven to be very efficient for this purpose for the following reasons:

– they are easy to handle graphically;

– the size of the models increases linearly according to the number of components to be modelled;

– they are very flexible and allow modelling almost all type of constraints;

– they are a perfect support for Monte Carlo simulation (see B.6.6.8 of IEC 61508-7).

Originally developed in the 1960's for the formal proof on automata, they have been quickly hijacked in two steps by reliability engineers, in the seventies, for the automatic building of big Markov graphs and in the 1980's, for Monte Carlo simulation purpose.

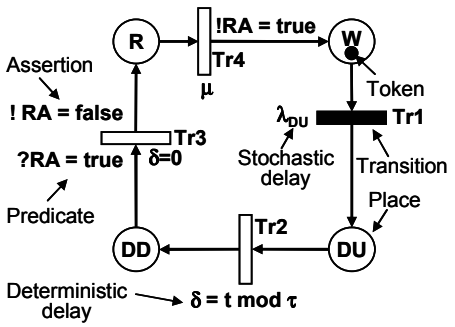


Figure B.33 – Petri net for modelling a single periodically tested component

The typical sub-Petri net for a simple periodically tested component is made of three parts:

1) the static part (i.e. a drawing):
   a) places (circles) corresponding to potential states;
   b) transitions (rectangles) corresponding to potential events;
   c) upstream arrows (from places to transitions) validating transitions;
   d) downstream arrows (from transitions to places) indicating what happens when transitions are fired.
2) the scheduling part:
   a) stochastic delays representing random delays elapsing before events occur;
   b) deterministic delays representing known delays elapsing before events occur.
3) the dynamic part:
   a) tokens (small black circles) moving when events occur to indicate which of the potential states are actually achieved;
   b) predicates (any formula which may be true or false) validating transitions;
   c) assertions (any equation) updating some variables when a transition is fired.

In addition some rules allow validating and firing a transition:

4) validation of a transition (i.e. conditions for the corresponding event may arise):
   a) all upstream places have at least one token;
   b) all predicates must be "true".
5) firing of a transition(i.e. what happens when the corresponding event is arising):
   a) one token is removed from upstream places;
   b) one token is added in downstream places;
   c) assertions are updated.

Most of the notions in relationship with Petri nets are introduced above and the remaining ones will be introduced when needed.

B.5.3.2 Monte Carlo simulation principle

Monte Carlo simulation consists of the animation of behavioural models by using random numbers to evaluate how many times the system remains in states governed either by random or deterministic delays (see also B.6.6.8 of IEC 61508-7).

This can be explained by using the Petri net presented on Figure B.33:

– At the beginning the token is in place *W* and the component is in good working order.
– Only one event may arise from this state - a dangerous undetected failure- (transition *Tr1* is valid and drawn in black).
– The time spent in this state is stochastic and governed by an exponential distribution of parameter λ_{DU}. The Monte Carlo simulation consists of firing a random number (see below) to calculate the delay *d1* before the failure is going to occur (i.e. *Tr1* is going to be fired).
– When *d1* is elapsed, *Tr1* is fired and the token moves to place *DU* (more precisely one token is removed from place *W* and one token is added in place *DU*).
– The component reaches the dangerous undetected state and the transition *Tr2* becomes valid.
– The detection of the dangerous failure occurs after a deterministic delay *d2* (*d*2 = *t modulo* τ when *t* is the current time and τ the test interval). This simulates the test interval.

– When *t*2 is elapsed, i.e. the dangerous failure is detected, the token enters in place *DD.* The component is now waiting to be repaired and *Tr*3 becomes valid.

– The delay *d*3 for firing *Tr*3 (start of repair) does not depend on the component itself but on the availability of the repair resources represented by the message *RA*. This is governed by events arising in another part of the whole Petri net not represented on Figure B.33.

– The repair starts as soon as the repair team becomes available (i.e. the predicate *?RA = true* becomes true) and the token enters in place *R*. Repair resources become immediately unavailable for another intervention and the assertion *!RA = false* is used to update the value of *RA*. This prevents any other repair at the same time.

– The stochastic transition *Tr*4 (i.e. the end of the repair) becomes valid and the delay *d4* may be calculated by firing a random number according to the repair rate μ.

– When *d*4 is elapsed, *Tr*4 is fired and the component is coming back in its good working state (the token enters in place *W*). The repair resources are again available and *RA* is updated through the assertion *!RA = true*.

– And so on... as long as the firing of next valid transition belongs to the period under interest *[0, T]*.

When the next firing is no longer inside *[0, T]*, the simulation is stopped and one history of the component is achieved. All along the progress of the history, relevant parameters may be recorded as the mean marking of the places (i.e. the ratio of the time with one token in the place over the duration T), the transition firing frequencies, the time to the first occurrence of a given event, etc.

The principle of Monte Carlo simulation is to realize a great number of such histories and to perform classical statistics on the results in order to assess the relevant parameters.

Contrary to analytical calculations, Monte Carlo simulation allows to mix easily deterministic and random delays which may be simulated from their cumulated probability distribution *F(d)* and random numbers z_i uniformly distributed over *[0, 1]*. Those random numbers are available in almost any programming languages and powerful algorithms are available to do that.

Then, a sample (d_i), distributed according to *F(d),* is obtained from a sample (z_i) by the operation: $d_i = F^{-1}(z_i)$. This is very easy when the analytical form of $F^{-1}(z)$ is available as, for example, exponentially distributed delays: $d_i = -\frac{1}{\lambda_{DU}} Log(z_i)$.

In respect of the accuracy of the calculations, concerning a given simulated parameter *X*, the basic statistics allow the calculation of the average, variance, standard deviation and confidence of the sample (X_i) which has been simulated:

– average : $\overline{X} = \frac{\sum_i x_i}{N}$

– variance: $\sigma^2 = \frac{\sum_i (x_i - \overline{X})^2}{N}$ and standard deviation : σ

– 90 % confidence interval around $\overline{X}$: $Conf = 1{,}64 \frac{\sigma}{\sqrt{N}}$

Therefore, when using Monte Carlo simulation, the accuracy of the results can always be estimated. For example, considering 90 % of chance that the true result $\hat{X}$ belongs to the interval $\left[\overline{X} - 1{,}64\sigma / \sqrt{N},\quad \overline{X} + 1{,}64\sigma / \sqrt{N}\right]$.

This interval is reducing when the number of histories increases and when the frequency of occurrence of *X* increases.

With present time personal computers, there are no real difficulties to achieve calculations even for SIL 4 E/E/PE safety-related systems.

B.5.3.3 Principle of *PFD* calculations

The sub-Petri-net on Figure B.33 may be used directly to evaluate the PFD_{avg} of the component because the mean marking of place *W* which is equal to the ratio of the time spent in *W* (i.e. with *W* marked by the token) to the duration *T*, is in fact the average availability *A* of the component. We have $PFD_{avg} = 1 - A$.

The accuracy of the calculation may be estimated as explained above.

More complex behaviours may be represented by using specific sub-Petri Nets. Figure B.34 gives an idea of what can be done for modelling periodically tested components, common cause failures (CCF) and repair resources.

On the left hand side is modelled a periodically tested component which jumps across the states working (*W*), dangerously failed undetected (*DU*), under testing (DUT), dangerously failed detected (*DD*), ready for repair (*RR*) and under repair (*R*).

When it fails (*DU*), the message *!-Ci* (equivalent to *!Ci = false*) is emitted to inform that the component is failed. Then it waits until a periodical test is started (DUT). The periodic test interval is τ and the staggering θ. After what the test is performed for a duration equal to π and the state *DD* is reached. If a spare part is available (at least one token in *SP*), the component becomes ready for repair (*RR*) and the variable *NbR* is increased by 1 to inform the repair resources of the number of components needing to be repaired. When the repair resources are on location (one token in *OL*) the repair starts (*R*) and the token is removed from *OL*. When it is achieved the component comes back in good functioning state, the message *!Ci* is emitted (i.e. !*Ci* = *true*), *NbR* is decreased by 1 and the token is given back in *OL* to allow further repairs. And so on.

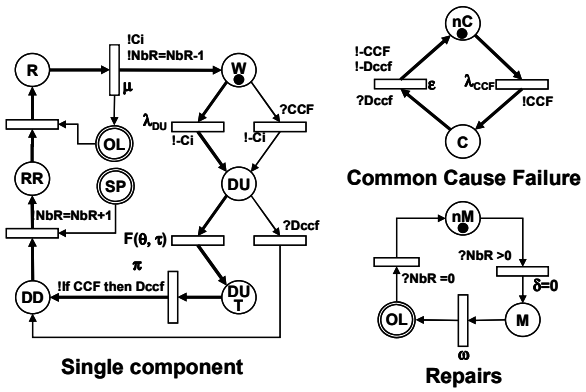


Figure B.34 – Petri net to model common cause failure and repair resources

The variable *NbR* is used by the sub-Petri net devoted to repairs. When it becomes positive, the mobilisation of the resources is started (*M*) and after a certain delay they are ready to work on location (*OL*). The token in *OL* is used to validate the starting of the repair of one failed component. Therefore, only one repair may be done at the same time. When all repairs have been performed (i.e. *NbR* = 0) the repair resources are demobilized.

On Figure B.34 a common cause failure (CCF) has also been modelled. When it occurs (λ_{DCC}), the message *!CCF* becomes true and is used to put all the affected components in their *DU* states. The relevant messages C_i become false and the components are repaired

independently from each other. When the test of a component is finished, the assertion *!IF CCF then Dccf* allows to inform all the other components that a CCF has been detected. This message is used to put them immediately in their *DD* states. This message is also used to reset the CCF sub-Petri net but this is done after a while (ε) to insure that all components have been put in their *DD* state before resetting.

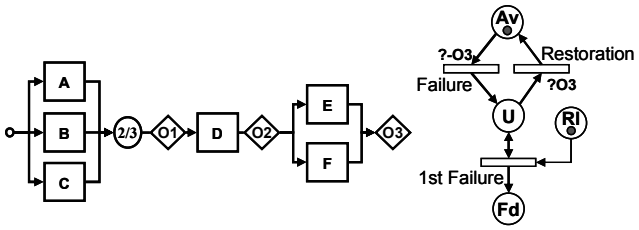


Figure B.35 – Using reliability block diagrams to build Petri net and auxiliary Petri net for *PFD* and *PFH* calculations

The sub-Petri Nets on Figure B.34 are intended to be used as parts of more complex models. One way to use them is illustrated on Figure B.35 where the reliability block diagram of Figure B.16 which has been slightly adapted by introducing the intermediary outputs *Oi*.

The components A, B, C, D, E, F may be modelled by a set of sub- Petri nets like those on Figure B.34 with for example a CCF for (A, B, C) and another one for (E, F) and the same repair resources for all components. The remaining problem is only to link the component together according to the logic of the reliability block diagram and to calculate the PFD_{avg} under interest.

Linking the components is very easy by using the messages C_i and building the following assertions:

– $O_1 = C_a.C_b + C_a.C_c + C_b.C_c$
– $O_2 = O_1.C_d$
– $O_3 = O_2.(C_e + C_f)$

Therefore when O_3 is true, the whole E/E/PE safety-related system is working well and it is unavailable otherwise. This message is used in the sub-Petri net on the right hand side in order to model the various states of the E/E/PE safety-related systems: available (*Av*), unavailable (*U*), reliable(*Rl*) and unreliable (*Fd*).

For *PFD* calculation the focus is only on *Av* and *U*: when O_3 becomes false, the system fails and becomes unavailable and when O_3 becomes true, the system is restored and becomes available again. This is very simple and the mean marking of *Av* is the average availability of the system and the mean marking of *U* its average unavailability, i.e. its PFD_{avg}.

Therefore, the Monte Carlo simulation performs automatically the integral of the instantaneous unavailability and it is not necessary to calculate it except if the saw tooth curve is wanted. This would be easily done by evaluating the mean marking of *U* at given instant rather over the whole *[0, T]* period.

What is exposed above only intends to illustrate the broad lines of using Petri nets for SIL calculations purposes but the potential modelling possibilities are virtually endless.

B.5.3.4 Principle of *PFH* calculations

For the *PFH* calculation, the principles remain exactly the same as above and the same sub models can be used for DU failures. Figure B.36 illustrates a sub-Petri net modelling a DD failure which is revealed and repaired as soon as it has been detected.

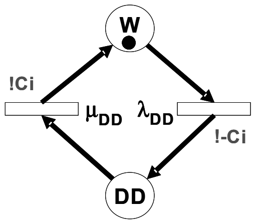


Figure B.36 – Simple Petri net for a single component with revealed failures and repairs

Such components' models may be used as explained above in relationship with a reliability block diagram representing the whole system like on Figure B.35.

When the E/E/PE safety-related system working in continuous mode is the ultimate safety barrier, an accident occurs as soon as it is failing and the *PFH* evaluation must be achieved through the reliability of the system. This is done by the lower part of the sub PN presented on the right hand side of Figure B.35: the average frequency of the first failure of the system over *[0, T]* is its unreliability *F(T)*. Then, when *F(T)* is small compared to 1, and according to the *PFH* definition, we have *PFH* = *F(T)/T*.

Due to the token in *Rl*, the first failure is a one shot transition. Provided that all histories lead to a failure (i.e. T is long enough) the mean time spent with a token in *Rl* is the *MTTF* of the system. Then *PFH* ≈ 1/*MTTF* provides an upper bound of *PFH*.

When the E/E/PE safety-related system working in continuous mode is not the ultimate safety barrier it does not provoke directly an accident when it fails. Then it is repaired after an overall failure and its *PFH* shall be calculated through the unavailability of the system. It is obtained directly from the frequency *Nbf* of the transition failure. This provides the number of times the system has failed over a given period and therefore we have *PFH(T) = Nbf/T*.

It is interesting to note that when *T* is long enough, the *MUT* may be calculated through the mean cumulated time MCT_{Av} in state *Av* and the *MDT* through the mean cumulated time MCT_{U} in state *U*. The mean cumulated times MCT_{A} and MCT_{U} are very easy to calculate within the Monte Carlo simulation just by cumulating the times when a token is present in *Av* or *U*. We have $MUT = MCT_A / Nbf$ and $MUT = MCT_u / Nbf$. This may be used for evaluating *PFH* = 1/*(MUT* + *MDT)* = 1/*MTBF* = *Nbf/T.*

All these results are obtained directly because the Monte Carlo simulation provides naturally the average values. What is exposed above only intends to illustrate the broad lines of using Petri nets for SIL calculations purposes but the potential modelling possibilities are virtually endless.

B.5.4 Other approaches

The relationship between the size of the models and the number of components of the system under study varies dramatically according to the type of approach in use. It is linear for fault trees and Petri nets but exponential for Markov processes. Therefore fault tree and Petri net approaches make it potentially easier to handle much larger systems than Markovian approach. This is why Petri nets are sometimes used to produce large Markov graphs.

The underlying formal languages behind the graphical representations described here above produce flat models: each component is described separately, at the same level. This makes large models sometimes hard to master and to maintain. A way to overcome this problem is to use structured languages providing compact hierarchical models. Several such formal languages have been developed recently and some software packages are available. As an example, we can consider, the AltaRica Data Flow language published in 2 000 in order to be freely used by the reliability community and designed to accurately model the functional and dysfunctional properties of industrial systems (see references in B.7).

Figure B.37 is equivalent to the reliability block diagram presented Figure B.1. This model is hierarchical because single modules are modelled only once and then reused as many times as needed at the system level (i.e. in the node main). This allows achieving very compact models.

In order to simplify the presentation, only two transitions have been represented for the components: failure and repair (i.e. DD failures revealed and repaired as soon as they arise).

Logical operators (*or*, *and*) are used to describe the logic of the system. This is done in direct relationship with the reliability block diagram and the flow Out models the state of the system: it is working when *Out* is *true* and failed when *Out* is *false*.

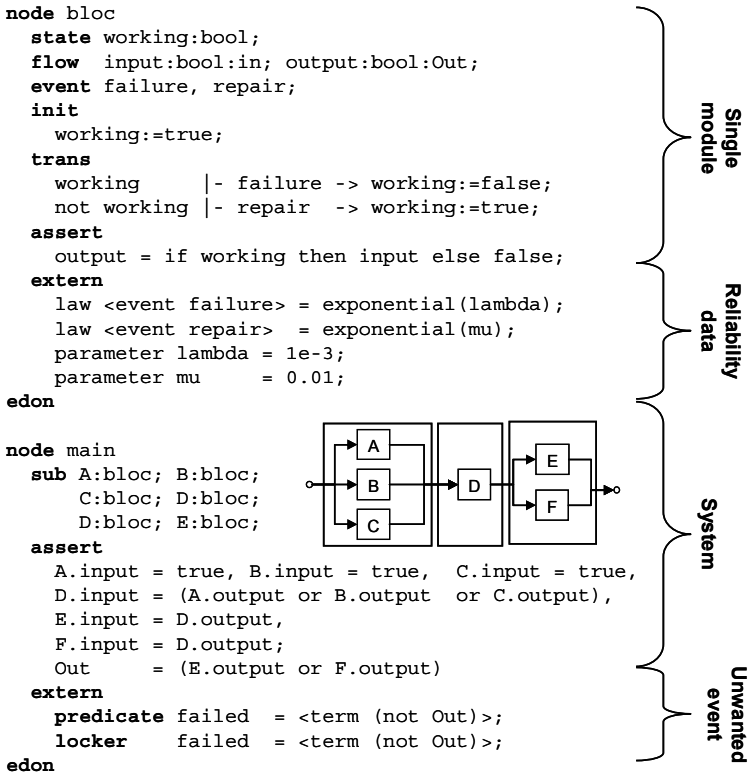


Figure B.37 – Example of functional and dysfunctional modelling with a formal language

This provides good behavioural models for efficient Monte Carlo simulation and all what has been described above for Petri net remains valid here for PFD_{avg} or *PFH* calculations. Therefore we are not developing this part further.

This formal language possesses similar mathematical properties as Petri nets and therefore it is possible to compile one model towards the other without difficulty. But it also generalizes the properties of the underlying languages behind Fault trees or Markov processes. Therefore, providing that the description has been restricted to the properties of Markov processes or Fault trees, it is possible to compile the model into equivalent Markov graph or fault trees. It is the purpose of the key words “predicate” and “locker” at the end of the model to provide directives for fault trees or Markov model generation or for direct Monte Carlo simulation.

Using a formal language designed to model properly the system behaviour both from functional and dysfunctional points of view allows:

– Monte Carlo simulations to be performed directly on the models;

– Markov graphs to be generated and analytical calculations to be performed as previously shown (when the language has been restricted to Markov properties);

– Equivalent Fault trees to be generated and analytical calculations to be performed as previously shown (when the language has been restricted to Boolean properties).

Such functional and dysfunctional formal languages are general purpose languages. There are no difficulties to use them in the particular case of E/E/PE safety-related systems. They provide an efficient way to master PFD_{avg} and *PFH* calculations of E/E/PE safety-related systems when several protection layers, various types of failure modes, complex proof test patterns, components dependencies, maintenance resources, etc., i.e. when the other methods have shown that they have reached their limits.

B.6 Handling uncertainties

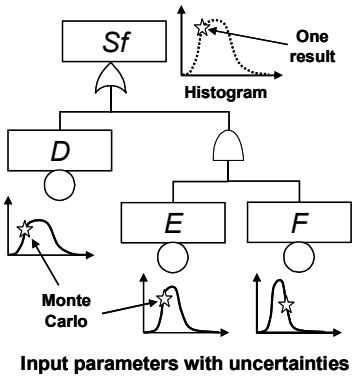


Figure B.38 – Uncertainty propagation principle

One of the main problems encountered when performing probabilistic calculations is linked to the uncertainties on the reliability parameters. Therefore, it is useful when performing *PFD* or *PFH* calculations to evaluate what the corresponding impact is on the uncertainty of the results.

Care needs to be taken when dealing with this issue and using Monte Carlo simulation provides an efficient way for this purpose as it is illustrated on Figure B.38.

On this figure the input reliability parameters (e.g. the dangerous undetected failure rates) are no longer certain and they are replaced by random variables. The density of probability of such random variable is more or less sharp or flat according to the degree of uncertainty: the probability density of F is sharper than the one of E or D. This means that there is less uncertainty on F than on E or D for example.

The principle of calculation is the following:

1) generating one set of input parameters by using random numbers according to the probabilistic distributions of those parameters (similar to what has been explained in B.3.2) ;
2) performing one calculation by using the above generated set of input parameters;
3) recording the output result (this constitutes one value used in step 4);
4) performing steps 1 to 3 again and again until a sufficient number of values (for example 100 or 1 000) is obtained in order to constitute an histogram (dotted line on Figure B.38);
5) analysing statistically the histogram to obtain the average and the standard deviation of the output result.

The average of this histogram is the PFD_{avg} or the *PFH* according to the type of calculation performed and the standard deviation measures the uncertainty on this results. The smaller the standard deviation, the more accurate is the PFD_{avg} or the *PFH* calculation.

The principle illustrated here on fault tree is very general and may be applied on any of the calculation methods depicted in this annex: simplified formulae, Markov processes and even Petri nets or formal languages approaches. When the calculation is already performed by Monte Carlo simulation, a two step Monte Carlo simulation shall be used.

The probabilistic distribution for a given input reliability parameter shall be chosen according to the knowledge gathered about it. This may be:

– a uniform distribution between lower and upper bounds;

– a triangular distribution with a most probable value;

– a log-normal law with a given error factor;

– a Chi square law, etc.

The first ones may be assessed by engineering judgement when there is not very much field feedback available. When there is more field feedback available, the last ones may be used because the field feedback provides average parameter values as well as confidence intervals on these average values.

For example if n failures have been observed over a cumulated observation time T, we have:

– $\hat{\lambda} = n/T$ is the maximum likelihood estimator of the failure rate

– $\lambda_{Inf,\alpha} = \frac{1}{2T}\chi^2_{(1-\alpha),2n}$ lower bound with a probability α % to be lower than $\lambda_{\text{Inf},\alpha}$

– $\lambda_{Sup,\alpha} = \frac{1}{2T}\chi^2_{\alpha,2(n+1)}$ upper bound with a probability α % to be higher than $\lambda_{\text{Sup},\alpha}$

When α = 5 %, then the true value of λ has 90 chances over 100 to belong to the interval $[\lambda_{\text{Inf},\alpha}, \lambda_{\text{Sup},\alpha}]$. The smaller this interval, the more accurate the value of λ. Normally, good reliability data bases provide this information. Analysts should consider reliability data provided without confidence intervals (or information allowing to calculate them) very cautiously.

$\hat{\lambda}$, $\lambda_{\text{Inf},\alpha}$ and $\lambda_{\text{Sup},\alpha}$ can be used to build a relevant distribution to model the failure rate λ of a given failure mode and its uncertainties. This is clear for χ^2 distribution but the log-normal law has also shown this to be very efficient for that purpose. Such a log-normal law is defined by its average $\hat{\lambda}$ or its median $\lambda_{50\ \%}$ and its so-called error factor.

This law has a very interesting property: $\lambda_{\text{Inf},\alpha} = \lambda_{50\ \%}/ef_\alpha$ and $\lambda_{\text{Sup},\alpha} = \lambda_{50\ \%}.ef_\alpha$.

Then it is defined with only two parameters: $\hat{\lambda}$ *and* $ef_\alpha \approx \sqrt{\frac{\lambda_{Sup,\alpha}}{\lambda_{Inf,\alpha}}}$

When ef_α = 1 there is no uncertainties, when ef_α = 3,3 there is a factor of about 10 between the lower and upper confidence bounds, etc.

These laws may be used in turn with Monte Carlo simulations in order to take under consideration both the impacts of average values and uncertainties on PFD_{avg} or *PFH*. Therefore it is always possible to master the uncertainties within probabilistic calculations. Some software packages implement directly such calculations.

When analysing redundant systems the analysis should not only consider the uncertainty of the basic element failure rate but also the accuracy of the CCF failure rate. Even if there is good field feed back data for each of the elements there is rarely good CCF field data and hence this will be the most uncertain.

B.7 References

References [4] to [9] and [22] to [24] in the Bibliography give further details on evaluating probabilities of failure.

Annex C
(informative)

Calculation of diagnostic coverage and safe failure fraction – worked example

A method for calculating diagnostic coverage and safe failure fraction is given in Annex C of IEC 61508-2. This annex briefly describes the use of this method to calculate the diagnostic coverage. It is assumed that all of the information specified in IEC 61508-2 is available and has been used where required in obtaining the values shown in Table C.1. Table C.2 gives limitations on diagnostic coverage that can be claimed for certain E/E/PE safety-related elements. The values in Table C.2 are based on engineering judgement.

To understand all the values in Table C.1, a detailed hardware schematic would be required, from which the effect of all failure modes could be determined. These values are only examples, for instance some components in Table C.1 assume no diagnostic coverage because it is practically impossible to detect all failure modes of all components.

Table C.1 has been derived as follows:

a) A failure mode and effect analysis has been carried out to determine the effect of each failure mode for every component on the behaviour of the system without diagnostic tests. The fractions of the overall failure rate associated with each failure mode are shown for each component, divided between safe (S) and dangerous (D) failures. The division between safe and dangerous failures may be deterministic for simple components but is otherwise based on engineering judgement. For complex components, where a detailed analysis of each failure mode is not possible, a division of failures into 50 % safe, 50 % dangerous is generally accepted. For this table, the failure modes given in reference a) have been used, although other divisions between failure modes are possible and may be preferable.

b) The diagnostic coverage for each specific diagnostic test on each component is given (in the column labelled "DC_{comp}"). Specific diagnostic coverages are given for the detection of both safe and dangerous failures. Although open-circuit or short-circuit failures for simple components (for example resistors, capacitors and transistors) are shown to be detected with a specific diagnostic coverage of 100 %, the use of table C.2 has limited the diagnostic coverage with respect to item U16, a complex type B component, to 90 %.

c) Columns (1) and (2) give the safe and dangerous failure rates, in the absence of diagnostic tests, for each component (λ_S and $\lambda_{DD} + \lambda_{Du}$ respectively).

d) We can consider a detected dangerous failure to be effectively a safe failure, so we now find the division between effectively safe failures (i.e. either detected safe, undetected safe or detected dangerous failures) and undetected dangerous failures. The effective safe failure rate is found by multiplying the dangerous failure rate by the specific diagnostic coverage for dangerous failures and adding the result to the safe failure rate (see column (3)). Likewise, the undetected dangerous failure rate is found by subtracting the specific diagnostic coverage for dangerous failures from one and multiplying the result by the dangerous failure rate (see column (4)).

e) Column (5) gives the detected safe failure rate and column (6) gives the detected dangerous failure rate, found by multiplying the specific diagnostic coverage by the safe and dangerous failure rates respectively.

f) The table yields the following results:

   – total safe failure rate $\sum \lambda_S + \sum \lambda_{Dd} = 9{,}9 \times 10^{-7}$
     (including detected dangerous failures)

   – total undetected dangerous failure rate $\sum \lambda_{Du} = 5{,}1 \times 10^{-8}$

- total failure rate $\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du} = 1{,}0 \times 10^{-6}$
- total undetected safe failure rate $\sum \lambda_{Su} = 2{,}7 \times 10^{-8}$
- diagnostic coverage for safe failures $\frac{\sum \lambda_{Sd}}{\sum \lambda_S} = \frac{3{,}38}{3{,}65} = 93\ \%$
- diagnostic coverage for dangerous failures
  $\frac{\sum \lambda_{Dd}}{\sum \lambda_{Dd} + \sum \lambda_{Du}} = \frac{6{,}21}{6{,}72} = 92\ \%$ (normally termed simply “diagnostic coverage”)
- safe failure fraction $\frac{\sum \lambda_S + \sum \lambda_{Dd}}{\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}} = \frac{986}{365 + 672} = 95\ \%$

g) The division of the failure rate without diagnostic tests is 35 % safe failures and 65 % dangerous failures.

Table C.1 – Example calculations for diagnostic coverage and safe failure fraction

Item	No	Type	Division of safe and dangerous failures for each failure mode								Division of safe and dangerous failures for diagnostic coverage and calculated failure rates ($\times 10^{-9}$)						
			OC		SC		Drift		Function		DC_{comp}		(1)	(2)	(3)	(4)	(5)	(6)
			S	D	S	D	S	D	S	D	S	D	λ_S	$\lambda_{DD}+\lambda_{Du}$	$\lambda_S+\lambda_{DD}$	λ_{DU}	λ_{SD}	λ_{DD}
Print	1	Print	0,5	0,5	0,5	0,5	0	0	0	0	0,99	0,99	11,0	11,0	21,9	0,1	10,9	10,9
CN1	1	Con96pin	0,5	0,5	0,5	0,5					0,99	0,99	11,5	11,5	22,9	0,1	11,4	11,4
C1	1	100nF	1	0	1	0	0	0	0	0	1	0	3,2	0,0	3,2	0,0	3,2	0,0
C2	1	10µF	0	0	1	0	0	0	0	0	1	0	0,8	0,0	0,8	0,0	0,8	0,0
R4	1	1M	0,5	0,5	0,5	0,5					1	1	1,7	1,7	3,3	0,0	1,7	1,7
R6	1	100k									0	0	0,0	0,0	0,0	0,0	0,0	0,0
OSC1	1	OSC24 MHz	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	1	16,0	16,0	32,0	0,0	16,0	16,0
U8	1	74HCT85	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U16	1	MC68000-12	0	1	0	1	0,5	0,5	0,5	0,5	0,90	0,90	260,4	483,6	695,6	48,4	234,4	435,2
U26	1	74HCT74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U27	1	74F74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	14,4	14,4	28,7	0,1	14,3	14,3
U28	1	PAL16L8A	0	1	0	1	0	1	0	1	0,98	0,98	0,0	88,0	86,2	1,8	0,0	86,2
T1	1	BC817	0	0	0	0,67	0	0,5	0	0	1	1	0,0	0,2	0,4	0,0	0,0	0,2
Total													365	672	986	50,9	338	621

NOTE None of the failure modes of item R6 are detected, but a failure does not affect either safety or availability.

Key

S	Safe failure
D	Dangerous failure
OC	Open circuit
SC	Short circuit
Drift	Change of value
Function	Functional failures
DC_{comp}	Specific diagnostic coverage for the component

See also Table B.1, although in this table failure rates are for the individual components in question rather than every component in a channel.

Table C.2 – Diagnostic coverage and effectiveness for different elements

Component	Low diagnostic coverage	Medium diagnostic coverage	High diagnostic coverage
CPU (see Note 3)	total less than 70 %	total less than 90 %	
register, internal RAM	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
coding and execution including flag register	50 % - 60 %	75 % - 95 %	-
(see Note 3)	50 % - 70 %	85 % - 98 %	-
address calculation (see Note 3)	50 % - 60 %	60 % - 90 %	85 % - 98 %
program counter, stack pointer	50 % - 70 %		
	40 % - 60 %		
Bus			
memory management unit	50 %	70 %	90 % - 99 %
bus-arbitration	50 %	70 %	90 % - 99 %
Interrupt handling	40 % - 60 %	60 % - 90 %	85 % - 98 %
Clock (quartz) (see Note 4)	50 %	-	95 % - 99 %
Program flow monitoring			
temporal (see Note 3)	40 % - 60 %	60 % - 80 %	-
logical (see Note 3)	40 % - 60 %	60 % - 90 %	-
temporal and logical (see Note 5)	-	65 % - 90 %	90 % - 98 %
Invariable memory	50 % - 70 %	99 %	99,99 %
Variable memory	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
Discrete hardware			
digital I/O	70 %	90 %	99 %
analogue I/O	50 % - 60 %	70 % - 85 %	99 %
power supply	50 % - 60 %	70 % - 85 %	99 %
Communication and mass storage	90 %	99,9 %	99,99 %
Electromechanical devices	90 %	99 %	99,9 %
Sensors	50 % - 70 %	70 % - 85 %	99 %
Final elements	50 % - 70 %	70 % - 85 %	99 %

NOTE 1 This table should be read in conjunction with Table A.1 of IEC 61508-2 which provides the failure modes to be considered.

NOTE 2 When a range is given for diagnostic coverage, the upper interval boundaries may be set only for narrowly tolerated monitoring means, or for test measures that stress the function to be tested in a highly dynamic manner.

NOTE 3 For techniques where there is no high diagnostic coverage figure, at present no measures and techniques of high effectiveness are known.

NOTE 4 At present no measures and techniques of medium effectiveness are known for quartz clocks.

NOTE 5 The minimum diagnostic coverage for a combination of temporal and logical program flow monitoring is medium.

See references [10] to [12] in the Bibliography.

Annex D
(informative)

A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems

D.1 General

D.1.1 Introduction

This standard incorporates a number of measures which deal with systematic failures. However, no matter how well these measures are applied, there is a residual probability of systematic failures occurring. Although this does not significantly affect the reliability calculations for single-channel systems, the potential for failures which may affect more than one channel in a multi-channel system (or several components in a redundant safety system), i.e. common cause failures, results in substantial errors when reliability calculations are applied to multi-channel or redundant systems.

This informative annex describes two methodologies which allow common cause failures to be taken into account in the safety assessment of multi-channel or redundant E/E/PE systems. Using these methodologies gives a more accurate estimation of the integrity of such a system than ignoring the potential for common cause failures.

The first methodology is used to calculate a value for β, factor frequently used in the modelling of common cause failures. This can be used to estimate the rate of common cause failures applicable to two or more systems operating in parallel from the random hardware failure rate of one of those systems (see D.5). It is generally accepted that the random hardware failure figures that are collected will include a number of failures that were caused by systematic failures.

Alternative methodologies may be preferred in some cases, for example, where a more accurate β-factor can be proven as a result of the availability of data on common cause failures or when the number of impacted elements is higher than four. The second methodology, i.e. the binomial failure rate (also called shock model) method, can be used

D.1.2 Brief overview

The failures of a system are considered to arise from two dissimilar sources:

– random hardware failures; and

– systematic failures.

The former are assumed to occur randomly in time for any component and to result in a failure of a channel within a system of which the component forms part when the latter appears immediately and in a deterministic way when the system reach the situation for which the underlying systematic error is existing.

There is a finite probability that independent random hardware failures could occur in all channels of a multi-channel system so that all of the channels were simultaneously in a failed state. Because random hardware failures are assumed to occur randomly with time, the probability of such failures concurrently affecting parallel channels is low compared to the probability of a single channel failing. This probability can be calculated using well-established techniques but the result may be very optimistic when the failures are not fully independent from each other.

Dependent failures are traditionally split between (see reference [18] in the Bibliography):

– Common Cause Failure (CCF) causing multiple failures from a single shared cause. The multiple failures may occur simultaneous or over a period of time;

– Common Mode Failures (CMF) which are a particular case of CCF in which multiple equipment items fail in the same mode;

– Cascade failures which are propagating failures.

The term CCF is often used to cover all kind of dependant failures as it is done in this annex. They are also split between

– Dependent failures due to clear deterministic causes;

– Residual potential multiple failure events not explicitly considered in the analysis because of not enough accuracy, no clear deterministic causes or impossibility to gather reliability data.

The first one should be analysed, modelled and quantified in a conventional way and only the second ones should be handled as shown in this informative Annex D. Nevertheless, the systematic failures -which are perfect dependent failures not identified during the safety analysis (otherwise they would have been removed)- are handled in particular manner in this standard and this annex applies mainly for hardware random dependent failures.

Therefore, common cause failures which result from a single cause, may affect more than one channel or more than one component. These may result from a systematic fault (for example, a design or specification mistake) or an external stress leading to an early random hardware failure (for example, an excessive temperature resulting from the random hardware failure of a common cooling fan, which accelerates the life of the components or takes them outside their specified operating environment) or, possibly, a combination of both. Because common cause failures are likely to affect more than one channel in a multi-channel system, the probability of common cause failure is likely to be the dominant factor in determining the overall probability of failure of a multi-channel system and if this is not taken into account a realistic estimate of the safety integrity level of the combined system is unlikely to be obtained.

D.1.3 Defence against common cause failures

Although common cause failures result from a single cause, they do not all manifest themselves necessarily simultaneously in all channels. For example, if a cooling fan fails, all of the channels of a multi-channel E/E/PE system could fail, leading to a common cause failure. However, all of the channels are unlikely to warm at the same rate or to have the same critical temperature. Therefore, failures occur at different times in the different channels.

The architecture of programmable systems allows them to carry out internal diagnostic testing functions during their on-line operation. These can be employed in a number of ways, for example

– a single channel PE system can continuously be checking its internal operation together with the functionality of the input and output devices. If designed from the outset, a test coverage in the region of 99 % is achievable (see [13] in the Bibliography). If 99 % of internal faults are revealed before they can result in a failure, the probability of single-channel faults which can ultimately contribute to common cause failures is significantly reduced.

– in addition to internal testing, each channel in a PE system can monitor the outputs of other channels in a multi-channel PE system (or each PE device can monitor another PE device in a multi-PE system). Therefore, if a failure occurs in one channel, this can be detected and a safe shut-down initiated by the one or more remaining channels that have not failed and are executing the cross-monitoring test. (It should be noted that cross-monitoring is effective only when the state of the control system is continuously changing, for example the interlock of a frequently used guard in a cyclic machine, or when brief changes can be introduced without affecting the controlled function.) This cross-

monitoring can be carried out at a high rate, so that, just before a non-simultaneous common cause failure, a cross-monitoring test is likely to detect the failure of the first channel to fail and is able to put the system into a safe state before a second channel is affected.

In the case of the cooling fan example, the rate of temperature rise and the susceptibility of each channel are slightly different, resulting in the second channel failing possibly several tens of minutes after the first. This allows the diagnostic testing to initiate a safe shutdown before the second channel succumbs to the common cause fault.

As a result of the above

– PE-based systems have the potential to incorporate defences against common cause failures and, therefore, be less susceptible to them when compared to other technologies;

– a different β-factor may be applicable to PE-based systems when compared to other technologies. Therefore, β-factor estimates based on historic data are likely to be invalid. (None of the existing investigated models used for estimating the probability of common cause failure allow for the effect of automatic cross-monitoring.)

– because common cause failures that are distributed in time may be revealed by the diagnostic tests before they affect all channels, such failures may not be recognized or reported as being common cause failures.

There are three avenues that can be taken to reduce the probability of potentially dangerous common cause failures.

a) Reduce the number of random hardware and systematic failures overall. (This reduces the areas of the ellipses in Figure D.1 leading to a reduction in the area of overlap.)

b) Maximize the independence of the channels (separation and diversity). (This reduces the amount of overlap between the ellipses in Figure D.1 whilst maintaining their area.)

c) Reveal non-simultaneous common cause failures while only one, and before a second, channel has been affected, i.e. use diagnostic tests or proof test staggering.

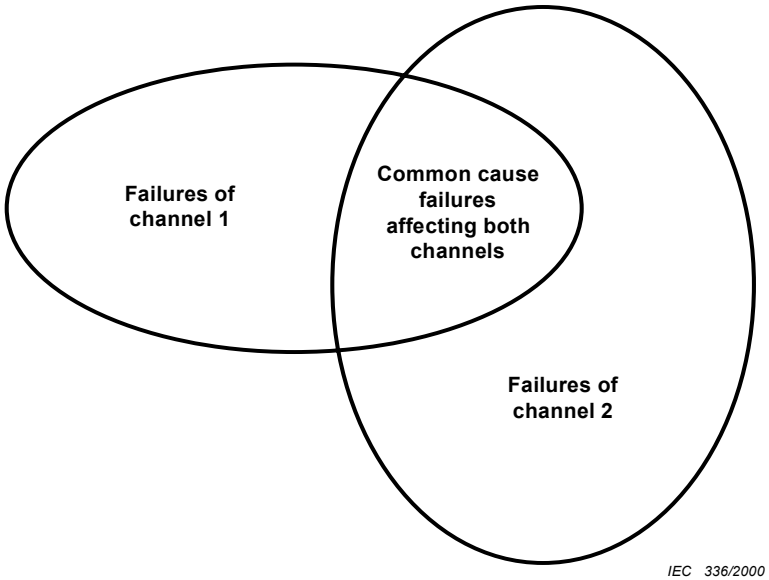


Figure D.1 – Relationship of common cause failures to the failures of individual channels

With systems with more than two channels, the common cause failure may affect all channels or only multiple channels but not all depending on the source of the common mode. Thus the approach taken in this annex, according to the first method, is to calculate the β value based on a duplex system voting 1oo2 and then use a multiplying factor to the derived β depending on the total number of channels and the voting requirements. (see Table D.5).

D.1.4 Approach adopted in the IEC 61508 series

The IEC 61508 series is based on these three avenues and requires a threefold approach:

a) Apply the techniques specified in IEC 61508-2/3 to reduce the overall probability of systematic failure to a level commensurate with the probability of random hardware failure.

b) Quantify those factors that can be quantified, i.e. take into account the probability of random hardware failure, as specified in IEC 61508-2.

c) Derive, by what is considered at the present time to be the best practicable means, a factor relating the probability of common cause failure of the hardware to the probability of random hardware failure. The methodology described in this annex relates to the derivation of this factor.

Most methodologies for estimating the probability of common cause failures attempt to make their predictions from the probability of random hardware failure. Clearly, the justification for any direct relationship between these probabilities is tenuous, nevertheless, such a correlation has been found in practice and probably results from second-order effects. For example, the higher the probability of random hardware failure of a system

– the higher the amount of maintenance required by the system. The probability of a systematic fault being introduced during maintenance depends on the number of times maintenance is carried out, and this also affects the rate of human errors leading to common cause failures. This leads to a relationship between the probability of random hardware failure and the probability of common cause failure. For example:
  - a repair, followed by testing and, possibly, recalibration is required each time a random hardware failure occurs;
  - for a given safety integrity level, a system with a higher probability of random hardware failure requires proof tests to be carried out more frequently and with greater depth/complexity, leading to additional human interference.
– the more complex the system. The probability of random hardware failure depends on the number of components, and, hence, the complexity of a system. A complex system is less easily understood, so is more prone to the introduction of systematic faults. In addition, the complexity makes it difficult to detect the faults, by either analysis or test, and can lead to parts of the logic of a system not being exercised except in infrequent circumstances. Again, this leads to a relationship between the probability of random hardware failure and the probability of common cause failure.

Several approaches are currently in use to handle CCF (β factor, multiple Greek letters, α factor, binomial failure rate ...) [20]. Two of the current models are proposed in this informative annex for the third part of the threefold approach already described. Despite the limitations, it is believed that they represent the best way forward at the present time to handle the probability of common cause failure:

– the well-established β-factor model which is widely used and realistic to deal with multi-channel system typically up to four dependent elements.
– the binomial failure rate [21] (also known as the shock model) which can be used when the number of dependent elements is greater than four.

The following two difficulties are faced when using the β-factor or the shock models on a E/E/PE system.

– What value should be chosen for the parameters? Many sources (for example reference [13]) suggest ranges within which the value of the β-factor is likely to occur but no actual value is given, leaving the user to make a subjective choice. To overcome this problem, the β-factor methodology in this annex is based on the system originally described in reference [14] and recently redefined in reference [15].

– Neither the β-factor nor the shock models take into account the sophisticated diagnostic testing capabilities of modern PE systems, which can be used to detect a non-simultaneous common cause failure before it has had sufficient time to manifest itself fully. To overcome this deficiency, the approach described in references [14] and [15] has been modified to reflect the effect of diagnostic tests in the estimation of the likely value of β.

The diagnostic testing functions running within a PE system are continuously comparing the operation of the PE system with predefined states. These states can be predefined in software or in hardware (for example, by a watchdog timer). Looked on in this way, the diagnostic testing functions may be thought of as an additional, and partially diverse, channel running in parallel with the PE system.

Cross-monitoring between channels also can be carried out. For many years, this technique has been used in dual-channel interlocking systems based solely on relays. However, with relay technology, it is usually possible to carry out the cross-checks only when the channels change state, making such tests inappropriate for revealing non-simultaneous common cause failures where systems remain in the same (for example, ON) state for long periods. With PE system technology, cross-monitoring may be carried out with a high repetition frequency.

D.2 Scope of the methodology

The scope of the methodology is limited to common cause failures within hardware. The reasons for this include the following:

– the β-factor and shock models relate the probability of common cause failure to the probability of random hardware failure. The probability of common cause failures which involve the system as a whole depends on the complexity of the system (possibly dominated by the user software) and not on the hardware alone. Clearly, any calculations based on the probability of random hardware failure cannot take into account the complexity of the software;

– reporting of common cause failures is generally limited to hardware failures, the area of most concern to the manufacturers of the hardware;

– it is not considered practicable to model systematic failures (for example software failures);

– the measures specified in IEC 61508-3 are intended to reduce the probability of software-related common cause failure to an acceptable level for the target safety integrity level.

Therefore, the estimate of the probability of common cause failure derived by this methodology relates to only those failures associated with the hardware. It should NOT be assumed that the methodology can be used to obtain an overall failure rate which takes the probability of software-related failure into account.

D.3 Points taken into account in the methodology

Because sensors, logic subsystem and final elements are subject to, for example, different environmental conditions and diagnostic tests with varying levels of capability, the methodology should be applied to each of these subsystems separately. For example, the logic subsystem is more likely to be in a controlled environment, whereas the sensors may be mounted outside on pipework that is exposed to the elements.

Programmable electronic channels have the potential for carrying out sophisticated diagnostic testing functions. These can

– have a high diagnostic coverage within the channels;
– monitor additional redundancy channels;
– have a high repetition rate; and
– in an increasing number of cases, also monitor sensors and/or final elements.

A large fraction of common cause failures do not occur concurrently in all of the affected channels. Therefore, if the repetition frequency of the diagnostic tests is sufficiently high, a large fraction of common cause failures can be revealed and, hence, avoided before they affect all available channels.

Not all features of a multi-channel system, that has a bearing on its immunity to common cause failures, can be evaluated by diagnostic tests. However, those features relating to diversity or independence are made more effective. Any feature which is likely to increase the time between channel failures in a non-simultaneous common cause failure (or reduce the fraction of simultaneous common cause failures) increases the probability of the diagnostic tests detecting the failure and putting the plant into a safe state. Therefore, the features relating to immunity to common cause failures are divided into those whose effect is thought to be increased by the use of diagnostic tests and those whose effect is not. This leads to the two columns, X and Y respectively, in Table D.1.

Although, for a three-channel system, the probability of common cause failures which affect all three channels is likely to be slightly lower than the probability of failures which affect two channels, it is assumed, in order to simplify the β-factor methodology, that the probability is independent of the number of affected channels, i.e. it is assumed that if a common cause failure occurs it affects all channels. An alternative method is the shock model.

There is no known data on hardware-related common cause failures available for the calibration of the methodology. Therefore, the tables in this annex are based on engineering judgement.

Diagnostic test routines are sometimes not regarded as having a direct safety role so may not receive the same level of quality assurance as the routines providing the main control functions. The methodology was developed on the presumption that the diagnostic tests have an integrity commensurate with the target safety integrity level. Therefore, any software-based diagnostic test routines should be developed using techniques appropriate to the target safety integrity level.

D.4 Using the β-factor to calculate the probability of failure in an E/E/PE safety-related system due to common cause failures

Consider the effect of common cause failures on a multi-channel system with diagnostic tests running within each of its channels.

Using the β-factor model, the common cause dangerous failure rate is:

$$\lambda_D \beta$$

where

λ_D is the random hardware dangerous failure rate for each individual channel and β is the β-factor in the absence of diagnostic tests, i.e. the fraction of single-channel failures that affect all channels.

We now assume that common cause failures affect all channels, and that the span of time between the first channel and all channels being affected is small compared to the time interval between successive common cause failures.

Suppose that there are diagnostic tests running in each channel which detect and reveal a fraction of the failures. We can divide all failures into two categories: those that lie outside the coverage of the diagnostic tests (and so can never be detected) and those that lie within the coverage (so would eventually be detected by the diagnostic tests).

The overall failure rate due to dangerous common cause failures is then given by:

$$\lambda_{DU}\beta + \lambda_{DD}\beta_D$$

where

- λ_{DU} is the undetected dangerous failure rate of a single channel, i.e. the failure rate of the failures which lie outside the coverage of the diagnostic tests; clearly, any reduction in the β-factor resulting from the repetition rate of the diagnostic tests cannot affect this fraction of the failures;
- β is the common cause failure factor for undetectable dangerous faults, which is equal to the overall β-factor that would be applicable in the absence of diagnostic testing;
- λ_{DD} is the detected dangerous failure rate of a single channel, i.e. the failure rate of the failures of a single channel that lie within the coverage of the diagnostic tests. If the repetition rate of the diagnostic tests is high, a fraction of the failures are revealed leading to a reduction in the value of β, i.e. β_D;
- β_D is the common cause failure factor for detectable dangerous faults. As the repetition rate of the diagnostic testing is increased, the value of β_D falls increasingly below β;
- β is obtained from Table D.5 which uses the results of D.4, using a score, $S = X + Y$ (see D.5);
- β_D is obtained from Table D.5 which uses the results of D.4, using a score, $S_D = X(Z+1)+Y$.

D.5 Using the tables to estimate β

The β-factor should be calculated for the sensors, the logic subsystem and the final elements separately.

In order to minimize the probability of occurrence of common cause failures, one should first establish which measures lead to an efficient defence against their occurrence. The implementation of the appropriate measures in the system lead to a reduction in the value of the β-factor used in estimating the probability of failure due to common cause failures.

Table D.1 lists the measures and contains associated values, based on engineering judgement, which represent the contribution each measure makes in the reduction of common cause failures. Because sensors and final elements are treated differently to the programmable electronics, separate columns are used in the table for scoring the programmable electronics and the sensors or final elements.

Extensive diagnostic tests may be incorporated into programmable electronic systems which allow the detection of non-simultaneous common cause failures. To allow diagnostic tests to be taken into account in the estimation of the β-factor, the overall contribution of each measure in Table D.1 is divided, using engineering judgement, into two sets of values, X and Y. For each measure, the X:Y ratio represents the extent to which the measure's contribution against common clause failures can be improved by diagnostic testing.

The user of Table D.1 should ascertain which measures apply to the system in question, and sum the corresponding values shown in each of columns X_{LS} and Y_{LS} for the logic subsystem,

or X_{SF} and Y_{SF} for the sensors or final elements, the sums being referred to as X and Y, respectively.

Tables D.2 and D.3 may be used to determine a factor Z from the frequency and coverage of the diagnostic tests, taking into account the important Note 4 which limits when a non-zero value of Z should be used. The score S is then calculated using the following equations, as appropriate (see previous clause):

– $S = X + Y$ to obtain the value of β_{int} (the β-factor for undetected failures); and

– $S_D = X(Z + 1) + Y$ to obtain the value of $\beta_{\text{D int}}$ (the β-factor for detected failures).

Here S or S_D is a score which is used in Table D.4 to determine the appropriate β_{int} -factor.

β_{int} and $\beta_{\text{D int}}$ are the values of the common cause failure prior to considering the effect of different degrees of redundancy.

Table D.1 – Scoring programmable electronics or sensors/final elements

Item	Logic subsystem		Sensors and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Separation/segregation				
Are all signal cables for the channels routed separately at all positions?	1,5	1,5	1,0	2,0
Are the logic subsystem channels on separate printed-circuit boards?	3,0	1,0		
Are the logic subsystems physically separated in an effective manner? For example, in separate cabinets.	2,5	0,5		
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?			2,5	1,5
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?			2,5	0,5
Diversity/redundancy				
Do the channels employ different electrical technologies for example, one electronic or programmable electronic and the other relay?	8,0			
Do the channels employ different electronic technologies for example, one electronic, the other programmable electronic?	6,0			
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc?			9,0	
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?			6,5	
Is low diversity used, for example hardware diagnostic tests using the same technology?	2,0	1,0		
Is medium diversity used, for example hardware diagnostic tests using different technology?	3,0	2,0		
Were the channels designed by different designers with no communication between them during the design activities?	1,5	1,5		
Are separate test methods and people used for each channel during commissioning?	1,0	0,5	1,0	2,0
Is maintenance on each channel carried out by different people at different times?	3,0		3,0	
Complexity/design/application/maturity/experience				
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0,5	0,5	0,5	0,5
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	0,5	1,0	1,0	1,0
Is there more than 5 years experience with the same hardware used in similar environments?	1,0	1,5	1,5	1,5
Is the system simple, for example no more than 10 inputs or outputs per channel?		1,0		
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1,5	0,5	1,5	0,5
Are all devices/components conservatively rated (for example, by a factor of 2 or more)?	2,0		2,0	
Assessment/analysis and feedback of data				
Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3,0		3,0
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3,0		3,0
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0,5	3,5	0,5	3,5
Procedures/human interface				
Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?		1,5	0,5	1,5
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	1,5	0,5	2,0	1,0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?	0,5	0,5	0,5	0,5
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0,5	1,0	0,5	1,5
Does the system have low diagnostic coverage (60 % to 90 %) and report failures to the level of a field-replaceable module?	0,5			
Does the system have medium diagnostics coverage (90 % to 99 %) and report failures to the level of a field-replaceable module?	1,5	1,0		
Does the system have high diagnostics coverage (>99 %) and report failures to the level of a field-replaceable module?	2,5	1,5		
Do the system diagnostic tests report failures to the level of a field-replaceable module?			1,0	1,0

Table D.1 *(continued)*

Item	Logic subsystem		Sensors and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Competence/training/safety culture				
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	2,0	3,0	2,0	3,0
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?	0,5	4,5	0,5	4,5
Environmental control				
Is personnel access limited (for example locked cabinets, inaccessible position)?	0,5	2,5	0,5	2,5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3,0	1,0	3,0	1,0
Are all signal and power cables separate at all positions?	2,0	1,0	2,0	1,0
Environmental testing				
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10,0	10,0	10,0	10,0

NOTE 1 A number of the items relate to the operation of the system, which may be difficult to predict at design time. In these cases, the designers should make reasonable assumptions and subsequently ensure that the eventual user of the system is made aware of, for example, the procedures to be put in place in order to achieve the designed level of safety integrity. This could be by including the necessary information in the accompanying documentation.

NOTE 2 The values in the *X* and *Y* columns are based on engineering judgement and take into account the indirect as well as the direct effects of the items in column 1. For example, the use of field-replaceable modules leads to

– repairs being carried out by the manufacturer under controlled conditions instead of (possibly incorrect) repairs being made under less appropriate conditions in the field. This leads to a contribution in the *Y* column because the potential for systematic (and, hence, common cause) failures is reduced;

– a reduction in the need for on-site manual interaction and the ability quickly to replace faulty modules, possibly on-line, so increasing the efficacy of the diagnostics for identifying failures before they become common-cause failures. This leads to a strong entry in the *X* column.

Table D.2 – Value of *Z* – programmable electronics

Diagnostic coverage	Diagnostic test interval		
	Less than 1 min	Between 1 min and 5 min	Greater than 5 min
≥ 99 %	2,0	1,0	0
≥ 90 %	1,5	0,5	0
≥ 60 %	1,0	0	0

Table D.3 – Value of *Z* – sensors or final elements

Diagnostic coverage	Diagnostic test interval			
	Less than 2 h	Between 2 h and two days	Between two days and one week	Greater than one week
≥ 99 %	2,0	1,5	1,0	0
≥ 90 %	1,5	1,0	0,5	0
≥ 60 %	1,0	0,5	0	0

NOTE 1 The methodology is most effective if account is taken uniformly across the list of the categories in Table D.1. Therefore, it is strongly recommended that the total score in the *X* and *Y* columns for each category should be not less than the total score in the *X* and *Y* columns divided by 20. For example, if the total score (*X* + *Y*) is 80, none of the categories (for example, procedures/human interface) should have a total score (*X* + *Y*) of less than four.

NOTE 2 When using Table D.1, take account of the scores for all items that apply. The scoring has been designed to allow for items which are not mutually exclusive. For example, a system with logic subsystem channels in separate racks is entitled to both the score for "Are the logic subsystem channels in separate cabinets?" and that for "Are the logic subsystem channels on separate printed-circuit boards?".

NOTE 3 If sensors or final elements are PE-based, they should be treated as part of the logic subsystem if they are enclosed within the same building (or vehicle) as the device that constitutes the major part of the logic subsystem, and as sensors or final elements if they are not so enclosed.

NOTE 4 For a non-zero value of *Z* to be used, it should be ensured that the equipment under control is put into a safe state before a non-simultaneous common cause failure can affect all the channels. The time taken to assure this safe state should be less than the claimed diagnostic test interval. A non-zero value for *Z* can be used only if:

– the system initiates an automatic shut-down on detection of a fault; or

– a safe shut-down is not initiated after a first fault [9], but the diagnostic tests:
  – determine the locality of the fault and are capable of localizing the fault; and
  – continue to be capable of placing the EUC in a safe state after the detection of any subsequent faults; or

– a formal system of work is in place to ensure that the cause of any revealed fault is fully investigated within the claimed diagnostic test interval; and
  – if the fault has the potential for leading to a common cause failure, the plant is immediately shut-down; or
  – the faulty channel is repaired within the claimed diagnostic test interval.

NOTE 5 In the process industries, it is unlikely to be feasible to shut down the EUC when a fault is detected within the diagnostic test interval as described in Table D.2. This methodology should not be interpreted as a requirement for process plants to be shut down when such faults are detected. However, if a shut-down is not implemented, no reduction in the β-factor can be gained by the use of diagnostic tests for the programmable electronics. In some industries, a shut-down may be feasible within the described time. In these cases, a non-zero value of *Z* may be used.

NOTE 6 Where diagnostic tests are carried out in a modular way, the repetition time used in Tables D.2 or D.3 is the time between the successive completions of the full set of diagnostic testing modules. The diagnostic coverage is the total coverage provided by all of the modules.

Table D.4 – Calculation of β_{int} or $\beta_{D\ int}$

Score (*S* or S_D)	Corresponding value of β_{int} or $\beta_{D\ int}$ for the:	
	Logic subsystem	**Sensors or final elements**
120 or above	0,5 %	1 %
70 to 120	1 %	2 %
45 to 70	2 %	5 %
Less than 45	5 %	10 %
NOTE 1 The maximum levels of $\beta_{D\ int}$ shown in this table are lower than would normally be used, reflecting the use of the techniques specified elsewhere in this standard for the reduction in the probability of systematic failures as a whole, and of common cause failures as a result of this. NOTE 2 Values of $\beta_{D\ int}$ lower than 0,5 % for the logic subsystem and 1 % for the sensors would be difficult to justify.		

The β_{int} derived from Table D.4 is the common cause failure associated with a 1oo2 system. For other levels of redundancy (MooN) this β_{int} value will change as given in Table D.5 to yield the final value of β.

Table D.5 can also be used to determine the final value of β_D but where there is β_{int} this can be substituted for $\beta_{D\ int}$.

NOTE 7 For related relevant information (on PDS method) see [25] in Bibliography

9) The operation of the system on the identification of a fault should be taken into account. For example, a simple 2oo3 system should be shut down (or repaired) within the times quoted in Tables D.2 or D.3, following the identification of a single failure. If this is not done, a failure of a second channel could result in the two failed channels outvoting the remaining (good) channel. A system which automatically reconfigures itself to 1oo2 voting when one channel fails, and which automatically shuts down on the occurrence of a second failure, has an increased probability of revealing the fault in the second channel and so a non-zero value for *Z* may be claimed.

Table D.5 – Calculation of β for systems with levels of redundancy greater than 1oo2

MooN		N			
		2	3	4	5
M	1	β_{int}	0,5 β_{int}	0,3 β_{int}	0,2 β_{int}
	2	-	1,5 β_{int}	0,6 β_{int}	0,4 β_{int}
	3	-	-	1,75 β_{int}	0,8 β_{int}
	4	-	-	-	2 β_{int}

D.6 Examples of the use of the β-factor methodology

In order to demonstrate the effect of using the β-factor methodology, some simple examples have been worked through in Table D.6 for the programmable electronics.

For categories not relating to diversity nor redundancy, typical values for X and Y were used. These were obtained by halving the maximum score for the category.

In the diverse system examples, the values for the diversity/redundancy category are derived from the following properties considered in Table D.1:

– one system is electronic, the other uses relay technology;
– the hardware diagnostic tests use different technologies;
– the different designers did not communicate during the design process;
– different test methods and test personnel were used to commission the systems; and
– maintenance is carried out by different people at different times.

In the redundancy system examples, the values for the diversity/redundancy category are derived from the property that the hardware diagnostics are carried out by an independent system, which uses the same technology as the redundancy systems.

For both the diverse and redundancy systems, a maximum and minimum value was used for *Z*, leading to four example systems in total.

Table D.6 – Example values for programmable electronics

Category		Diverse system with good diagnostic testing	Diverse system with poor diagnostic testing	Non Diverse system with good diagnostic testing	Non Diverse system with poor diagnostic testing
Separation/segregation	*X*	3,50	3,50	3,50	3,50
	Y	1,50	1,50	1,50	1,50
Diversity/redundancy	*X*	14,50	14,50	2,00	2,00
	Y	3,00	3,00	1,00	1,00
Complexity/design/.....	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Assessment/analysis/....	*X*	0,25	0,25	0,25	0,25
	Y	4,75	4,75	4,75	4,75
Procedures/human interface	*X*	3,50	3,50	3,50	3,50
	Y	3,00	3,00	3,00	3,00
Competence/training/...	*X*	1,25	1,25	1,25	1,25
	Y	3,75	3,75	3,75	3,75
Environmental control	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Environmental test	*X*	5,00	5,00	5,00	5,00
	Y	5,00	5,00	5,00	5,00
Diagnostic coverage	*Z*	2,00	0,00	2,00	0,00
Total *X*		33,5	33,5	21	21
Total *Y*		25,5	25,5	23,5	23,5
Score *S*		59	59	44,5	44,5
β		2 %	2 %	5 %	5 %
Score S_D		126	59	86,5	44,5
β_D		0,5 %	2 %	1 %	5 %
Diverse system 1002 (Table D.5) Non Diverse system is triplex with 2003 voting (Table D.5)		0,5 %	2 %	1,5 %	7,5 %

D.7 Binomial failure rate (Shock model) – CCF approach

The common cause failure (CCF) field feedback shows that if numerous double failures, a few triple failures and perhaps one quadruple failure have been observed, no multiple failures beyond order four have ever been observed from an explicit single cause which could not have been identified during the safety analysis. Consequently, the probability of multiple dependent failures decreases when the order of the CCF increases. Therefore, if the β-factor model is realistic for double failures and slightly pessimistic for triple failures it becomes much too conservative for quadruple failures and beyond. Let us consider the typical example of a safety instrumented system which closes the n production wells (e.g. n=150) of an oil field when a blocked outlet is occurring. Of course 2, 3 or even 4 wells may fail to close due to a non explicit CCF but not the n wells as modelled by the β-factor (otherwise the CCF would be explicit and should be analysed as an individual failure). Another typical example occurs when dealing with several safety layers at the same time. Considering, for example, the potential CCF between sensors of two protection layers may imply to consider the CCFs between six sensors (i.e. 3 sensors for each layer).

Several models have been proposed [18] to deal with this difficulty but most of them require so many reliability parameters (e.g. multiple Greek letters or α-models) that they become unrealistic. Among them, the binomial failure rate (Shock model) introduced by Vesely in 1977 and improved by Atwood in 1986 provides a pragmatic solution [18, 19]. The principle is that when a CCF occurs, it is similar to a shock on the related components. This shock may be lethal (i.e. same impact as in the β-factor model) or non-lethal and in this case there is only a certain probability that a given component fails due to the shock. Then the probability of having *k* failures due to the non-lethal shock is binomially distributed.

This model needs only 3 parameters to be implemented:

- ω lethal shock rate;
- ρ non-lethal shock rate;
- γ conditional probability of failure of a component given a non-lethal shock.

Figure D.2 gives an example on implementing this method when using a fault tree.

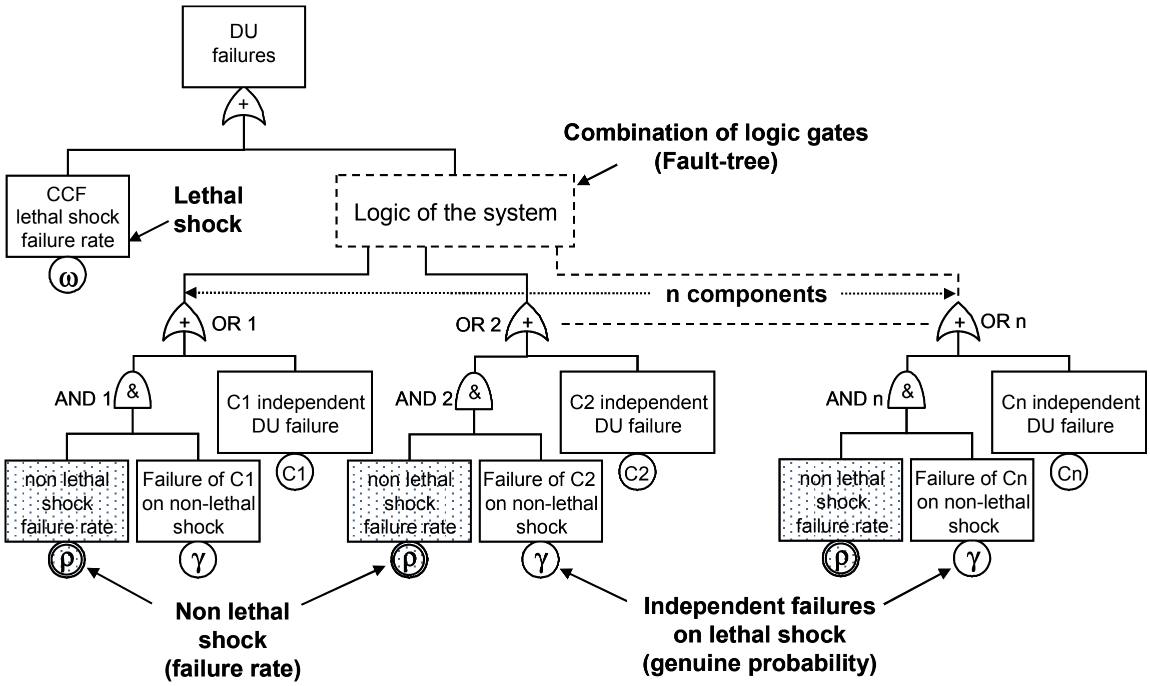


Figure D.2 – Implementing shock model with fault trees

Identical components can be linked to the *β*-factor model by splitting β in two parts β_L and β_{NL}:

- $\beta = \beta_L + \beta_{NL}$
- failure rate due to lethal shock: $\lambda_{DU} \times \beta_L$
- failure rate due to non lethal shock: $\lambda_{DU} \times \beta_{NL}$
- independent failure rate: $\lambda_{DU}[1 - (\beta_L + \beta_{NL})]$

In the fault tree represented in Figure D.2, this becomes:

- lethal shock rate: $\omega = \lambda_{DU} \times \beta_L$
- non-lethal shock rate : $\rho = \lambda_{DU} \times \beta_{NL} / \gamma$

As usual, the main problem is to evaluate the values of the three parameters (ω, ρ, γ) or (β_L, β_{NL}, $\tilde{\gamma}$) Reference [19] gives some indications and provides other references about the statistical treatments allowing to evaluate(ω, ρ, γ) from field feedback.

If no data are available the engineering judgement can be used through pragmatic approaches. For example the following procedure may be used with fault tree modelling when there are more than 3 similar items:

1) estimate β as in the β-factor method;
2) consider that β_L is negligible ($\beta_{NL} = \beta$);

3) estimate γ in order to be sure to obtain conservative results. Considered that double failures have at least an impact 10 times higher than the quadruple failure (hypothesis which is certainly conservative), the following formula may be used:

$$\gamma = \sqrt{\frac{C_N^2}{10.C_N^4}}$$

where

N is the number of similar items;

C_N^2 is the number of potential double failures; and

C_N^4 is the number of potential quadruple failures

4) calculate ρ in function of the number N of similar items:

$$\rho = \frac{\beta\lambda_{DU}}{C_N^2\gamma^2 + C_N^3\gamma^3}$$

In this method of working, the top contributors are double and triple failures and the results are conservative compared to the results obtained with the β factor method with only 3 components. The CCF double and triple failures are taken under consideration properly and unrealistic multiple failures are not completely neglected.

This model is very easily implemented into fault tree calculation models like those presented in Annex B, e.g. fault trees in B.4.3. This allows handling safety systems comprising a lot of similar components in a very simple and easy way.

D.8 References

References [13] to [15] and [20] and [21] in the Bibliography provide useful information relating to common cause failures.

Annex E
(informative)

Example applications of software safety integrity tables of IEC 61508-3

E.1 General

This annex gives two worked examples in the application of the software safety integrity tables specified in Annex A of IEC 61508-3:

a) safety integrity level 2: a programmable electronic safety-related system required for a process within a chemical plant;

b) safety integrity level 3: a shut-down application based on a high-level language.

These examples illustrate how software development techniques might be selected in particular circumstances from the tables of Annexes A and B of IEC 61508-3.

It should be emphasized that these illustrations are not definitive applications of the standard to these examples. IEC 61508-3 states clearly at several points that given the large number of factors that affect software systematic capability, it is not possible to give an algorithm for combining the techniques and measures that will be correct for any given application.

For a real system, all the entries in the tables should be supported by documented justification that the comments made are correct and that they represent an appropriate response for the particular system and application. This justification is likely to be assisted by referring to the guidance of IEC 61508-3 Annex C which discusses the desirable properties which, if achieved in the appropriate lifecycle phase, may convincingly justify confidence that the eventual software has sufficient systematic safety integrity.

E.2 Example for safety integrity level 2

This example is a safety integrity level 2 programmable electronic safety-related system required for a process within a chemical plant. The programmable electronic safety-related system utilizes ladder logic for the application program, and is an illustration of limited variability language application programming.

The application consists of several reactor vessels linked by intermediate storage vessels which are filled with inert gas at certain points in the reaction cycle to suppress ignition and explosions. The programmable electronic safety-related system functions include: receiving inputs from the sensors; energizing and interlocking the valves, pumps and actuators; detecting dangerous situations and activating the alarm; interfacing to a distributed control system, as required by the safety requirements specification.

Assumptions:

– the programmable electronic safety-related system controller is a PLC;

– the hazard and risk analysis has established that a programmable electronic safety-related system is required, and that safety integrity level 2 is required in this application (by the application of IEC 61508-1 and IEC 61508-2);

– although the controller operates in real time, only a relatively slow response is needed;

– there are interfaces to a human operator and to a distributed control system;

– the source code of the system software and the design of the programmable electronics of the PLC is not available for examination, but has been qualified against IEC 61508-3 to safety integrity level 2;

– the language used for application programming is ladder logic, produced using the PLC supplier's development system;

– the application code is required to run on only a single type of PLC;

– the whole of the software development was reviewed by a person independent of the software team;

– a person independent of the software team witnessed and approved the validation testing;

– modifications (if needed) require authorization by a person independent of the software team.

NOTE 1 For the definition of an independent person, see IEC 61508-4.

NOTE 2 See the notes to 7.4.2, 7.4.3, 7.4.4 and 7.4.5 of IEC 61508-3 for information on the division of responsibility between the PLC supplier and user when limited variability programming is used.

The following tables show how Annex A of IEC 61508-3 may be interpreted for this application.

Table E.1 – Software safety requirements specification

(See 7.2 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1a	Semi-formal methods	Table B.7	R	Cause-effect diagrams, sequence diagrams, function blocks. Typically used for PLC application software requirements specification
1b	Formal methods	B.2.2, C.2.4	R	Not used for limited variability programming
2	Forward traceability between the system safety requirements and the software safety requirements	C.2.11	R	Check completeness: review to ensure that all system safety requirements are addressed by software safety requirements
3	Backward traceability between the safety requirements and the perceived safety needs	C.2.11	R	Minimise complexity and functionality: review to ensure that all software safety requirements are actually needed to address system safety requirements
4	Computer-aided specification tools to support appropriate techniques/measures above	B.2.4	R	Development tools supplied by the PLC manufacturer

NOTE 1 In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.

NOTE 2 The software safety requirements were specified in natural language.

Table E.2 – Software design and development – software architecture design

(see 7.4.3 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Fault detection	C.3.1	R	Checking of data range, watch-dog timer, I/O, communication. Raise an alarm if errors (see 3a)
2	Error detecting codes	C.3.2	R	Embedded with user options - careful selection required
3a	Failure assertion programming	C.3.3	R	Dedicate some PLC program ladder logic to test certain essential safety conditions (see 1)
3b	Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer)	C.3.4	R	Not preferred: increased software complexity to guarantee independence.
3c	Diverse monitor techniques (with separation between the monitor computer and the monitored computer)	C.3.4	R	Check legal I/O combinations in an independent hardware safety monitor
3d	Diverse redundancy, implementing the same software safety requirements specification	C.3.5	---	Not preferred: insufficient increased safety benefit over 3c.
3e	Functionally diverse redundancy, implementing different software safety requirements specification	C.3.5	---	Not preferred: substantially achieved by 3c.
3f	Backward recovery	C.3.6	R	Embedded with user options – careful selection required
3g	Stateless software design (or limited state design)	C.2.12	---	Not used. Process control needs states to memorise plant condition.
4a	Re-try fault recovery mechanisms	C.3.7	R	Used as required by the application (see 2 and 3c)
4b	Graceful degradation	C.3.8	R	Not used for limited variability programming
5	Artificial intelligence - fault correction	C.3.9	NR	Not used for limited variability programming
6	Dynamic reconfiguration	C.3.10	NR	Not used for limited variability programming
7	Modular approach	Table B.9	HR	
8	Use of trusted/verified software elements (if available)	C.2.10	HR	Pre-existing code from earlier projects
9	Forward traceability between the software safety requirements specification and software architecture	C.2.11	R	Check completeness: review to ensure that all software safety requirements are addressed by the software architecture
10	Backward traceability between the software safety requirements specification and software architecture	C.2.11	R	Minimise complexity and functionality: review to ensure that all architecture safety requirements are actually needed to address software safety requirements
11a	Structured diagrammatic methods	C.2.1	HR	Data flow methods and data logic tables may be used for representing at least the design architecture
11b	Semi-formal methods	Table B.7	R	May be used for DCS interface
11c	Formal design and refinement methods	B.2.2, C.2.4	R	Rarely used for limited variability programming
11d	Automatic software generation	C.4.6	R	Not used for limited variability programming
12	Computer-aided specification and design tools	B.2.4	R	Development tools supplied by the PLC manufacturer

Technique/Measure		Ref.	SIL 2	Interpretation in this application
13a	Cyclic behaviour, with guaranteed maximum cycle time	C.3.11	HR	Not used. Hardware monitoring of PLC cycle time.
13b	Time-triggered architecture	C.3.11	HR	Not used. Hardware monitoring of PLC cycle time.
13c	Event-driven, with guaranteed maximum response time	C.3.11	HR	Not used. Hardware monitoring of PLC cycle time.
14	Static resource allocation	C.2.6.3	R	Not used. Dynamic resources issues do not arise in limited variability programming
15	Static synchronisation of access to shared resources	C.2.6.3	---	Not used. Dynamic resources issues do not arise in limited variability programming
NOTE 1 In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B. NOTE 2 It is impractical to implement some of the above techniques in limited variability programming.				

Table E.3 – Software design and development – support tools and programming language

(See 7.4.4 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Suitable programming language	C.4.5	HR	Usually ladder, and often the proprietary variety of the PLC supplier
2	Strongly typed programming language	C.4.1	HR	Not used. Use PLC-oriented structured text (see [16] in the Bibliography)
3	Language subset	C.4.2	---	Beware of complex "macro" instructions, interrupts which alter PLC scan cycle, etc.
4a	Certified tools and certified translators	C.4.3	HR	Available from some PLC manufacturers
4b	Tools and translators: increased confidence from use	C.4.4	HR	PLC supplier's development kit; in-house tools developed over several projects
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.4 – Software design and development – detailed design

(See 7.4.5 and 7.4.6 of IEC 61508-3)
(Includes software system design, software module design and coding)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1a	Structured methods	C.2.1	HR	Not used for limited variability programming
1b	Semi-formal methods	Table B.7	HR	Cause-effect diagrams, sequence diagrams, function blocks. Typical for limited variability programming
1c	Formal design and refinement methods	B.2.2, C.2.4	R	Not used for limited variability programming
2	Computer-aided design tools	B.3.5	R	Development tools supplied by the PLC manufacturer
3	Defensive programming	C.2.5	R	Included in the system software
4	Modular approach	Table B.9	HR	Order and group the PLC program ladder logic to maximize its modularity with respect to the functions required
5	Design and coding standards	C.2.6 Table B.1	HR	In-house conventions for documentation and maintainability
6	Structured programming	C.2.7	HR	Similar to modularity in this context
7	Use of trusted/verified software elements (if available)	C.2.10	HR	Function blocks, part programs
8	Forward traceability between the software safety requirements specification and software design	C.2.11	R	Check completeness: review to ensure that all software safety requirements are addressed by the software design

NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.

Table E.5 – Software design and development – software module testing and integration

(See 7.4.7 and 7.4.8 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Probabilistic testing	C.5.1	R	Not used for limited variability programming
2	Dynamic analysis and testing	B.6.5 Table B.2	HR	Used
3	Data recording and analysis	C.5.2	HR	Records of test cases and results
4	Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	Input data is selected to exercise all specified functional cases, including error handling. Test cases from cause consequence diagrams, boundary value analysis, and input partitioning
5	Performance testing	Table B.6	R	Not used for limited variability programming
6	Model based testing	C.5.27	R	Not used for limited variability programming
7	Interface testing	C.5.3	R	Included in functional and black-box testing
8	Test management and automation tools	C.4.7	HR	Development tools supplied by the PLC manufacturer
9	Forward traceability between the software design specification and the module and integration test specifications	C.2.11	R	Check completeness: review to ensure that an adequate test is planned to examine the functionality of all modules and their integration with appropriately related modules.
10	Formal verification	C.5.12	---	Not used for limited variability programming
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.6 – Programmable electronics integration (hardware and software)

(See 7.5 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	Input data is selected to exercise all specified functional cases, including error handling. Test cases from cause consequence diagrams, boundary value analysis, and input partitioning
2	Performance testing	Table B.6	R	When the PLC system is assembled for factory acceptance test
3	Forward traceability between the system and software design requirements for hardware/software integration and the hardware/software integration test specifications	C.2.11	R	Review to ensure that the hardware/software integration tests are adequate
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.7 – Software aspects of system safety validation

(See 7.7 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Probabilistic testing	C.5.1	R	Not used for limited variability programming
2	Process simulation	C.5.18	R	Not used for limited variability programming, but becoming more commonly used in PLC systems development
3	Modelling	Table B.5	R	Not used for limited variability programming, but becoming more commonly used in PLC systems development
4	Functional and black-box testing	B.5.1 B.5.2 Table B.3	HR	Input data is selected to exercise all specified functional cases, including error handling. Test cases from cause consequence diagrams, boundary value analysis, and input partitioning
5	Forward traceability between the software safety requirements specification and the software safety validation plan	C.2.11	R	Check completeness: review to ensure that adequate software validation tests are planned to address the software safety requirements
6	Backward traceability between the software safety validation plan and the software safety requirements specification	C.2.11	R	Minimise complexity: review to ensure that all validation tests are relevant.
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.8 – Software modification

(See 7.8 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Impact analysis	C.5.23	HR	An impact analysis is carried out to consider how the effect of the proposed changes is limited by the modularity of the overall system
2	Reverify changed software module	C.5.23	HR	Repeat earlier tests
3	Reverify affected software modules	C.5.23	HR	Repeat earlier tests
4a	Revalidate complete system	Table A.7	R	Impact analysis showed that the modification is necessary, so revalidation is done as required
4b	Regression validation	C.5.25	HR	
5	Software configuration management	C.5.24	HR	Baselines, records of changes, impact on other system requirements
6	Data recording and analysis	C.5.2	HR	Records of test cases and results
7	Forward traceability between the Software safety requirements specification and the software modification plan (including reverification and revalidation)	C.2.11	R	Adequate modification procedures to achieve the software safety requirements
8	Backward traceability between the software modification plan (including reverification and revalidation)and the Software safety requirements specification	C.2.11	R	Adequate modification procedures to achieve the software safety requirements
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.9 – Software verification

(See 7.9 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Formal proof	C.5.12	R	Not used for limited variability programming
2	Animation of specification and design	C.5.26	R	
3	Static analysis	B.6.4 Table B.8	HR	Clerical cross-referencing of usage of variables, conditions, etc.
4	Dynamic analysis and testing	B.6.5 Table B.2	HR	Automatic test harness to facilitate regression testing
5	Forward traceability between the software design specification and the software verification (including data verification) plan	C.2.11	R	Check completeness: review to ensure adequate test of functionality.
6	Backward traceability between the software verification (including data verification) plan and the software design specification	C.2.11	R	Minimise complexity: review to ensure that all verification tests are relevant.
7	Offline numerical analysis	C.2.13	R	Not used. The numerical stability of calculations is not a major concern here
Software module testing and integration		See Table E.5 of this standard		
Programmable electronics integration testing		See Table E.6 of this standard		
Software system testing (validation)		See Table E.7 of this standard		
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.10 – Functional safety assessment

(see Clause 8 of IEC 61508-3)

Technique/Measure		Ref.	SIL 2	Interpretation in this application
1	Checklists	B.2.5	R	Used
2	Decision/truth tables	C.6.1	R	Used to a limited degree
3	Failure analysis	Table B.4	R	Cause-consequence diagrams at system level, but otherwise, failure analysis is not used for limited variability programming
4	Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3	R	Not used for limited variability programming
5	Reliability block diagram	C.6.4	R	Not used for limited variability programming
6	Forward traceability between the requirements of Clause 8 and the plan for software functional safety assessment	C.2.11	R	Check completeness of coverage of the functional safety assessment
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

E.3 Example for safety integrity level 3

This second example is a shut-down application based on a high-level language, of safety integrity level 3.

The software system is relatively large in terms of safety systems; more than 30 000 lines of source code are developed specifically for the system. Also, the usual intrinsic functions are used – at least two diverse operating systems and pre-existing code from earlier projects (proven in use). In total, the system constitutes more than 100 000 lines of source code, if it were available as such.

The whole hardware (including sensors and actuators) is a dual-channel system with its outputs to the final elements connected as a logical AND.

Assumptions:

– although fast response is not required a maximum response time is guaranteed;
– there are interfaces to sensors, actuators and annunciators to human operators;
– the source code of the operating systems, graphic routines and commercial mathematical routines is not available;
– the system is very likely to be subject to later changes;
– the specifically developed software uses one of the common procedural languages;
– it is partially object oriented;
– all parts for which source code is not available are implemented diversely, with the software components being taken from different suppliers and their object code generated by diverse translators;
– the software runs on several commercially available processors that fulfil the requirements of IEC 61508-2;
– all requirements of IEC 61508-2 for control and avoidance of hardware faults are fulfilled by the embedded system; and
– the software development was assessed by an independent organization.

NOTE For the definition of an independent organization, see IEC 61508-4.

The following tables show how the annex tables of IEC 61508-3 may be interpreted for this application.

Table E.11 – Software safety requirements specification

(See 7.2 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1a	Semi-formal methods	Table B.7	HR	Block diagrams, sequence diagrams, state transition diagrams
1b	Formal methods	B.2.2, C.2.4	R	Only exceptionally
2	Forward traceability between the system safety requirements and the software safety requirements	C.2.11	HR	Check completeness: review to ensure that all system safety requirements are addressed by software safety requirements
3	Backward traceability between the safety requirements and the perceived safety needs	C.2.11	HR	Minimise complexity and functionality: review to ensure that all software safety requirements are actually needed to address system safety requirements
4	Computer-aided specification tools to support appropriate techniques/measures above	B.2.4	HR	Tools supporting the chosen methods
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.12 – Software design and development – software architecture design

(see 7.4.3 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Fault detection	C.3.1	HR	Used as far as dealing with sensor, actuator and data transmission failures and which are not covered by the measures within the embedded system according to the requirements of IEC 61508-2
2	Error detecting codes	C.3.2	R	Only for external data transmissions
3a	Failure assertion programming	C.3.3	R	Results of the application functions are checked for validity
3b	Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer)	C.3.4	R	Not preferred: increased software complexity to guarantee independence.
3c	Diverse monitor techniques (with separation between the monitor computer and the monitored computer)	C.3.4	R	Used for some safety related functions where 3a is not used
3d	Diverse redundancy, implementing the same software safety requirements specification	C.3.5	---	Used for some functions where source code is not available
3e	Functionally diverse redundancy, implementing different software safety requirements specification	C.3.5	R	Not preferred: substantially achieved by 3c.
3f	Backward recovery	C.3.6	---	Not used
3g	Stateless software design (or limited state design)	C.2.12	R	Not used. A controlled shutdown needs states to memorise plant condition.
4a	Re-try fault recovery mechanisms	C.3.7	---	Not used
4b	Graceful degradation	C.3.8	HR	Yes, because of the nature of the technical process

Technique/Measure		Ref.	SIL 3	Interpretation in this application
5	Artificial intelligence - fault correction	C.3.9	NR	Not used
6	Dynamic reconfiguration	C.3.10	NR	Not used
7	Modular approach	Table B.9	HR	Needed because of the size of the system
8	Use of trusted/verified software elements (if available)	C.2.10	HR	pre-existing code from earlier projects
9	Forward traceability between the software safety requirements specification and software architecture	C.2.11	HR	Review to ensure that all software safety requirements are addressed by the software architecture
10	Backward traceability between the software safety requirements specification and software architecture	C.2.11	HR	Minimise complexity and functionality: review to ensure that all architecture safety requirements are actually needed to address software safety requirements
11a	Structured diagrammatic methods	C.2.1	HR	Needed because of the size of the system
11b	Semi-formal methods	Table B.7	HR	Block diagrams, sequence diagrams, state transition diagrams
11c	Formal design and refinement methods	B.2.2, C.2.4	R	Not used
11d	Automatic software generation	C.4.6	R	Not used. Avoid translator/generator uncertainty.
12	Computer-aided specification and design tools	B.2.4	HR	Tools supporting the chosen method
13a	Cyclic behaviour, with guaranteed maximum cycle time	C.3.11	HR	Not used
13b	Time-triggered architecture	C.3.11	HR	Not used
13c	Event-driven, with guaranteed maximum response time	C.3.11	HR	Not used
14	Static resource allocation	C.2.6.3	HR	Not used. Choose programming language to avoid dynamic resources issues
15	Static synchronisation of access to shared resources	C.2.6.3	R	Not used. Choose programming language to avoid dynamic resources issues
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.13 – Software design and development – support tools and programming language

(See 7.4.4 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Suitable programming language	C.4.5	HR	Full variability high-level language selected
2	Strongly typed programming language	C.4.1	HR	Used
3	Language subset	C.4.2	HR	Defined subset for the selected language
4a	Certified tools and certified translators	C.4.3	HR	Not available
4b	Tools and translators: increased confidence from use	C.4.4	HR	Available, and used
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.14 – Software design and development – detailed design

(See 7.4.5 and 7.4.6 of IEC 61508-3)
(Includes software system design, software module design and coding)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1a	Structured methods	C.2.1	HR	Widely used. In particular, SADT and JSD
1b	Semi-formal methods	Table B.7	HR	Finite state machines/state transition diagrams, block diagrams, sequence diagrams
1c	Formal design and refinement methods	B.2.2, C.2.4	R	Only exceptionally, for some very basic components only
2	Computer-aided design tools	B.3.5	HR	Used for the selected methods
3	Defensive programming	C.2.5	HR	All measures except those which are automatically inserted by the compiler are explicitly used in application software where they are effective
4	Modular approach	Table B.9	HR	Software module size limit, information hiding/encapsulation, one entry/one exit point in subroutines and functions, fully defined interface, …
5	Design and coding standards	C.2.6 Table B.1	HR	Use of coding standard, no dynamic objects, no dynamic variables, limited use of interrupts, limited use of pointers, limited use of recursion, no unconditional jumps, …
6	Structured programming	C.2.7	HR	Used
7	Use of trusted/verified software elements (if available)	C.2.10	HR	Available, and used
8	Forward traceability between the software safety requirements specification and software design	C.2.11	HR	Review to ensure that all software safety requirements are addressed by the software design

NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.

Table E.15 – Software design and development – software module testing and integration

(See 7.4.7 and 7.4.8 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Probabilistic testing	C.5.1	R	Used for software modules where no source code available and the definition of boundary values and equivalence classes for test data is difficult
2	Dynamic analysis and testing	B.6.5 Table B.2	HR	Used for software modules where source code is available. Test cases from boundary value analysis, performance modelling, equivalence classes and input partitioning, structure-based testing
3	Data recording and analysis	C.5.2	HR	Records of test cases and results
4	Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	Used for software module testing where no source code is available and for integration testing. Input data is selected to exercise all specified functional cases, including error handling. Test cases from cause consequence diagrams, prototyping, boundary value analysis, equivalence classes and input partitioning

Technique/Measure		Ref.	SIL 3	Interpretation in this application
5	Performance testing	Table B.6	HR	Used during integration testing on the target hardware
6	Model based testing	C.5.27	HR	Not used
7	Interface testing	C.5.3	HR	Included in functional and black-box testing
8	Test management and automation tools	C.4.7	HR	Used where available
9	Forward traceability between the software design specification and the module and integration test specifications	C.2.11	HR	Review to ensure that the integration tests are sufficient
10	Formal verification	C.5.12	R	Not used
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.16 – Programmable electronics integration (hardware and software)

(See 7.5 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	Used as additional tests to software integration testing (see Table E.15 above) Input data is selected to exercise all specified functional cases, including error handling. Test cases from cause consequence diagrams, prototyping, boundary value analysis, equivalence classes and input partitioning
2	Performance testing	Table B.6	HR	Extensively used
3	Forward traceability between the system and software design requirements for hardware/software integration and the hardware/software integration test specifications	C.2.11	HR	Review to ensure that the integration tests are sufficient
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.17 – Software aspects of system safety validation

(See 7.7 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Probabilistic testing	C.5.1	R	Not used for validation
2	Process simulation	C.5.18	HR	Finite state machines, performance modelling, prototyping and animation
3	Modelling	Table B.5	HR	Not used for validation
4	Functional and black-box testing	B.5.1 B.5.2 Table B.3	HR	Input data is selected to exercise all specified functional cases, including error handling. Test cases from cause consequence diagrams, boundary value analysis, and input partitioning
5	Forward traceability between the software safety requirements specification and the software safety validation plan	C.2.11	HR	Check completeness: review to ensure that all software safety requirements are addressed by the validation plan
6	Backward traceability between the software safety validation plan and the software safety requirements specification	C.2.11	HR	Minimise complexity: review to ensure that all validation tests are relevant
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.18 – Modification

(See 7.8 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Impact analysis	C.5.23	HR	Used
2	Reverify changed software module	C.5.23	HR	Used
3	Reverify affected software modules	C.5.23	HR	Used
4a	Revalidate complete system	Table A.7	HR	Depends on the result of the impact analysis
4b	Regression validation	C.5.25	HR	Used
5	Software configuration management	C.5.24	HR	Used
6	Data recording and analysis	C.5.2	HR	Used
7	Forward traceability between the Software safety requirements specification and the software modification plan (including reverification and revalidation)	C.2.11	HR	Check completeness: review to ensure that the modification procedures are adequate to achieve the software safety requirements
8	Backward traceability between the software modification plan (including reverification and revalidation)and the software safety requirements specification	C.2.11	HR	Minimise complexity: review to ensure that all modification procedures are necessary
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.19 – Software verification

(See 7.9 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Formal proof	C.5.12	R	Only exceptionally, for some very basic classes only
2	Animation of specification and design	C.5.26	R	Not used
3	Static analysis	B.6.4 Table B.8 C.5.14	HR	For all newly developed code. Boundary value analysis, checklists, control flow analysis, data flow analysis, Fagan inspections, design reviews
4	Dynamic analysis and testing	B.6.5 Table B.2	HR	For all newly developed code
5	Forward traceability between the software design specification and the software verification (including data verification) plan	C.2.11	HR	Check completeness: review to ensure that the modification procedures are adequate for the software safety requirements
6	Backward traceability between the software verification (including data verification) plan and the software design specification	C.2.11	HR	Minimise complexity: review to ensure that all modification procedures are necessary
7	Offline numerical analysis	C.2.13	HR	Not used. The numerical stability of calculations is not a major concern here
Software module testing and integration		See Table E.15 of this standard		
Programmable electronics integration testing		See Table E.16 of this standard		
Software system testing (validation)		See Table E.17 of this standard		
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

Table E.20 – Functional safety assessment

(see Clause 8 of IEC 61508-3)

Technique/Measure		Ref.	SIL 3	Interpretation in this application
1	Checklists	B.2.5	R	Used
2	Decision/truth tables	C.6.1	R	Used, to a limited degree
3	Failure analysis	Table B.4	HR	Fault-tree analysis is extensively used, and cause consequence diagrams are used to a limited degree
4	Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3	HR	Used
5	Reliability block diagram	C.6.4	R	Used
6	Forward traceability between the requirements of Clause 8 and the plan for software functional safety assessment	C.2.11	HR	Check completeness of coverage of the functional safety assessment
NOTE In the reference columns (entitled Ref), the informative references “B.x.x.x”, “C.x.x.x” refer to descriptions of techniques in IEC 61508-7 Annexes B and C, while “Table A.x”, “Table B.x” refer to tables of techniques in IEC 61508-3 Annexes A and B.				

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*

The following references give further details on evaluating probabilities of failure (see Annex B).

[4] IEC 61078:2006, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

[5] IEC 61165:2006, *Application of Markov techniques*

[6] BS 5760, *Reliability of system equipment and components – Part 2: Guide to assessment of reliability*

[7] D. J. SMITH, *Reliability, maintainability and risk – Practical methods for engineers*, Butterworth-Heinemann, 5th edition, 1997, ISBN 0-7506-3752-8

[8] R. BILLINGTON and R. N. ALLAN, *Reliability evaluation of engineering systems*, Plenum, 1992, ISBN 0-306-44063-6

[9] W. M. GOBLE, *Evaluating control system reliability – Techniques and applications*, Instrument Society of America, 1992, ISBN 1-55617-128-5

Useful references for the calculation of diagnostic coverage (see Annex C) include the following.

[10] Reliability Analysis Center (RAC), *Failure Mode/Mechanism Distributions*, 1991, Department of Defense, United States of America, PO Box 4700, 201 Mill Street, Rome, NY 13440-8200, Organization report number: FMD-91, NSN 7540-01-280-5500

[11] ALLESSANDRO BIROLINI*, Qualität und Zuverlassigkeit technischer Systeme, Theorie, Praxis, Management*, Dritte Auflage,1991, Springer-Verlag, Berlin Heidelberg New York, ISBN 3-540-54067-9, 3 Aufl., ISBN 0-387-54067-9 3 ed. (available in German only)

[12] MIL-HDBK-217F, *Military Handbook Reliability prediction of electronic equipment*, 2 December 1991, Department of Defense, United States of America

The following references provide useful information relating to common cause failures (see Annex D).

[13] *Health and Safety Executive Books*, email hsebooks@prolog.uk.com

[14] R. HUMPHREYS, A., PROC., *Assigning a numerical value to the beta factor common-cause evaluation,* Reliability 1987

[15] UPM3.1, *A pragmatic approach to dependent failures assessment for standard systems*, AEA Technology, Report SRDA-R-13, ISBN 085 356 4337, 1996

The following standard is referred to in Table E.3.

[16] IEC 61131-3:2003, *Programmable controllers – Part 3: Programming languages*

[17] ISA-TR84.00.02-2002 – Parts 1-5, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques Package.

[18] IEC 61025:2006, *Fault tree analysis (FTA)*

[19] IEC 62551, *Analysis techniques for dependability – Petri Net technique*[10]

[20] ANIELLO AMENDOLA, kluwer academic publisher, ISPRA 16-19 November 1987, *Advanced seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment,* ISBN 0-7923-0268-0

[21] CORWIN L. ATWOOD, *The Binomial Failure Rate Common Cause Model,* Technometrics May 1986 Vol 28 n°2

[22] A. ARNOLD, A. GRIFFAULT, G. POINT, AND A. RAUZY. *The altarica language and its semantics*. *Fundamenta Informaticae*, 34,pp.109–124, 2000

[23] M. BOITEAU, Y. DUTUIT, A. RAUZY AND J.-P. SIGNORET, The AltaRica *Data-Flow Language in Use: Assessment of Production Availability of a MultiStates System*, *Reliability Engineering and System Safety*, Elsevier, Vol. 91, pp 747-755

[24] A. RAUZY. *Mode automata and their compilation into fault trees. Reliability Engineering and System Safety*, Elsevier 2002, Volume 78, Issue 1, pp 1-12

[25] For PDS method; see <www.sintef.no/pds>; and further background material in:Hokstad, Per; Corneliussen, Kjell Source: Reliability Engineering and System Safety, v 83, n 1, p 111-120, January 2004

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

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

[28] 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*

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

———————

10 Under consideration.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3

AVANT-PROPOS

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

La Norme internationale CEI 61508-6 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition publiée en 2000 dont elle constitue une révision technique.

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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/553/FDIS	65A/577/RVD

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

– fixe des objectifs chiffrés de défaillance pour les fonctions de sécurité exécutées par les systèmes E/E/PE relatifs à la sécurité, qui sont en rapport avec les niveaux d'intégrité de sécurité,
– fixe une limite inférieure pour les objectifs chiffrés de défaillance pour une fonction de sécurité exécutée par un système E/E/PE relatif à la sécurité unique. Pour des systèmes E/E/PE relatifs à la sécurité fonctionnant
  – en mode de fonctionnement à faible sollicitation, la limite inférieure est fixée pour une probabilité moyenne de défaillance dangereuse de 10^{-5} en cas de sollicitation,
  – en mode de fonctionnement continu ou à sollicitation élevée, la limite inférieure est fixée à une fréquence moyenne de défaillance dangereuse de 10^{-9} [h^{-1}],

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

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

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

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

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

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

Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3

1 Domaine d'application

1.1 La présente partie de la CEI 61508 contient des informations et lignes directrices sur la CEI 61508-2 et la CEI 61508-3.

– L'Annexe A présente un bref aperçu des exigences de la CEI 61508-2 et de la CEI 61508-3 et établit les étapes fonctionnelles de leur application.

– L'Annexe B donne une technique servant d'exemple pour le calcul des probabilités de défaillance du matériel; il convient de la lire conjointement au 7.4.3 et à l'Annexe C de la CEI 61508-2, et à l'Annexe D.

– L'Annexe C donne un exemple élaboré de calcul de la couverture de diagnostic; il convient de la lire conjointement avec l'Annexe C de la CEI 61508-2.

– L'Annexe D donne une méthodologie de quantification de l'effet des défaillances de cause commune relatives au matériel sur la probabilité de défaillance.

– L'Annexe E donne des exemples d'application des tableaux d'intégrité de sécurité du logiciel spécifiés dans l'Annexe A de la CEI 61508-3 pour les niveaux 2 et 3 d'intégrité de sécurité.

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

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

1.4 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-6 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

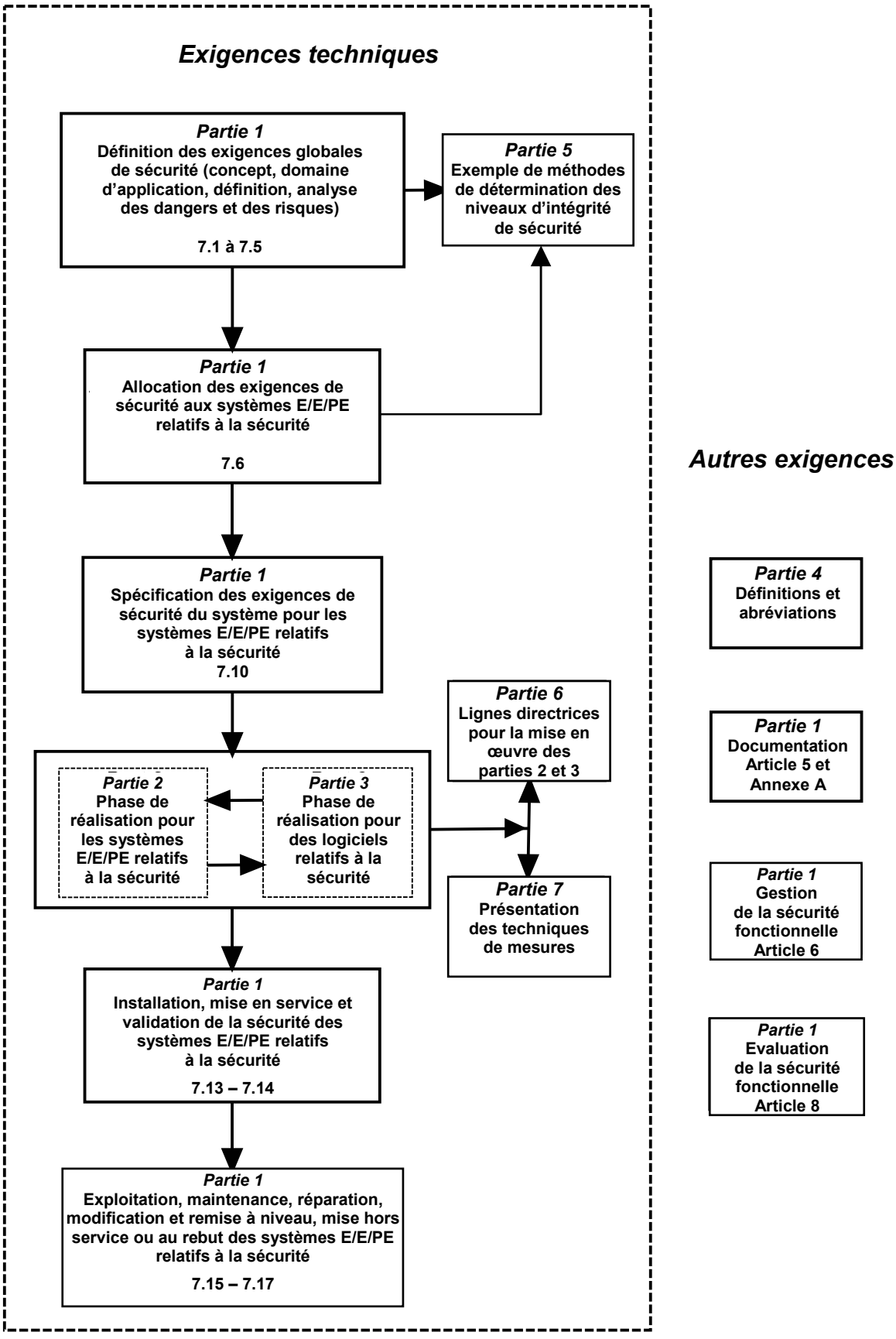


Figure 1 – Structure générale de la série CEI 61508

2 Références normatives

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

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

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

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

3 Définitions et abréviations

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

Annexe A
(informative)

Application de la CEI 61508-2 et de la CEI 61508-3

A.1 Généralités

Les machines, les installations de processus de transformation et autres équipements peuvent, en cas de dysfonctionnement (par exemple en raison de défaillances de dispositifs électriques, électroniques et/ou électroniques programmables), présenter des risques pour les individus et l'environnement résultant d'événements dangereux tels que des incendies, explosions, surexpositions aux rayonnements, incarcération, etc. Des défaillances peuvent survenir soit à cause d'anomalies physiques (provoquant par exemple des défaillances aléatoires du matériel), soit à cause d'anomalies systématiques (par exemple des erreurs humaines lors de la spécification et de la conception d'un système entraînant des défaillances systématiques dans certaines combinaisons des données), soit sous certaines conditions environnementales.

La CEI 61508-1 présente un cadre général fondé sur une approche des risques pour la prévention et/ou la maîtrise de défaillances de dispositifs électromécaniques, électroniques ou électroniques programmables.

L'objectif principal est d'assurer que les installations et les équipements peuvent être automatisés en toute sécurité. Un des objectifs clés de la présente norme est la prévention:

– de défaillances de systèmes de commande déclenchant d'autres événements, qui peuvent à leur tour entraîner un danger (par exemple un incendie, des émanations de matières toxiques, des à-coups répétés d'une machine, etc.); et
– de défaillances non détectées dans les systèmes de protection (par exemple dans un système d'arrêt d'urgence), rendant ces systèmes inopérants pour une action de sécurité.

La CEI 61508-1 exige l'exécution d'une analyse de danger et des risques au niveau processus/machine afin de déterminer l'ampleur de la réduction de risque nécessaire pour remplir les critères de risque de l'application. Le risque est fondé sur l'évaluation à la fois de la conséquence (ou sévérité) et de la fréquence (ou probabilité) de l'événement dangereux.

La CEI 61508-1 exige de plus que l'ampleur de la réduction de risque évaluée par l'analyse des risques soit utilisée pour déterminer si un ou plusieurs systèmes relatifs à la sécurité[1] sont exigés et les fonctions de sécurité (chacune ayant une intégrité de sécurité spécifiée)[2] pour lesquelles ils sont nécessaires.

Les CEI 61508-2 et 61508-3 traitent des fonctions de sécurité et exigences relatives à l'intégrité de sécurité allouée à tout système, dit système E/E/PE relatif à la sécurité, par l'application de la CEI 61508-1 et établissent les exigences relatives aux activités de cycle de vie de sécurité qui:

– doivent être appliquées lors de la spécification, de la conception et de la modification du matériel et du logiciel; et

---

1 Les systèmes nécessaires pour la sécurité fonctionnelle et comportant un ou plusieurs dispositifs électriques (électromécaniques), électroniques ou électroniques programmables (E/E/PE) sont *appelés* systèmes E/E/PE relatifs à la sécurité et comportent tous les équipements nécessaires à l'exécution de la fonction de sécurité requise (voir 3.5.1 de la CEI 61508-4).

2 L'intégrité de sécurité est spécifiée comme un parmi quatre niveaux discrets. Le niveau 4 d'intégrité de sécurité est le plus élevé et le niveau 1 d'intégrité de sécurité est le plus faible (voir 3.5.4 et 3.5.8 de la CEI 61508-4).

– se concentrent sur les moyens de prévention et/ou de maîtrise des défaillances aléatoires de matériel et des défaillances systématiques (les cycles de vie de sécurité des E/E/PE et du logiciel)[3].

Les CEI 61508-2 et 61508-3 ne donnent pas d'indication sur le niveau d'intégrité de sécurité adéquat pour un risque tolérable requis donné. Cette décision dépend de nombreux facteurs, y compris la nature de l'application, de la mesure dans laquelle d'autres systèmes réalisent les fonctions de sécurité, ainsi que de facteurs sociaux et économiques (voir les CEI 61508-1 et 61508-5).

Les exigences de la CEI 61508-2 et de la CEI 61508-3 comprennent:

– l'application de mesures et techniques[4], classées en fonction du niveau d'intégrité de sécurité, afin d'éviter des défaillances systématiques[5] par des méthodes de prévention; et

– la maîtrise de défaillances systématiques (y compris des défaillances du logiciel) et de défaillances aléatoires du matériel par des caractéristiques de conception telles que la détection d'anomalies, la redondance de caractéristiques architecturales (par exemple la diversité).

Dans la CEI 61508-2, l'assurance que l'objectif d'intégrité de sécurité a été atteint pour des défaillances aléatoires dangereuses du matériel se fonde sur:

– des exigences de tolérance aux anomalies de matériel (voir Tableaux 2 et 3 de la CEI 61508-2); et

– la couverture de diagnostic et la fréquence des essais périodiques de sous-systèmes et de composants, en effectuant une analyse de fiabilité utilisant des données appropriées.

Dans la CEI 61508-2 et la CEI 61508-3, l'assurance que l'objectif d'intégrité de sécurité a été atteint pour des défaillances systématiques est obtenue par:

– l'application correcte des procédures de gestion de la sécurité;

– la compétence établie du personnel;

– l'application des activités spécifiées du cycle de vie de sécurité, y compris les techniques et mesures spécifiées[6]; et

– une évaluation indépendante de la sécurité fonctionnelle[7].

Le principal objectif est d'assurer que les anomalies systématiques résiduelles n'entraînent pas, compte tenu du niveau d'intégrité de sécurité, une défaillance du système E/E/PE relatif à la sécurité.

---

3 Pour permettre une structure claire des exigences de la présente norme, il a été décidé d'ordonner les exigences selon un modèle de processus de développement dans lequel les étapes se suivent dans un ordre défini avec peu d'itération (parfois appelé modèle en cascade). Cependant, il est à noter que toute méthode de cycle de vie peut être utilisée pourvu qu'une déclaration d'équivalence soit fournie dans le plan de sécurité du projet (voir l'Article 7 de la CEI 61508-1).

4 Les techniques et mesures requises pour chaque niveau d'intégrité de sécurité sont données dans les tableaux des Annexes A et B de la CEI 61508-2 et de la CEI 61508-3.

5 En général, les défaillances systématiques ne peuvent pas être quantifiées. Les causes comprennent: les anomalies de spécification et de conception du matériel et du logiciel, les défaillances dues à l'environnement (par exemple la température), des défaillances liées au fonctionnement (par exemple une interface médiocre).

6 Des mesures remplaçant celles spécifiées dans la norme sont acceptables pourvu qu'elles soient justifiées lors de la planification de la sécurité (voir Article 6 de la CEI 61508-1).

7 Une évaluation indépendante n'implique pas forcément une évaluation par une tierce partie (voir l'Article 8 de la CEI 61508-1).

La CEI 61508-2 a été élaborée afin de fournir des exigences permettant de réaliser une intégrité de sécurité du matériel[8] des systèmes E/E/PE relatifs à la sécurité, y compris les capteurs et éléments finaux. Des techniques et mesures sont exigées à la fois contre les défaillances aléatoires du matériel et contre les défaillances systématiques du matériel. Cela implique une combinaison appropriée de mesures d'évitement des anomalies et de maîtrise des défaillances comme indiqué ci-dessus. Lorsqu'une action manuelle est nécessaire pour la sécurité fonctionnelle, des exigences sont fournies pour l'interface opérateur. Des techniques et mesures d'essai de diagnostic sont également spécifiées dans la CEI 61508-2; elles se fondent sur le logiciel et le matériel (par exemple la diversité) pour la détection de défaillances aléatoires du matériel.

La CEI 61508-3 a été élaborée afin de fournir des exigences permettant de réaliser l'intégrité de sécurité pour les logiciels, tant pour les logiciels systèmes (y compris les moyens de détection d'anomalies par diagnostic) que pour les logiciels applicatifs. La CEI 61508-3 exige une combinaison d'approches: évitement des anomalies (assurance de qualité) et tolérance aux anomalies (architecture du logiciel), car il n'existe aucun moyen connu permettant de prouver l'absence d'anomalies dans un logiciel relatif à la sécurité raisonnablement complexe, particulièrement l'absence d'anomalies de spécification et de conception. La CEI 61508-3 exige l'adoption de principes d'ingénierie de logiciel tels que: conception hiérarchisée, modularité, vérification de chaque phase du cycle de vie de développement, modules logiciels et bibliothèques de modules logiciels vérifiés, documents clairs pour faciliter la vérification et la validation. Les différents niveaux de logiciel exigent différents niveaux garantissant l'application correcte de ces principes et des principes qui leur sont liés.

Le développeur du logiciel peut être indépendant ou non de l'organisation qui développe l'ensemble du système E/E/PE. Dans tous les cas, une coopération étroite est nécessaire, particulièrement pour ce qui concerne le développement de l'architecture des systèmes électroniques programmables où des compromis entre les architectures du matériel et du logiciel doivent être pris en compte en termes d'impact sur la sécurité (voir Figure 4 de la CEI 61508-2).

A.2 Etapes fonctionnelles dans l'application de la CEI 61508-2

Les étapes fonctionnelles pour l'application de la CEI 61508-2 sont illustrées par les Figures A.1 et A.2. Les étapes fonctionnelles pour l'application de la CEI 61508-3 sont illustrées par la Figure A.3.

Les étapes fonctionnelles pour la CEI 61508-2 (voir Figures A.1 et A.2) sont les suivantes:

a) Obtenir l'allocation des exigences de sécurité (voir CEI 61508-1). Mettre à jour la planification de la sécurité de manière adéquate pendant le développement du système E/E/PE.

b) Déterminer les exigences pour les systèmes E/E/PE relatifs à la sécurité, y compris les exigences relatives à l'intégrité de sécurité, pour chaque fonction de sécurité (voir 7.2 de la CEI 61508-2). Attribuer des exigences au logiciel et les transmettre au fournisseur et/ou au développeur du logiciel pour l'application de la CEI 61508-3.

NOTE 1 Il est nécessaire à cette étape de prendre en compte la possibilité de défaillances coïncidentes du système de commande de l'EUC et du (des) système(s) E/E/PE relatif(s) à la sécurité (voir A.5.4 de la CEI 61508-5). Ces défaillances peuvent résulter de défaillances de composants ayant une cause commune, par exemple des influences environnementales similaires. L'existence de telles défaillances peut conduire à un risque résiduel plus élevé que prévu si les précautions appropriées n'étaient pas prises.

c) Entreprendre la phase de planification pour la validation de sécurité du système E/E/PE relatif à la sécurité (voir 7.3 de la CEI 61508-2).

d) Spécifier l'architecture (configuration) pour le sous-système logique E/E/PE relatif à la sécurité, capteurs et éléments finaux. Revoir, avec le fournisseur/développeur de logiciel,

---

[8] Y compris les logiciels fixes intégrés ou logiciels équivalents (également appelés microprogrammes), tels que les circuits intégrés à application spécifique (ASIC).

l'architecture du matériel et du logiciel ainsi que les incidences des compromis entre le matériel et le logiciel sur la sécurité (voir Figure 4 de la CEI 61508-2). Répéter cette étape si nécessaire.

e) Développer un modèle d'architecture du matériel pour le système E/E/PE relatif à la sécurité. Développer ce modèle en examinant chacune des fonctions de sécurité séparément et déterminer le sous-système (composant) à utiliser pour prendre en charge cette fonction.

f) Établir les paramètres du système pour chacun des sous-systèmes (composants) utilisés pour le système E/E/PE relatif à la sécurité. Pour chacun des sous-systèmes (composants), déterminer:

   – l'intervalle entre essais périodiques pour des défaillances qui ne sont pas automatiquement révélées;
   – la durée moyenne de rétablissement;
   – la couverture de diagnostic (voir Annexe C de la CEI 61508-2);
   – la probabilité de défaillance;
   – les contraintes architecturales requises: pour le Parcours 1_H voir 7.4.4.2 et Annexe C de la CEI 61508-2 et pour le Parcours 2_H voir 7.4.4.3 de la CEI 61508-2.

g) Créer un modèle de fiabilité pour chacune des fonctions de sécurité exigées pour le système E/E/PE relatif à la sécurité.

NOTE 2 Un modèle de fiabilité est une formule mathématique qui décrit la relation entre la fiabilité et les paramètres caractéristiques de l'équipement et des conditions d'utilisation.

h) Calculer une prévision de fiabilité pour chaque fonction de sécurité en utilisant une technique appropriée. Comparer le résultat avec l'objectif chiffré de défaillance déterminé en b) ci-dessus et les exigences du Parcours 1_H (voir 7.4.4.2 de la CEI 61508-2) ou du Parcours 2_H (voir 7.4.4.3 de la CEI 61508-2). Si la fiabilité prévue ne satisfait pas à l'objectif chiffré de défaillance et/ou ne remplit pas les exigences du Parcours 1_H ou du Parcours 2_H, modifier alors

   – un ou plusieurs paramètres du sous-système (revenir à f) ci-dessus), lorsque c'est possible et/ou
   – l'architecture du matériel (revenir à d) ci-dessus).

NOTE 3 Plusieurs méthodes de modélisation sont disponibles et il convient que l'analyste choisisse la plus appropriée (voir Annexe B pour des recommandations sur quelques méthodes qui peuvent être utilisées).

i) Mettre en œuvre la conception du système E/E/PE relatif à la sécurité. Choisir des mesures et techniques de maîtrise de défaillances systématiques du matériel, des défaillances dues à des influences environnementales et opérationnelles (voir Annexe A de la CEI 61508-2).

j) Intégrer le logiciel vérifié (voir la CEI 61508-3) dans le matériel cible (voir 7.5 de la CEI 61508-2 et l'Annexe B de la CEI 61508-2), développer parallèlement les procédures que les utilisateurs et l'équipe de maintenance suivent lors de l'exploitation du système (voir 7.6 de la CEI 61508-2 et l'Annexe B de la CEI 61508-2). Inclure des aspects logiciels (voir A.3 f)).

k) En collaboration avec le développeur du logiciel (voir 7.7 de la CEI 61508-3), valider le système E/E/PE relatif à la sécurité (voir 7.7 de la CEI 61508-2 et l'Annexe B de la CEI 61508-2).

l) Remettre le matériel et les résultats de la validation de sécurité du système E/E/PE relatif à la sécurité aux ingénieurs système pour intégration ultérieure dans le système global.

m) Si une maintenance/modification du système E/E/PE relatif à la sécurité est nécessaire pendant la durée de vie opérationnelle, relancer alors la CEI 61508-2 comme indiqué (voir 7.8 de la CEI 61508-2).

Un certain nombre d'activités s'appliquent pendant tout le cycle de vie du système E/E/PE relatif à la sécurité. Cela comprend la vérification (voir 7.9 de la CEI 61508-2) et l'évaluation de la sécurité fonctionnelle (voir l'Article 8 de la CEI 61508-1).

En appliquant les étapes mentionnées ci-dessus, les techniques et mesures de sécurité du système E/E/PE relatif à la sécurité appropriées au niveau d'intégrité de sécurité requis sont sélectionnées. Pour faciliter cette sélection, des tableaux ont été élaborés, évaluant les différentes techniques/mesures selon les quatre niveaux d'intégrité de sécurité (voir l'Annexe B de la CEI 61508-2). Un aperçu de chaque technique et mesure, correspondant à ces tableaux et comprenant des références à d'autres sources d'information, est fourni (voir les Annexes A et B de la CEI 61508-7).

L'Annexe B donne une technique possible de calcul des probabilités de défaillance du matériel pour les systèmes E/E/PE relatifs à la sécurité.

NOTE 4 Lors de l'application des étapes ci-dessus, des mesures remplaçant celles spécifiées dans la norme sont acceptables pourvu qu'elles soient justifiées lors de la planification de la sécurité (voir Article 6 de la CEI 61508-1).

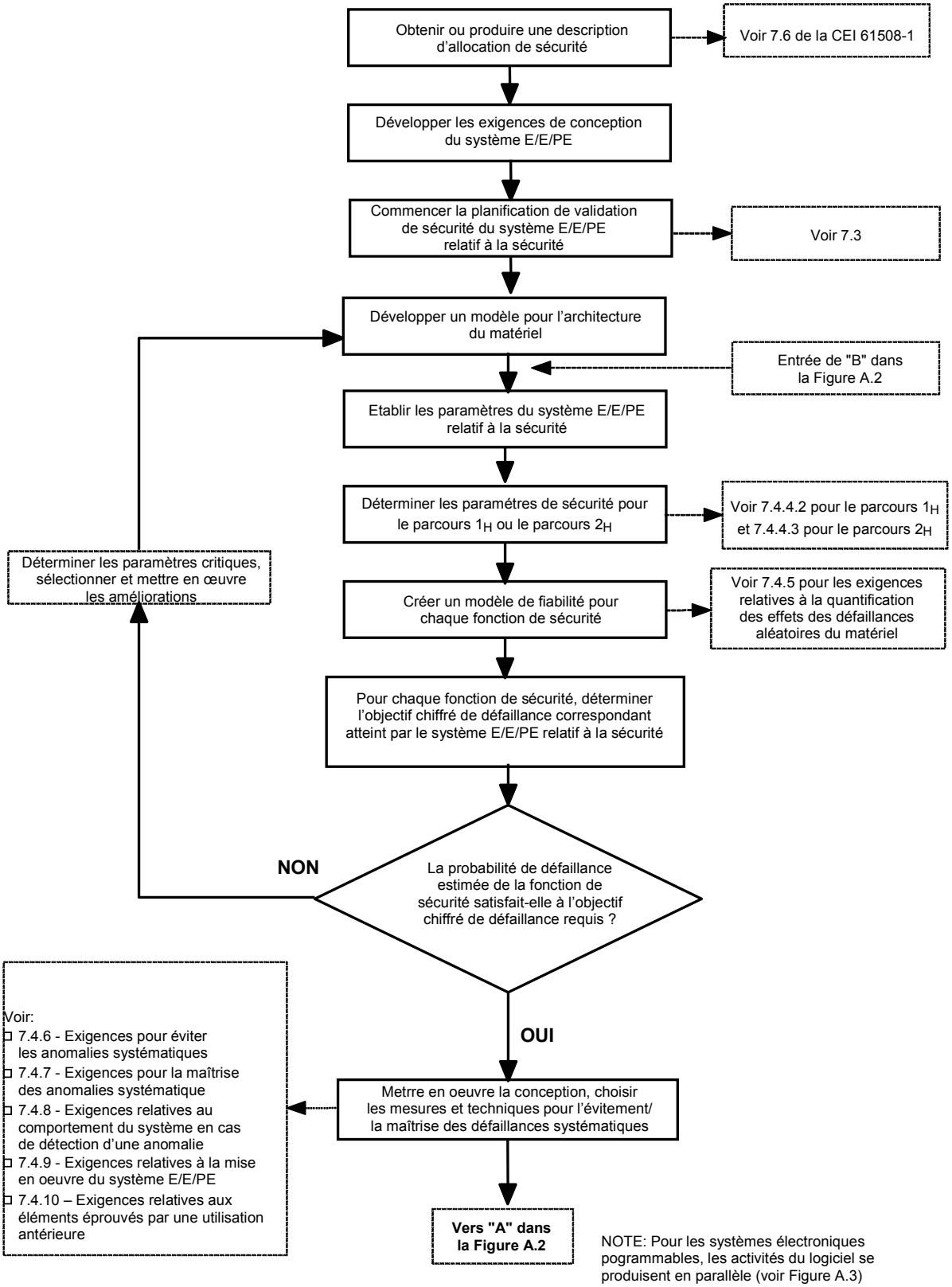
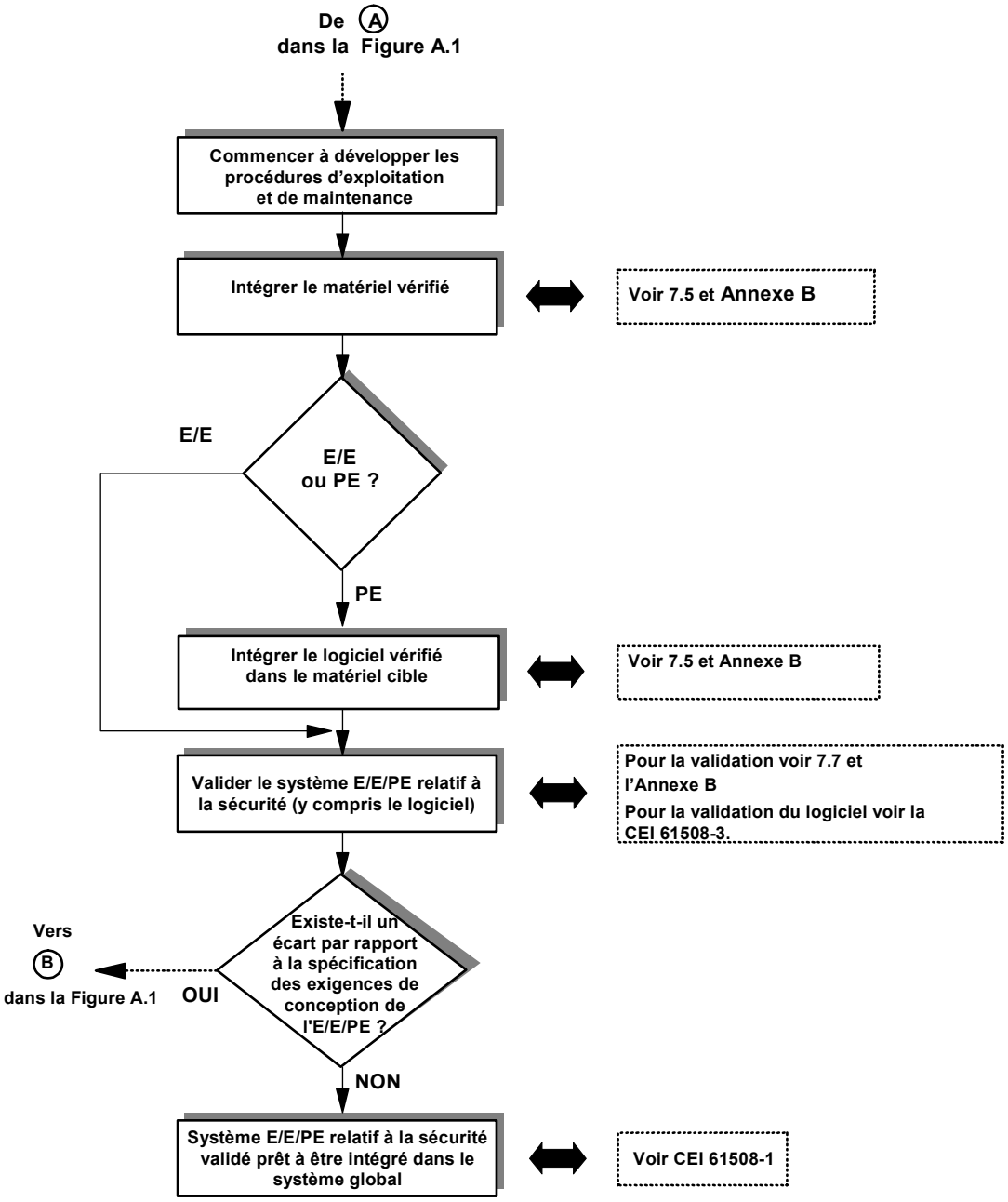


Figure A.1 – Application de la CEI 61508-2



NOTE Pour les systèmes électroniques programmables relatifs à la sécurité, les activités du logiciel se produisent en parallèle (voir Figure A.3)

Figure A.2 – Application de la CEI 61508-2 (Figure A.1 *suite*)

A.3 Étapes fonctionnelles pour l'application de la CEI 61508-3

Les étapes fonctionnelles pour la CEI 61508-3 (voir Figure A.3) sont les suivantes.

a) Obtenir les exigences pour les systèmes E/E/PE relatifs à la sécurité et les parties pertinentes de la planification de sécurité (voir 7.3 de la CEI 61508-2). Mettre à jour la planification de sécurité de manière adéquate pendant le développement du logiciel.

NOTE 1 Des phases précédentes du cycle de vie ont déjà:

– spécifié les fonctions de sécurité requises et les niveaux d'intégrité de sécurité correspondants (voir 7.4 et 7.5 de la CEI 61508-1);

– alloué les fonctions de sécurité à des systèmes E/E/PE relatifs à la sécurité (voir 7.6 de la CEI 61508-1); et

- alloué des fonctions au logiciel dans chaque système E/E/PE relatif à la sécurité (voir 7.2 de la CEI 61508-2).

b) Déterminer l'architecture du logiciel pour toutes les fonctions de sécurité allouées au logiciel (voir 7.4 de la CEI 61508-3 et l'Annexe A de la CEI 61508-3).

c) Revoir, en collaboration avec le fournisseur/développeur du système E/E/PE relatif à la sécurité, l'architecture du logiciel et du matériel ainsi que les incidences des compromis entre logiciel et matériel sur la sécurité (voir Figure 4 de la CEI 61508-2). Répéter si nécessaire.

d) Entamer la planification de la vérification et de la validation de la sécurité du logiciel (voir 7.3 et 7.9 de la CEI 61508-3).

e) Concevoir, développer et vérifier/soumettre à essai le logiciel selon:

- la planification de sécurité du logiciel;
- le niveau d'intégrité de sécurité du logiciel; et
- le cycle de vie de sécurité du logiciel.

f) Terminer l'activité de vérification finale du logiciel et intégrer le logiciel vérifié au matériel cible (voir 7.5 de la CEI 61508-3), développer parallèlement les aspects logiciels des procédures que les utilisateurs et l'équipe de maintenance suivent lors de l'exploitation du système (voir 7.6 de la CEI 61508-3, et A.2 k)).

g) En collaboration avec le développeur de matériel, (voir 7.7 de la CEI 61508-2), valider le logiciel dans les systèmes intégrés E/E/PE relatifs à la sécurité (voir 7.7 de la CEI 61508-3).

h) Remettre les résultats de la validation de la sécurité du logiciel aux ingénieurs système pour une intégration ultérieure dans le système global.

i) Si une modification du logiciel du système E/E/PE relatif à la sécurité est nécessaire pendant la durée de vie opérationnelle, relancer alors cette phase de la CEI 61508-3 comme indiqué (voir 7.8 de la CEI 61508-3).

Un certain nombre d'activités s'appliquent pendant tout le cycle de vie de sécurité du logiciel. Celles-ci comprennent la vérification (voir 7.9 de la CEI 61508-3) ainsi que l'évaluation de la sécurité fonctionnelle (voir l'Article 8 de la CEI 61508-3).

En appliquant les étapes susmentionnées, les techniques et mesures de sécurité du logiciel appropriées à l'intégrité de sécurité requise sont sélectionnées. Afin de faciliter cette sélection, des tableaux ont été élaborés, évaluant les différentes techniques/mesures selon les quatre niveaux d'intégrité de sécurité (voir Annexe A de la CEI 61508-3). Un aperçu de chaque technique et mesure, correspondant à ces tableaux et comprenant des références à d'autres sources d'information, est fourni (voir l'Annexe C de la CEI 61508-7).

Des exemples élaborés d'application des tableaux d'intégrité de sécurité sont donnés dans l'Annexe E; la CEI 61508-7 comprend une approche probabiliste afin de déterminer l'intégrité de sécurité pour logiciels pré-développés (voir l'Annexe D de la CEI 61508-7).

NOTE 2 Lors de l'application des étapes ci-dessus, des mesures remplaçant celles spécifiées dans la norme sont acceptables pourvu qu'elles soient justifiées lors de la planification de la sécurité (voir Article 6 de la CEI 61508-1).

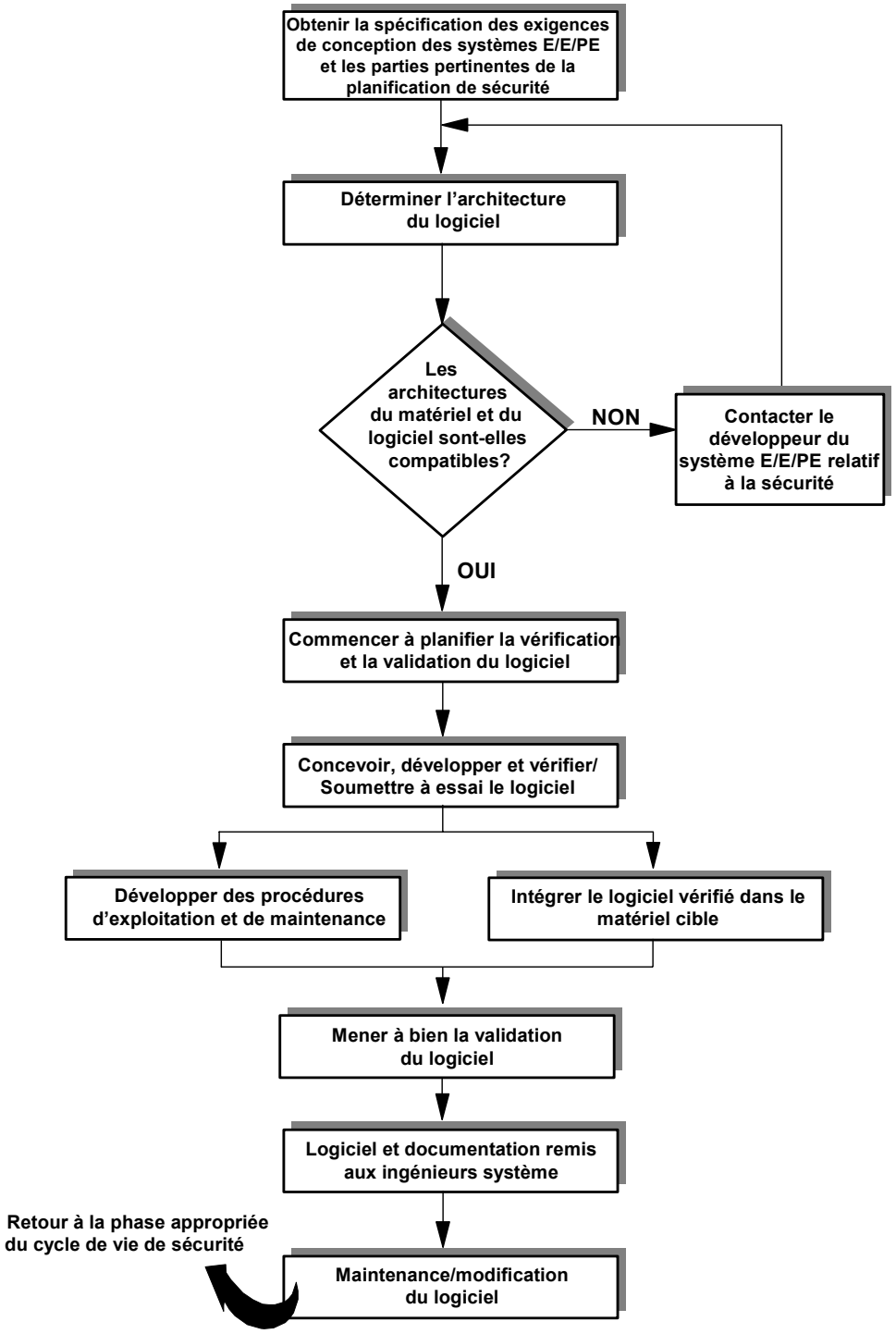


Figure A.3 – Application de la CEI 61508-3

Annexe B
(informative)

Exemple de technique permettant d'évaluer les probabilités de défaillance du matériel

B.1 Généralités

La présente annexe propose des techniques possibles de calcul des probabilités de défaillance du matériel pour les systèmes E/E/PE relatifs à la sécurité installés conformément à la CEI 61508-1, la CEI 61508-2 et la CEI 61508-3. Les informations fournies sont de nature informative et il convient de ne pas les interpréter comme la seule technique d'évaluation pouvant être utilisée. Cette annexe fournit toutefois une approche relativement simple d'évaluation de la capacité des systèmes E/E/PE relatifs à la sécurité et des lignes directrices relatives à l'utilisation de techniques de remplacement dérivées des techniques de calcul de fiabilité classiques.

NOTE 1 Les architectures systèmes indiquées dans la présente partie sont décrites au moyen d'exemples. Il convient toutefois de ne pas les considérer comme exhaustives dans la mesure où de nombreuses autres architectures peuvent être utilisées.

NOTE 2 Voir ISA-TR84.00.02-2002 [17] dans la bibliographie.

Un certain nombre de techniques de fiabilité peuvent être plus ou moins utilisées directement pour l'analyse de l'intégrité de sécurité du matériel de systèmes E/E/PE relatifs à la sécurité. De manière conventionnelle, elles sont classées selon les deux points de vue suivants:

– les modèles statiques (Booléen) par rapport aux modèles dynamiques (transitions d'état);
– les calculs analytiques par rapport à la simulation de Monte Carlo.

Les modèles booléens comprennent tous les modèles décrivant les liens logiques statiques entre les défaillances élémentaires et la défaillance du système dans son ensemble. Les diagrammes de fiabilité (RBD) (voir C.6.4 de la CEI 61508-7 et CEI 61078 [4]) et les arbres de panne (FT) (voir B.6.6.5 et B.6.6.9 de la CEI 61508-7) et la CEI 61025 [18] appartiennent aux modèles booléens.

Les modèles de transition d'état comprennent tous les modèles décrivant le comportement des systèmes (transition d'un état à l'autre) selon l'occurrence des événements (défaillances, réparations, essais, etc.). Les modèles markoviens (voir B.6.6.6 de la CEI 61508-7 et la CEI 61165 [5]), les réseaux de Pétri (voir B.2.3.3 et B.6.6.10 de la CEI 61508-7 et la CEI 62551 [19]) et les modèles en langage formel appartiennent aux modèles de transition d'état. Deux approches de Markov sont étudiées: une approche simplifiée basée sur des formules spécifiques (B.3) et une approche générale permettant de réaliser des calculs directs sur des diagrammes de Markov (B.5.2). Pour les systèmes de sécurité non markoviens, il est possible d'utiliser en lieu et place des simulations de Monte Carlo. Les ordinateurs personnels actuels permettent de réaliser ces méthodes, même pour les calculs de SIL 4. Les paragraphes B.5.3 et B.5.4 de la présente annexe donnent des lignes directrices relatives à l'application des simulations de Monte Carlo (voir B.6.6.8 de la CEI 61508-7) sur les modèles de comportement basés sur les réseaux de Pétri et la modélisation en langage formel.

L'approche simplifiée présentée en premier lieu est basée sur des représentations graphiques de diagrammes de fiabilité et des formules markoviennes spécifiques obtenues à partir des formules et hypothèses sous-jacentes relativement prudentes de Taylor, décrites en B.3.1.

Toutes ces méthodes peuvent s'appliquer à la plupart des systèmes relatifs à la sécurité. S'agissant de déterminer la technique à utiliser sur toute application particulière, il est essentiel que l'utilisateur soit compétent dans l'utilisation de la technique retenue, ce qui revêt une plus grande importance que la technique réellement appliquée. Il incombe à l'analyste de vérifier la

conformité des hypothèses sous-jacentes à toute méthode particulière ou la nécessité de toutes adaptations pour obtenir un résultat prudent et réaliste approprié. A défaut de disposer de données de fiabilité suffisamment précises ou d'une défaillance de cause commune dominante, il peut suffire d'appliquer le modèle / les techniques les plus simples. L'importance de la perte de précision ne peut être déterminée que dans des circonstances particulières.

Lorsque des programmes logiciels sont utilisés pour les calculs, l'analyste doit alors avoir une bonne connaissance des formules/techniques utilisées par le progiciel pour garantir qu'elles sont correctement utilisées pour l'application spécifique. Il convient également que l'analyste vérifie le progiciel en contrôlant son résultat avec des cas d'essai calculés manuellement.

Lorsqu'une défaillance du système de commande de l'EUC sollicite le système E/E/PE relatif à la sécurité, la probabilité d'occurrence d'un événement dangereux dépend alors également de la probabilité de défaillance du système de commande de l'EUC. Dans une telle situation, il est nécessaire de prendre en compte la possibilité de défaillances coïncidentes des composants du système de commande de l'EUC et du système E/E/PE relatif à la sécurité due à des mécanismes de défaillance de cause commune. L'existence de telles défaillances peut conduire à un risque résiduel plus élevé que prévu si les précautions appropriées ne sont pas prises.

B.2 Considérations relatives aux calculs probabilistes de base

B.2.1 Introduction

Le diagramme de fiabilité (RBD) de la Figure B.1 représente une boucle de sécurité constituée de trois capteurs (A, B, C), d'un solveur logique (D), de deux éléments finaux (E, F) et de défaillances de cause commune (CCF).

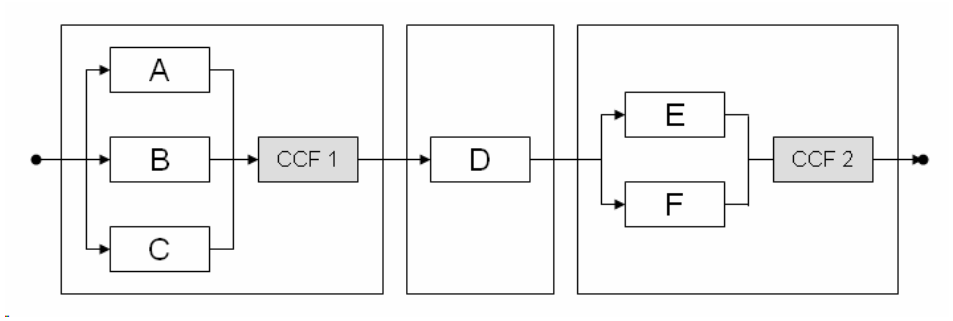


Figure B.1 – Diagramme de fiabilité d'une boucle de sécurité complète

Ceci permet d'identifier cinq combinaisons de défaillances donnant lieu à la défaillance du système E/E/PE relatif à la sécurité. Chacune d'entre elles représente une coupe d'ordre minimal:

– (A, B, C) est une défaillance triple;

– (E, F) est une défaillance double;

– (D) (CCF1) (CCF2) sont des défaillances simples.

B.2.2 Système E/E/PE relatif à la sécurité fonctionnant en mode faible sollicitation

Lorsqu'un système E/E/PE relatif à la sécurité est utilisé en mode faible sollicitation, la norme exige d'évaluer sa PFD_{avg} (c'est-à-dire son indisponibilité moyenne). Il s'agit du rapport *MDT(T)/T* où *MDT(T)* est le temps moyen d'indisponibilité sur la période [0, T] du système E/E/PE relatif à la sécurité.

Pour un système de sécurité, la probabilité de défaillance est généralement très faible et la probabilité d'occurrence simultanée de deux coupes d'ordre minimal est négligeable. Ainsi, la

somme des temps moyens d'indisponibilité dus à chaque ensemble de coupes donne une estimation prudente du temps moyen d'indisponibilité du système dans son ensemble. A partir de la Figure B.1, on obtient:

$$MDT \approx MDT^{ABC} + MDT^{D} + MDT^{EF}$$

En divisant par T, on obtient:

$$PFD_{avg} \approx PFD_{avg}^{ABC} + PFD_{avg}^{D} + PFD_{avg}^{EF}$$

Par conséquent, pour les parties en série, les calculs de PFD_{avg} sont très similaires à ceux réalisés avec des probabilités normales, lorsqu'elles sont très faibles par rapport à 1.

Cependant, pour les parties en parallèle pour lesquelles plusieurs défaillances sont nécessaires à la perte de la fonction telle que (E, F), il est évident qu'il n'est pas possible de calculer la valeur de MDT^{EF} directement à partir de MDT^{E} et de MDT^{F}: Le *MDT* (E,F) système doit être calculé comme suit

$$MDT^{EF} = \int_0^T PFD^{E}(t) PFD^{F}(t) dt$$

Par conséquent, les calculs probabilistes normaux (additions et multiplications) ne s'appliquent plus aux calculs de PFD_{avg} (intégrales) des parties en parallèle. La PFD_{avg} n'a pas les mêmes propriétés qu'une probabilité réelle et son assimilation en tant que telle est susceptible de donner lieu à des résultats non prudents. En particulier, il n'est pas possible d'obtenir la valeur de PFD_{avg} d'un système E/E/PE relatif à la sécurité en combinant simplement de manière classique la $PFD_{avg,i}$ de ses composants. Dans la mesure où les progiciels booléens du commerce incitent parfois à réaliser ce type d'opération, il convient que les analystes veillent tout particulièrement à éviter les calculs non prudents de cette nature et inappropriés en matière de sécurité.

NOTE Pour un canal redondant (1oo2) avec un taux de défaillances dangereuses non détectées λ_{DU} et un intervalle entre essais périodiques τ, un mauvais calcul de modèle de probabilité peut donner $(\lambda_{DU}.\tau)^2/4$ lorsque le résultat réel est de $(\lambda_{DU}.\tau)^2/3$.

Les calculs peuvent être réalisés de manière analytique ou en utilisant la simulation de Monte Carlo. La présente annexe décrit la réalisation de ces calculs en utilisant des modèles de fiabilité conventionnels sur base booléenne (diagramme de fiabilité ou arbres de panne) ou des modèles de transition d'état (Markov, réseaux de Pétri, etc.).

B.2.3 Système E/E/PE relatif à la sécurité fonctionnant en mode continu ou sollicitation élevée

B.2.3.1 Formule générale de *PFH*

Lorsqu'un système E/E/PE relatif à la sécurité est utilisé en mode continu ou sollicitation élevée, la norme exige de calculer sa Fréquence moyenne de défaillance dangereuse par heure (*PFH*), c'est-à-dire sa fréquence moyenne de défaillance dangereuse par unité de temps. Il s'agit de la moyenne de l'intensité de défaillance inconditionnelle (également désignée fréquence de défaillance) *w(t)* sur la période considérée:

$$PFH(T) = \frac{1}{T} \int_0^T w(t) dt$$

Lorsque le système E/E/PE relatif à la sécurité fonctionne en mode continu et constitue la dernière barrière de sécurité, la défaillance globale du système relatif à la sécurité donne alors directement lieu à une situation potentiellement dangereuse. De ce fait, pour les défaillances qui provoquent la perte de la fonction de sécurité globale, il n'est pas possible de considérer dans les calculs la réparation du système relatif à la sécurité global. Cependant, si la défaillance globale du système relatif à la sécurité ne donne pas directement lieu à un phénomène dangereux potentiel du fait d'une autre défaillance de la barrière ou de l'équipement de sécurité, il est alors possible de considérer la détection et la réparation du système relatif à la sécurité dans le calcul de réduction de risque correspondant.

B.2.3.2 Cas de non fiabilité (par exemple, barrière simple fonctionnant en mode continu)

Ce cas se produit lorsqu'un système E/E/PE relatif à la sécurité fonctionnant en mode continu constitue la dernière barrière de sécurité. Par conséquent, un phénomène dangereux potentiel peut survenir dès qu'il y a défaillance. Aucune défaillance globale du système n'est acceptable sur la période considérée.

Dans ce cas, la *PFH* peut être calculée en utilisant la non fiabilité sur la période considérée:

$$F(T):\ PFH(T) = \frac{1 - \exp\left[\int_0^T \Lambda(t)dt\right]}{T} = \frac{F(T)}{T}$$

Le taux de défaillance global du système ,$\Lambda(t)$, peut dépendre du temps ou être constant.

Lorsqu'il dépend du temps, on obtient: $PFH(T) = \frac{1 - \exp(-\Lambda_{avg}.T)}{T} \approx \Lambda_{avg}$

Lorsque le système est constitué de composants totalement et rapidement réparables, avec des taux de défaillance et de réparation constants (par exemple défaillances détectées dangereuses (DD)), $\Lambda(t)$ atteint rapidement une valeur asymptotique constante Λ_{as} et, lorsque $PFH(T) << 1.$, on obtient:

$$PFH(T) = \frac{1 - \exp(-\Lambda_{as}.T)}{T} \approx \Lambda_{as} = \frac{1}{MTTF}$$

Λ_{as} n'existe que lorsque le système E/E/PE relatif à la sécurité fonctionnant en mode continu ne comprend que des défaillances en sécurité et DD (c'est-à-dire rapidement détectées et réparées). Aucune réparation de défaillances susceptibles de provoquer directement la défaillance globale de la fonction de sécurité n'est acceptable. Pour une configuration redondante nécessitant de tenir compte d'essais périodiques, le taux de défaillance asymptotique ne s'applique pas et les équations précédentes doivent être utilisées. Il incombe à l'analyste de vérifier le cas qui s'applique.

B.2.3.3 Cas d'indisponibilité (par exemple, plusieurs barrières de sécurité)

Lorsque le système E/E/PE relatif à la sécurité fonctionnant en mode continu ne constitue pas la dernière barrière, ses défaillances n'augmentent que la fréquence de sollicitation sur les autres barrières de sécurité. C'est également le cas lorsqu'il fonctionne en mode sollicitation élevée de sorte qu'il est possible de détecter (automatiquement ou manuellement) et de réparer une anomalie susceptible de provoquer la perte directe de la fonction de sécurité pendant la période de sollicitation prévue. Dans ce cas, il est possible de réparer ses défaillances globales et de calculer *PFH* à partir de la disponibilité, *A(t),* et de l'intensité de défaillance conditionnelle, $\Lambda_V(t)$, du système.

Une fois encore, lorsque le système est constitué de composants totalement et rapidement réparables (c'est-à-dire, lorsque, dans toute situation dégradée, il existe une forte probabilité de revenir rapidement à un bon état de fonctionnement), $\Lambda_V(t)$ atteint rapidement sa valeur asymptotique, Λ_{vas}, qui constitue par ailleurs une bonne approximation du taux asymptotique réel de défaillance global du système, Λ_{as} ,introduit en B.2.3.2.

Ceci donne lieu aux approximations suivantes:

$$PFH = \frac{1}{MUT + MDT} = \frac{1}{MTBF} \approx \frac{1}{MUT} \approx \frac{1}{MTTF}$$

où

MUT est l'acronyme de Temps moyen de disponibilité;

MDT est l'acronyme de Temps moyen d'indisponibilité;

MTBF est l'acronyme de Temps moyen entre défaillances; et

MTTF est l'acronyme de Durée moyenne de fonctionnement avant défaillance.

B.2.3.4 Considérations relatives au taux de défaillance

Plusieurs des formules susmentionnées utilisent le taux de défaillance global du système $\Lambda(t)$. Son évaluation n'est pas toujours facile à réaliser et nécessite d'appliquer certains éléments de base.

Les structures en série sont très simples à traiter dans la mesure où il est possible d'ajouter les taux de défaillance. A partir de la Figure B.1, il est possible d'écrire $\Lambda(t) = \Lambda^{abc}(t) + \lambda^{CCF1}(t) + \lambda^{d}(t) + \Lambda^{ef}(t) + \lambda^{CCF2}(t)$ où $\Lambda(t)$ est le taux de défaillance global du système E/E/PE relatif à la sécurité et $\Lambda^{abc}(t)$, $\lambda^{CCF1}(t)$, $\lambda^{d}(t)$, $\Lambda^{ef}(t)$ et $\lambda^{CCF2}(t)$ sont les taux de défaillance des cinq ensembles de coupes minimales.

Cette opération est beaucoup moins simple pour les structures en parallèle dans la mesure où il n'existe pas de relation simple avec les taux de défaillance des composants individuels. Par exemple, considérons l'ensemble de coupes (E, F):

1) Lorsque E et F ne sont pas réparables (par exemple, défaillances DU), $\Lambda^{ef}(t)$ varie de manière continue de 0 à λ (taux de défaillance de E ou de F). Une valeur asymptotique est atteinte lorsque l'un des deux composants est susceptible d'être sujet à une défaillance. Il s'agit d'un processus très lent qui survient lorsque t devient plus important que $1/\lambda$. Cette valeur asymptotique n'est jamais atteinte au cours de la durée de vie réelle si E et F sont régulièrement soumis à des essais (périodiques) avec un intervalle de $\tau << 1/\lambda$.
2) Lorsque E et F sont rapidement réparables (par exemple, défaillances DD), $\Lambda^{ef}(t)$ tend très rapidement vers une valeur asymptotique $\Lambda^{ef}_{As} = 2\lambda^2/\mu$ qui peut être utilisée comme un taux de défaillance équivalent constant. Elle est atteinte lorsque t devient supérieur de l'ordre de deux ou trois fois la plus grande valeur de *MTTR* des composants. Il s'agit d'un cas particulier des systèmes totalement et rapidement réparables traités ci-dessus.

Par conséquent, s'agissant d'un cas général, l'évaluation du taux de défaillance global des systèmes implique de réaliser des calculs plus complexes que dans le cas d'une structure en série plus simple.

B.3 Approche du diagramme de fiabilité, supposant un taux de défaillance constant

B.3.1 Hypothèses sous-jacentes

Les calculs se fondent sur les hypothèses suivantes:

– la probabilité moyenne de non fonctionnement qui en résulte lors d'une sollicitation du système est inférieure à 10^{-1}; ou la fréquence moyenne de défaillance dangereuse par heure du système est inférieure à 10^{-5};

NOTE 1 Cette hypothèse signifie que le système E/E/PE relatif à la sécurité relève du domaine d'application de la série CEI 61508 et de la bande SIL 1 (voir Tableaux 2 et 3 de la CEI 61508-1).

– les taux de défaillance des composants sont constants sur toute la durée de vie du système;

– le sous-système capteur (entrée) comprend l'élément ou les éléments sensibles proprement dits et tous autres composants et câbles jusqu'au(x) composant(s) (mais non compris ce(s) composant(s)) qui combinent pour la première fois les signaux en utilisant une logique majoritaire ou un autre procédé (par exemple, pour deux canaux de capteur, la configuration serait du type illustré à la Figure B.2);

– le sous-système logique comprend le ou les composants où les signaux sont combinés pour la première fois, et tous les autres composants jusqu'à et y compris ceux où le ou les signaux de sortie sont présentés au sous-système « élément final »;

– le sous-système «élément final» (sortie) comprend tous les composants et câblages qui traitent le ou les signaux de sortie provenant du sous-système logique, y compris le ou les éléments de commande finaux;

– les taux de défaillance du matériel utilisés comme entrée pour les calculs et les tableaux sont déterminés pour un seul canal du sous-système (par exemple, si des capteurs 2oo3 sont utilisés, le taux de défaillance est déterminé pour un seul capteur et l'effet de 2oo3 est calculé séparément);

– les canaux d'un groupe à logique majoritaire ont tous les mêmes taux de défaillance et diagnostic de couverture;

– le taux de défaillance global du matériel d'un canal du sous-système est la somme du taux de défaillances dangereuses et du taux de défaillance en sécurité pour ce canal, ces deux taux étant supposés égaux;

NOTE 2 Cette hypothèse affecte la proportion de défaillance en sécurité (voir Annexe C de la CEI 61508-2), mais la proportion de défaillance en sécurité n'affecte pas les valeurs calculées pour la probabilité de défaillance donnée dans la présente annexe.

– pour chaque fonction de sécurité, il existe une procédure parfaite d'essai périodique et de réparation (c'est-à-dire que toutes les défaillances non détectées sont détectées par l'essai périodique); pour les effets d'un essai périodique imparfait, voir B.3.2.5;

– l'intervalle entre essais périodiques est supérieur à la durée moyenne de rétablissement d'un ordre de grandeur au moins;

– pour chaque sous-système, il existe un seul intervalle entre essais périodiques et une seule durée moyenne de rétablissement;

– l'intervalle escompté entre les sollicitations est supérieur d'au moins un ordre de grandeur à l'intervalle entre essais périodiques;

– pour tous les sous-systèmes utilisés en mode de fonctionnement faible sollicitation, ainsi que pour les groupes à logique majoritaire 1oo2, 1oo2D, 1oo3 et 2oo3 utilisés en mode de fonctionnement sollicitation élevée ou en mode continu, la proportion de défaillances spécifiée par la couverture de diagnostic est à la fois détectée et réparée pendant la MTTR utilisée pour déterminer les exigences d'intégrité de sécurité du matériel;

EXEMPLE Si l'on considère une MTTR de 8 h, cette période comprend l'intervalle entre essais de diagnostic qui est en général inférieur à 1 h, le temps restant constituant la durée moyenne de rétablissement.

NOTE 3 Pour les groupes à logique majoritaire 1oo2, 1oo2D, 1oo3 et 2oo3, on considère que toute réparation est effectuée en ligne. Lorsqu'un système E/E/PE relatif à la sécurité est configuré de telle sorte que pour toute

anomalie détectée, l'EUC est mis en état de sécurité, la probabilité moyenne de non fonctionnement en cas de sollicitation est améliorée. Le degré d'amélioration dépend de la couverture de diagnostic.

– pour les groupes à logique majoritaire 1oo1 et 2oo2 fonctionnant en mode sollicitation élevée ou en mode continu, le système E/E/PE relatif à la sécurité se met toujours en état de sécurité après détection d'une anomalie dangereuse; pour parvenir à ce résultat, l'intervalle escompté entre les sollicitations est au moins d'un ordre de grandeur supérieur à celui de l'intervalle entre essais de diagnostic, ou la somme de l'intervalle entre essais de diagnostic et le temps nécessaire à l'état de sécurité est inférieure au temps de mise en sécurité du processus;

NOTE 4 Pour le temps de mise en sécurité du processus, voir 3.6.20 de la CEI 61508-4.

– lorsqu'une défaillance de l'alimentation met hors tension un système E/E/PE relatif à la sécurité à déclenchement par manque d'alimentation et initie une évolution du système vers un état de sécurité, l'alimentation n'affecte pas la probabilité moyenne de non fonctionnement en cas de sollicitation du système E/E/PE relatif à la sécurité; si le système doit être alimenté pour se déclencher, ou si l'alimentation a des modes de défaillance qui peuvent entraîner un fonctionnement dangereux du système E/E/PE relatif à la sécurité, il convient de prendre en compte l'alimentation dans l'évaluation;

– lorsque le terme canal est utilisé, il se limite seulement à la partie du système prise en considération, c'est-à-dire, en général, au sous-système capteur, logique ou élément final;

– les abréviations des termes utilisés sont indiquées dans le Tableau B.1.

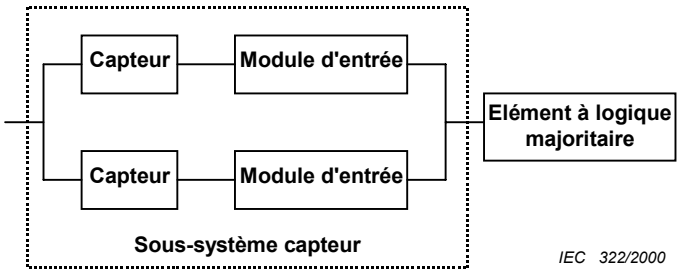


Figure B.2 – Exemple de configuration pour deux canaux de capteurs

Tableau B.1 – Termes et ordre de grandeur des paramètres correspondants utilisés dans cette annexe (s'applique à 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 et 2oo3)

Abréviation	Terme (unités)	Ordres de grandeur des paramètres dans les Tableaux B.2 à B.5 et B.10 à B.13
T_1	Intervalle de l'essai périodique (en heures)	Un mois (730 h)[1] Trois mois (2 190 h)[1] Six mois (4 380 h) Un an (8 760 h) Deux ans (17 520 h)[2] Dix ans (87 600 h)[2]
MTTR	Durée moyenne de rétablissement (en heures)	8 h NOTE MTTR = MRT = 8 heures repose sur l'hypothèse selon laquelle le temps de détection d'une défaillance dangereuse, basé sur une détection automatique, est << MRT.

Abréviation	Terme (unités)	Ordres de grandeur des paramètres dans les Tableaux B.2 à B.5 et B.10 à B.13
MRT	Temps moyen de dépannage (en heures)	8 h NOTE MTTR = MRT = 8 heures repose sur l'hypothèse selon laquelle le temps de détection d'une défaillance dangereuse, basé sur une détection automatique, est << MRT.
DC	Couverture de diagnostic (exprimée par une fraction dans les équations et par un pourcentage dans les autres cas)	0 % 60 % 90 % 99 %
β	Proportion de défaillances de cause commune non détectées (exprimée par une fraction dans les équations et par un pourcentage dans les autres cas) (dans les Tableaux B.2 à B.5 et B.10 à B.13, on suppose $\beta = 2 \times \beta_D$)	2 % 10 % 20 %
β_D	Défaillances détectées par les essais de diagnostic et ayant une cause commune (exprimées par une fraction dans les équations et par un pourcentage dans les autres cas) (dans les Tableaux B.2 à B.5 et B.10 à B.13, on suppose $\beta = 2 \times \beta_D$)	1 % 5 % 10 %
λ_{DU}	Taux de défaillance dangereuse non détectée (par heure) du canal d'un sous-système	$0{,}05 \times 10^{-6}$ $0{,}25 \times 10^{-6}$ $0{,}5 \times 10^{-6}$ $2{,}5 \times 10^{-6}$ 5×10^{-6} 25×10^{-6}
PFD_G	Probabilité moyenne de non fonctionnement en cas de sollicitation pour le groupe de canaux à logique majoritaire (si le sous-système capteur, logique ou élément final comporte seulement un groupe à logique majoritaire, alors PFD_G équivaut respectivement à PFD_S, PFD_L ou PFD_{FE})	
PFD_S	Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système capteur	
PFD_L	Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système logique	
PFD_{FE}	Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système élément final	
PFD_{SYS}	Probabilité moyenne de non fonctionnement en cas de sollicitation d'une fonction de sécurité pour le système E/E/PE relatif à la sécurité	
PFH_G	Fréquence de défaillance dangereuse moyenne par heure pour le groupe de canaux à logique majoritaire (si le sous-système capteur, logique ou élément final comprend seulement un groupe à logique majoritaire, alors PFH_G équivaut respectivement à PFH_S, PFH_L ou PFH_{FE})	
PFH_S	Fréquence de défaillance dangereuse moyenne par heure pour le sous-système capteur	
PFH_L	Fréquence de défaillance dangereuse moyenne par heure pour le sous-système logique	
PFH_{FE}	Fréquence de défaillance dangereuse moyenne par heure pour le sous-système élément final	

Abréviation	Terme (unités)	Ordres de grandeur des paramètres dans les Tableaux B.2 à B.5 et B.10 à B.13
PFH_{SYS}	Fréquence de défaillance dangereuse moyenne par heure d'une fonction de sécurité pour le système E/E/PE relatif à la sécurité	
λ	Taux de défaillance total (par heure) du canal d'un sous-système	
λ_D	Taux de défaillance dangereuse (par heure) du canal d'un sous-système, égal à 0,5 λ (suppose 50 % de défaillances dangereuses et 50 % de défaillances non dangereuses)	
λ_{DD}	Taux de défaillances dangereuses détectées (par heure) du canal d'un sous-système (somme de tous les taux de défaillances dangereuses détectées dans le canal du sous-système)	
λ_{DU}	Taux de défaillances dangereuses non détectées (par heure) du canal d'un sous-système (somme de tous les taux de défaillances dangereuses non détectées dans le canal du sous-système)	
λ_{SD}	Taux de défaillances en sécurité détectées (par heure) du canal d'un sous-système (somme de tous les taux de défaillances en sécurité détectées dans le canal du sous-système)	
t_{CE}	Temps moyen d'indisponibilité équivalent du canal (en heures) pour les architectures 1oo1, 1oo2, 2oo2 et 2oo3 (temps d'indisponibilité combiné pour tous les composants dans le canal du sous-système)	
t_{GE}	Temps moyen d'indisponibilité équivalent du groupe à logique majoritaire (en heures) pour les architectures 1oo2 et 2oo3 (temps d'indisponibilité combiné pour tous les canaux du groupe à logique majoritaire)	
t_{CE}'	Temps moyen d'indisponibilité équivalent du canal (en heures) pour l'architecture 1oo2D (temps d'indisponibilité combiné pour tous les composants du canal du sous-système)	
t_{GE}'	Temps moyen d'indisponibilité équivalent du groupe à logique majoritaire (en heures) pour l'architecture 1oo2D (temps d'indisponibilité combiné pour tous les canaux du groupe à logique majoritaire)	
T_2	Intervalle entre les sollicitations (en heures)	
K	Proportion de réussite du circuit d'autotest dans le système 1oo2D	
PTC	Couverture d'essai périodique	
1 Uniquement pour mode sollicitation élevée ou mode continu.		
2 Uniquement pour mode faible sollicitation.		

B.3.2 Probabilité moyenne de non fonctionnement en cas de sollicitation (pour mode de fonctionnement faible sollicitation)

B.3.2.1 Procédure de calcul

La probabilité moyenne de non fonctionnement en cas de sollicitation d'une fonction de sécurité du système E/E/PE relatif à la sécurité est déterminée par le calcul et la combinaison de la probabilité moyenne de non fonctionnement en cas de sollicitation pour tous les sous-systèmes assurant ensemble la fonction de sécurité. Cela peut être exprimé par la formule suivante, puisque les probabilités sont faibles dans la présente annexe (voir Figure B.3):

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

où

PFD_{SYS} est la probabilité moyenne de non fonctionnement en cas de sollicitation d'une fonction de sécurité du système E/E/PE relatif à la sécurité;

PFD_S est la probabilité moyenne de non fonctionnement en cas de sollicitation du sous-système capteur;

PFD_L est la probabilité moyenne de non fonctionnement en cas de sollicitation du sous-système logique;

PFD_{FE} est la probabilité moyenne de non fonctionnement en cas de sollicitation du sous-système élément final.

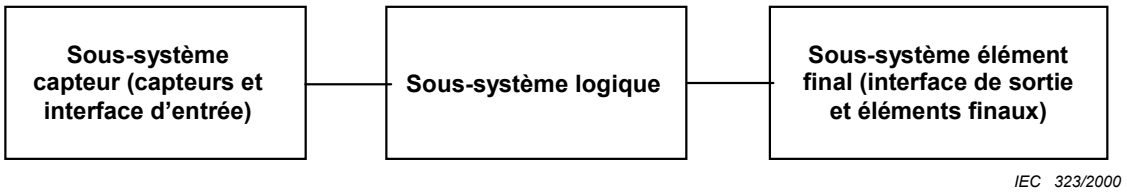


Figure B.3 – Structure du sous-système

Afin de déterminer la probabilité moyenne de non fonctionnement en cas de sollicitation de chacun des sous-systèmes, il convient que la procédure suivante soit appliquée à chacun des sous-systèmes à tour de rôle.

a) Tracer le diagramme de fiabilité en indiquant les composants du sous-système capteur (entrée), les composants du sous-système logique ou les composants du sous-système élément final (sortie). Par exemple, les composants du sous-système capteur peuvent être des capteurs, des barrières, des circuits d'adaptation d'entrées; les composants du sous-système logique peuvent être des processeurs et des dispositifs de balayage; les composants du sous-système élément final peuvent être des circuits d'adaptation de sorties, des barrières et des actionneurs. Représenter chaque sous-système par un ou plusieurs groupes à logique majoritaire 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 ou 2oo3.

b) Pour le tableau correspondant, se reporter aux Tableaux B.2 à B.5 donnés pour des intervalles entre essais périodiques de six mois, un an, deux ans et 10 ans. Ces tableaux prennent également pour hypothèse une durée moyenne de rétablissement de 8 h pour chaque défaillance à compter du moment où elle a été révélée.

c) Pour chaque groupe à logique majoritaire du sous-système, choisir à partir du tableau pertinent parmi les Tableaux B.2 à B.5:

   – l'architecture (par exemple, 2oo3);

   – la couverture de diagnostic de chaque canal (par exemple, 60 %);

   – le taux de défaillance dangereuse (par heure), λ_D, de chaque canal (par exemple 2,5 × 10^{-06});

   – les facteurs β de défaillance de cause commune, β et β_D pour l'interaction entre les canaux du groupe à logique majoritaire (par exemple, 2 % et 1 % respectivement).

NOTE 1 On suppose que chaque canal du groupe à logique majoritaire a la même couverture de diagnostic et le même taux de défaillances (voir B.1).

NOTE 2 On suppose dans les Tableaux B.2 à B.5 (et dans les Tableaux B.10 à B.13) que le facteur β, en l'absence d'essais de diagnostic (utilisé également pour les défaillances dangereuses non détectées en présence d'essais de diagnostic), β, est égal à deux fois le facteur β pour les défaillances détectées par les essais de diagnostic, β_D.

d) Obtenir, à partir du tableau approprié parmi les Tableaux B.2 à B.5, la probabilité moyenne de non fonctionnement en cas de sollicitation pour le groupe à logique majoritaire.

e) Si la fonction de sécurité dépend de plus d'un groupe de capteurs ou d'actionneurs à logique majoritaire, la probabilité moyenne combinée de non fonctionnement en cas de sollicitation du sous-système capteur ou élément final, PFD_S ou PFD_{FE} est donnée dans les équations suivantes, où PFD_{Gi} et PFD_{Gj} est la probabilité moyenne de non fonctionnement en cas de sollicitation de chaque groupe de capteurs à logique majoritaire et d'éléments finaux, respectivement:

$$PFD_S = \sum_i PFD_{Gi}$$

$$PFD_{FE} = \sum_i PFD_{Gj}$$

Les formules utilisées dans toutes les équations applicables à la *PFD* et au taux de défaillance du système sont toutes fonction du taux de défaillance du composant et du temps moyen d'indisponibilité (*MDT*). Lorsque le système est constitué d'un certain nombre d'éléments et qu'il est nécessaire de calculer la *PFD* globale des éléments combinés ou le taux de défaillance du système, il est le plus souvent nécessaire d'utiliser dans les équations une seule valeur du *MDT*. Cependant, chaque élément peut disposer de différents mécanismes de détection de défaillance avec différents *MDT* et différents éléments peuvent présenter différentes valeurs du *MDT* pour les mêmes mécanismes de défaillance, auquel cas, il est nécessaire de calculer une seule valeur du *MDT* susceptible de représenter tous les éléments dans le chemin. Ceci peut être réalisé en tenant compte du taux de défaillance global des chemins totaux, puis en rapportant l'équivalent du *MDT* individuel proportionnellement à leur contribution de taux de défaillance au taux de défaillance total considéré.

Par exemple, si deux éléments sont en série dont l'un est soumis à un essai périodique, T_1, et l'autre à un essai périodique, T_2, la valeur simple équivalente du *MDT* est alors de:

$$\lambda_T = \lambda_1 + \lambda_2$$

et

$$MDT_E = \frac{\lambda_1}{\lambda_T}\left(\frac{T_1}{2}\right) + \frac{\lambda_2}{\lambda_T}\left(\frac{T_2}{2}\right)$$

B.3.2.2 Architectures pour le mode de fonctionnement faible sollicitation

NOTE 1 Il convient de considérer ce paragraphe de manière séquentielle, en tenant compte du fait que les équations valides pour plusieurs architectures ne sont citées que lors de leur première utilisation.

NOTE 2 Les équations sont basées sur les hypothèses énumérées en B.3.1.

NOTE 3 Les exemples suivants représentent des configurations typiques qui ne sont pas destinées à être exhaustives.

B.3.2.2.1 1oo1

Cette architecture comprend un seul canal où toute défaillance dangereuse donne lieu à une défaillance de la fonction de sécurité en cas de sollicitation.

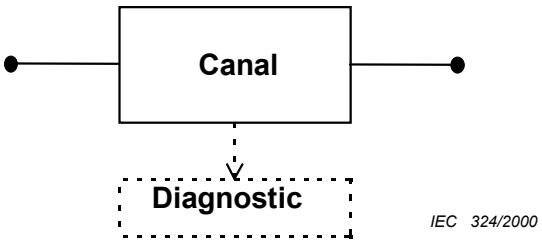


Figure B.4 – Diagramme du bloc physique 1oo1

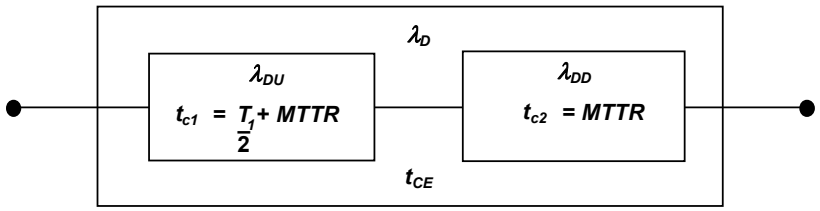


Figure B.5 – Diagramme de fiabilité 1oo1

Les Figures B.4 et B.5 comprennent les diagrammes de blocs pertinents. Le taux de défaillance dangereuse pour le canal est donné par

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

La Figure B.5 montre que l'on peut considérer que le canal a deux composants, l'un ayant un taux de défaillance dangereuse λ_{DU} résultant des défaillances non détectées et l'autre un taux de défaillance dangereuse λ_{DD} résultant des défaillances détectées. Il est possible de calculer un temps d'indisponibilité moyen équivalent s'appliquant au canal, t_{CE}, en additionnant les temps d'indisponibilité individuels des deux composants, t_{c1} et t_{c2} proportionnellement à la contribution de chaque composant individuel à la probabilité de défaillance du canal:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Pour chaque architecture, le taux de défaillances dangereuses détectées et le taux de défaillances dangereuses non détectées sont donnés par la formule

$$\lambda_{DU} = \lambda_D(1 - DC)\text{;} \quad \lambda_{DD} = \lambda_D DC$$

Pour un canal dont le temps d'indisponibilité t_{CE} résultant des défaillances dangereuses

$$PFD = 1 - e^{-\lambda_D t_{CE}}$$
$$\approx \lambda_D t_{CE} \qquad \text{puisque } \lambda_D t_{CE} << 1$$

Ainsi, pour une architecture 1oo1, la probabilité moyenne de non fonctionnement en cas de sollicitation est

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

B.3.2.2.2 1oo2

Cette architecture comprend deux canaux connectés en parallèle de sorte que chacun peut traiter la fonction de sécurité. Ainsi, il faudrait qu'il y ait une défaillance dangereuse dans les deux canaux pour qu'une fonction de sécurité ne fonctionne pas correctement en cas de sollicitation. On suppose que tout essai de diagnostic ne révélerait que les anomalies découvertes et ne modifierait pas les états de sortie ou la logique majoritaire des sorties.

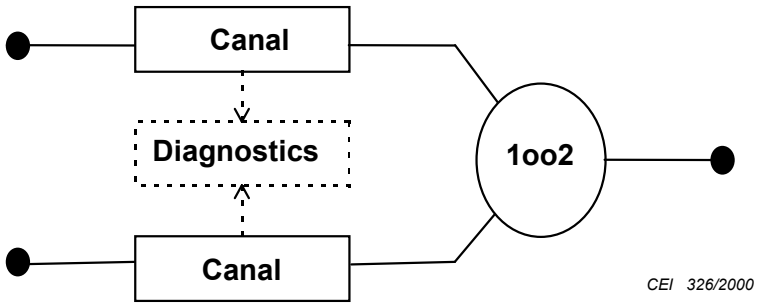


Figure B.6 – Diagramme du bloc physique 1oo2

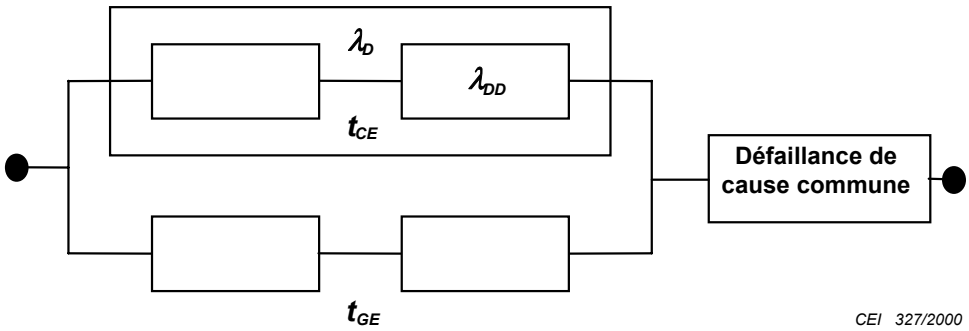


Figure B.7 – Diagramme de fiabilité 1oo2

Les Figures B.6 et B.7 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est donnée en B.3.2.2.1, et il est à présent nécessaire de calculer également le temps d'indisponibilité équivalent du système t_{GE} qui est donné par la formule

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

La probabilité moyenne de non fonctionnement en cas de sollicitation de l'architecture est

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

B.3.2.2.3 2oo2

Cette architecture comporte deux canaux connectés en parallèle de sorte qu'il est nécessaire que les deux canaux sollicitent la fonction de sécurité avant que celle-ci ne survienne. On suppose que tout essai de diagnostic n'indiquerait que les anomalies découvertes et ne modifierait pas les états de sortie ou la logique majoritaire de sortie.

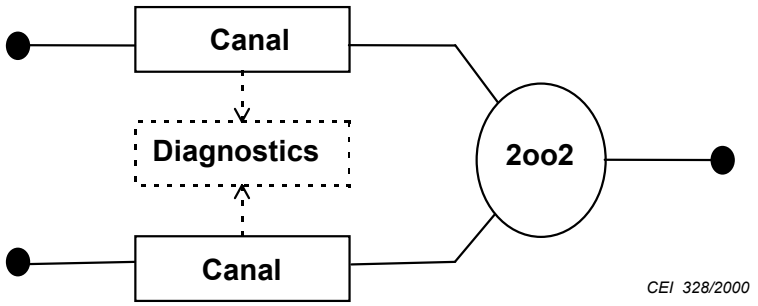


Figure B.8 – Diagramme du bloc physique 2oo2

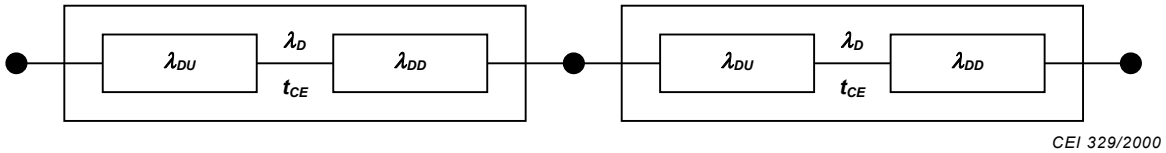


Figure B.9 – Diagramme de fiabilité 2oo2

Les Figures B.8 et B.9 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est donnée en B.3.2.2.1; la probabilité moyenne de non fonctionnement en cas de sollicitation pour l'architecture est

$$PFD_G = 2\lambda_D t_{CE}$$

B.3.2.2.4 1oo2D

Cette architecture comprend deux canaux connectés en parallèle. Dans des conditions normales d'utilisation, les deux canaux doivent solliciter la fonction de sécurité pour qu'elle agisse. De plus, si les essais de diagnostic détectent une anomalie dans l'un des canaux, alors la logique majoritaire de sortie s'adapte de sorte que l'état de la sortie générale suive alors celui de l'autre canal. Si les essais de diagnostic décèlent des anomalies dans les deux canaux ou une divergence qui ne peut être attribuée à l'un des canaux, la sortie se met alors en état de sécurité. Pour détecter une divergence entre les canaux, chaque canal peut déterminer l'état de l'autre canal par un moyen indépendant de l'autre canal. Le mécanisme de comparaison / commutation de canal peut ne pas se révéler efficace à 100 %, par conséquent K représente l'efficacité du mécanisme de comparaison / commutation entre canaux, c'est-à-dire que la sortie peut rester en vote majoritaire 2oo2 même lorsqu'un canal est détecté en défaillance.

NOTE Le paramètre K doit être déterminé par une AMDE (analyse des modes de défaillance et de leurs effets).

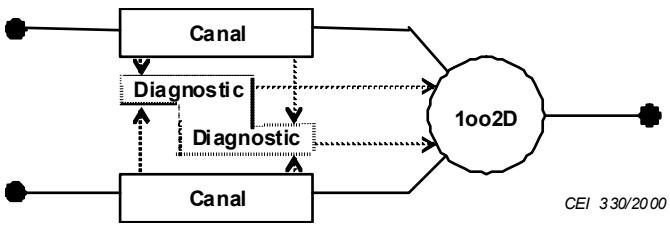


Figure B.10 – Diagramme du bloc physique 1oo2D

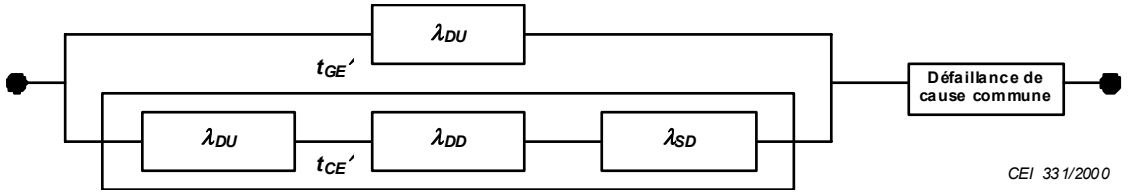


Figure B.11 – Diagramme de fiabilité 1oo2D

Le taux de défaillances en sécurité détectées pour chaque canal est donné par

$$\lambda_{SD} = \lambda_S DC$$

Les Figures B.10 et B.11 montrent les diagrammes de blocs pertinents. Les valeurs des temps moyens d'indisponibilité diffèrent de celles données pour les autres architectures en B.3.2.2 et sont pour cela désignées t_{CE}' et t_{GE}'. Leurs valeurs sont données par la formule

$$t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + (\lambda_{DD} + \lambda_{SD})}$$

$$t_{GE}' = \frac{T_1}{3} + MRT$$

La probabilité moyenne de non fonctionnement en cas de sollicitation pour l'architecture est donnée par la formule

$$PFD_G = 2(1-\beta)\lambda_{DU}\left((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\right)t_{CE}'\,t_{GE}' + 2(1-K)\lambda_{DD}t_{CE}' + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

B.3.2.2.5 2oo3

Cette architecture comprend trois canaux connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie, de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul canal donne un résultat différent des deux autres canaux.

On suppose que tout essai de diagnostic n'indiquerait que les anomalies décelées et ne modifierait ni les états de sortie, ni la logique majoritaire.

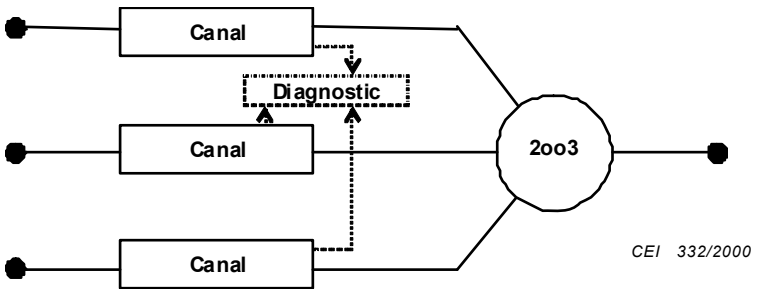


Figure B.12 – Diagramme du bloc physique 2oo3

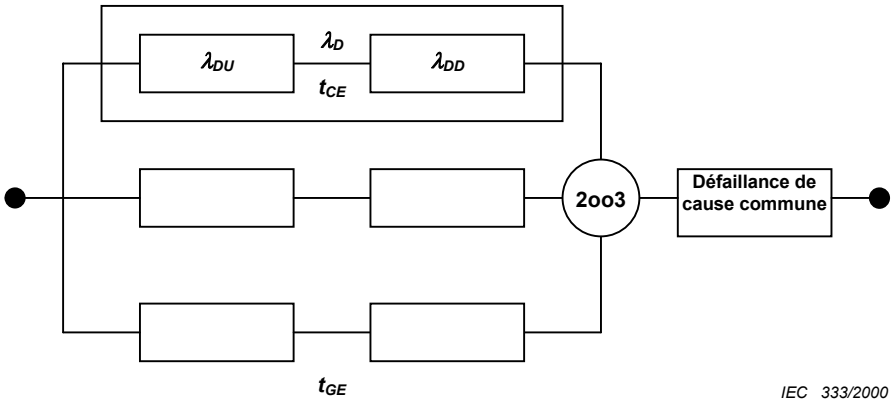


Figure B.13 – Diagramme de fiabilité 2oo3

Les Figures B.12 et B.13 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est celle donnée au B.3.2.2.1 et la valeur de t_{GE} est celle donnée au B.3.2.2.2. La probabilité moyenne de non fonctionnement en cas de sollicitation pour l'architecture est

$$PFD_G = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

B.3.2.2.6 1oo3

Cette architecture comprend trois canaux connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie, de telle sorte que l'état de sortie suit la logique majoritaire 1oo3.

On suppose que tout essai de diagnostic n'indiquerait que les anomalies décelées et ne modifierait ni les états de sortie, ni la logique majoritaire.

Le diagramme de fiabilité est le même que pour le cas de 2oo3 mais avec la logique de vote majoritaire 1oo3. La valeur de t_{CE} est donnée au B.3.2.2.1 et la valeur de t_{GE} est donnée au B.3.2.2.2. La probabilité moyenne de non fonctionnement en cas de sollicitation pour l'architecture est

$$PFD_G = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

CEI 332/2000

où

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

B.3.2.3 Tableaux détaillés pour le mode de fonctionnement faible sollicitation

Tableau B.2 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de six mois et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	1,1E-04			5,5E-04			1,1E-03		
	60 %	4,4E-05			2,2E-04			4,4E-04		
	90 %	1,1E-05			5,7E-05			1,1E-04		
	99 %	1,5E-06			7,5E-06			1,5E-05		
1oo2	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo2 (voir la Note 2)	**0 %**	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,3E-05			1,1E-04			2,3E-04		
	99 %	3,0E-06			1,5E-05			3,0E-05		
1oo2D (voir la Note 3)	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	1,4E-06	4,9E-06	9,3E-06	7,1E-06	2,5E-05	4,7E-05	1,4E-05	5,0E-05	9,3E-05
	90 %	4,3E-07	1,3E-06	2,4E-06	2,2E-06	6,6E-06	1,2E-05	4,3E-06	1,3E-05	2,4E-05
	99 %	6,0E-08	1,5E-07	2,6E-07	3,0E-07	7,4E-07	1,3E-06	6,0E-07	1,5E-06	2,6E-06
2oo3	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,6E-05	1,1E-04	2,7E-05	1,1E-04	2,2E-04
	60 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo3	**0 %**	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06

Architecture	*DC*	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	5,5E-03			1,1E-02			5,5E-02		
	60 %	2,2E-03			4,4E-03			2,2E-02		
	90 %	5,7E-04			1,1E-03			5,7E-03		
	99 %	7,5E-05			1,5E-04			7,5E-04		
1oo2	**0 %**	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	90 %	1,2E-05	5,6E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04	1,5E-04	6,0E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,4E-05	6,6E-05	1,3E-04
2oo2 (voir la Note 2)	**0 %**	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,3E-03			1,1E-02		
	99 %	1,5E-04			3,0E-04			1,5E-03		
1oo2D (voir la Note 3)	**0 %**	1,5E-04	5,8E-04	1,1E-03	3,8E-04	1,2E-03	2,3E-03	5,0E-03	9,0E-03	1,4E-02
	60 %	7,7E-05	2,5E-04	4,7E-04	1,7E-04	5,2E-04	9,5E-04	1,3E-03	3,0E-03	5,1E-03
	90 %	2,2E-05	6,6E-05	1,2E-04	4,5E-05	1,3E-04	2,4E-04	2,6E-04	6,9E-04	1,2E-03
	99 %	3,0E-06	7,4E-06	1,3E-05	6,0E-06	1,5E-05	2,6E-05	3,0E-05	7,4E-05	1,3E-04
2oo3	**0 %**	2,3E-04	6,5E-04	1,2E-03	6,8E-04	1,5E-03	2,5E-03	1,3E-02	1,5E-02	1,9E-02
	60 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,3E-03	3,9E-03	5,9E-03
	90 %	1,2E-05	5,7E-05	1,1E-04	2,7E-05	1,2E-04	2,3E-04	2,4E-04	6,8E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,7E-06	1,3E-05	2,6E-05	1,5E-05	6,7E-05	1,3E-04
1oo3	**0 %**	1,1E-04	5,5E-04	1,1E-03	2,2E-04	1,1E-03	2,2E-03	1,4E-03	5,7E-03	1,1E-02
	60 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	90 %	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFD_G est équivalent respectivement à PFD_S, PFD_L ou PFD_{FE} (voir B.3.2.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la probabilité moyenne de défaillance.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

Tableau B.3 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de un an et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,2E-05			1,1E-04			2,2E-04		
	99 %	2,6E-06			1,3E-05			2,6E-05		
1oo2	**0 %**	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,0E-06	4,4E-05	8,8E-05	1,9E-05	8,9E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
2oo2 (voir la Note 2)	**0 %**	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,5E-05			2,2E-04			4,5E-04		
	99 %	5,2E-06			2,6E-05			5,2E-05		
1oo2D (voir la Note 3)	**0 %**	4,5E-06	2,2E-05	4,4E-05	2,4E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	2,8E-06	9,8E-06	1,9E-05	1,4E-05	4,9E-05	9,3E-05	2,9E-05	9,9E-05	1,9E-04
	90 %	8,5E-07	2,6E-06	4,8E-06	4,3E-06	1,3E-05	2,4E-05	8,5E-06	2,6E-05	4,8E-05
	99 %	1,0E-07	2,8E-07	5,0E-07	5,2E-07	1,4E-06	2,5E-06	1,0E-06	2,8E-06	5,0E-06
2oo3	**0 %**	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,2E-05	2,4E-04	4,5E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,5E-06	4,5E-05	8,8E-05	2,1E-05	9,1E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo3	**0 %**	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	8,8E-06	4,4E-05	8,8E-05	1,8E-05	8,8E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06

Architecture	*DC*	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,2E-03			1,1E-02		
	99 %	1,3E-04			2,6E-04			1,3E-03		
1oo2	**0 %**	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60 %	1,1E-04	4,6E-04	9,0E-04	2,8E-04	9,7E-04	1,8E-03	3,4E-03	6,6E-03	1,1E-02
	90 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,9E-06	2,4E-05	4,8E-05	2,6E-05	1,2E-04	2,4E-04
2oo2 (voir la Note 2)	**0 %**	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,5E-03			2,2E-02		
	99 %	2,6E-04			5,2E-04			2,6E-03		
1oo2D (voir la Note 3)	**0 %**	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,9E-03	1,8E-02	2,5E-02	3,4E-02
	60 %	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03	3,9E-03	7,1E-03	1,1E-02
	90 %	4,4E-05	1,3E-04	2,4E-04	9,1E-05	2,7E-04	4,8E-04	5,8E-04	1,4E-03	2,5E-03
	99 %	5,2E-06	1,4E-05	2,5E-05	1,0E-05	2,8E-05	5,0E-05	5,4E-05	1,4E-04	2,5E-04
2oo3	**0 %**	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,8E-03	5,6E-03	4,8E-02	5,0E-02	5,3E-02
	60 %	1,6E-04	5,1E-04	9,4E-04	4,8E-04	1,1E-03	2,0E-03	8,4E-03	1,1E-02	1,5E-02
	90 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
	99 %	2,5E-06	1,2E-05	2,4E-05	5,1E-06	2,4E-05	4,8E-05	3,1E-05	1,3E-04	2,5E-04

Architecture	*DC*	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo3	**0 %**	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,7E-03	1,3E-02	2,3E-02
	60 %	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03	1,0E-03	4,5E-03	8,9E-03
	90 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,8E-06	2,4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFD_G est équivalent respectivement à PFD_S, PFD_L ou PFD_{FE} (voir B.3.2.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la probabilité moyenne de défaillance.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

Tableau B.4 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de deux ans et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1	**0 %**	4,4E-04			2,2E-03			4,4E-03		
(voir la Note 2)	**60 %**	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,4E-05			2,2E-04			4,4E-04		
	99 %	4,8E-06			2,4E-05			4,8E-05		
1oo2	**0 %**	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,9E-05	8,9E-05	1,8E-04	3,9E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
2oo2	**0 %**	8,8E-04			4,4E-03			8,8E-03		
(voir la Note 2)	**60 %**	3,5E-04			1,8E-03			3,5E-03		
	90 %	8,8E-05			4,4E-04			8,8E-04		
	99 %	9,6E-06			4,8E-05			9,6E-05		
1oo2D	**0 %**	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	9,0E-04
(voir la Note 3)	**60 %**	5,7E-06	2,0E-05	3,7E-05	2,9E-05	9,9E-05	1,9E-04	6,0E-05	2,0E-04	3,7E-04
	90 %	1,7E-06	5,2E-06	9,6E-06	8,5E-06	2,6E-05	4,8E-05	1,7E-05	5,2E-05	9,6E-05
	99 %	1,9E-07	5,4E-07	9,8E-07	9,5E-07	2,7E-06	4,9E-06	1,9E-06	5,4E-06	9,8E-06
2oo3	**0 %**	9,5E-06	4,4E-05	8,8E-05	6,2E-05	2,3E-04	4,5E-04	1,6E-04	5,0E-04	9,3E-04
	60 %	3,6E-06	1,8E-05	3,5E-05	2,1E-05	9,0E-05	1,8E-04	4,7E-05	1,9E-04	3,6E-04
	90 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,3E-07	4,6E-06	9,2E-06
1oo3	**0 %**	8,8E-06	4,4E-05	8,8E-05	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,8E-05	8,8E-05	1,8E-04	3,5E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,4E-03			2,2E-02		
	99 %	2,4E-04			4,8E-04			2,4E-03		
1oo2	**0 %**	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60 %	2,8E-04	9,7E-04	1,8E-03	7,5E-04	2,1E-03	3,8E-03	1,2E-02	1,8E-02	2,5E-02
	90 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	99 %	4,7E-06	2,3E-05	4,6E-05	9,5E-06	4,6E-05	9,2E-05	5,4E-05	2,4E-04	4,6E-04
2oo2 (voir la Note 2)	**0 %**	4,4E-02			8,8E-02			>1E-01		
	60 %	1,8E-02			3,5E-02			>1E-01		
	90 %	4,4E-03			8,8E-03			4,4E-02		
	99 %	4,8E-04			9,6E-04			4,8E-03		
1oo2D (voir la Note 3)	**0 %**	1,1E-03	2,7E-03	4,8E-03	3,4E-03	6,6E-03	1,1E-02	6,7E-02	7,7E-02	9,0E-02
	60 %	3,8E-04	1,1E-03	1,9E-03	9,6E-04	2,3E-03	4,0E-03	1,3E-02	1,9E-02	2,6E-02
	90 %	9,0E-05	2,6E-04	4,8E-04	1,9E-04	5,4E-04	9,8E-04	1,5E-03	3,2E-03	5,3E-03
	99 %	9,6E-06	2,7E-05	4,9E-05	1,9E-05	5,4E-05	9,8E-05	1,0E-04	2,8E-04	5,0E-04
2oo3	**0 %**	2,3E-03	3,7E-03	5,6E-03	8,3E-03	1,1E-02	1,4E-02	1,9E-01	1,8E-01	1,7E-01
	60 %	4,8E-04	1,1E-03	2,0E-03	1,6E-03	2,8E-03	4,4E-03	3,2E-02	3,5E-02	4,0E-02
	90 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,4E-03	4,0E-03	6,0E-03
	99 %	4,8E-06	2,3E-05	4,6E-05	1,0E-05	4,7E-05	9,2E-05	6,9E-05	2,5E-04	4,8E-04
1oo3	**0 %**	4,6E-04	2,2E-03	4,4E-03	1,0E-03	4,5E-03	8,9E-03	2,4E-02	3,7E-02	5,5E-02
	60 %	1,8E-04	8,8E-04	1,8E-03	3,6E-04	1,8E-03	3,5E-03	3,1E-03	9,9E-03	1,8E-02
	90 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	99 %	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFD_G est équivalent respectivement à PFD_S, PFD_L ou PFD_{FE} (voir B.3.2.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la probabilité moyenne de défaillance.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

Tableau B.5 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de dix ans et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	2,2E-03			1,1E-02			2,2E-02		
	60 %	8,8E-04			4,4E-03			8,8E-03		
	90 %	2,2E-04			1,1E-03			2,2E-03		
	99 %	2,2E-05			1,1E-04			2,2E-04		
1oo2	**0 %**	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	1,9E-05	8,9E-05	1,8E-04	1,1E-04	4,6E-04	9,0E-04	2,7E-04	9,6E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
2oo2 (voir la Note 2)	**0 %**	4,4E-03			2,2E-02			4,4E-02		
	60 %	1,8E-03			8,8E-03			1,8E-02		
	90 %	4,4E-04			2,2E-03			4,4E-03		
	99 %	4,5E-05			2,2E-04			4,5E-04		
1oo2D (voir la Note 3)	**0 %**	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	2,9E-05	9,9E-05	1,9E-04	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03
	90 %	8,4E-06	2,6E-05	4,8E-05	4,3E-05	1,3E-04	2,4E-04	9,0E-05	2,6E-04	4,8E-04
	99 %	8,9E-07	2,6E-06	4,8E-06	4,5E-06	1,3E-05	2,4E-05	8,9E-06	2,6E-05	4,8E-05
2oo3	**0 %**	6,2E-05	2,3E-04	4,5E-04	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,7E-03	5,6E-03
	60 %	2,1E-05	9,0E-05	1,8E-04	1,6E-04	5,0E-04	9,3E-04	4,7E-04	1,1E-03	2,0E-03
	90 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,3E-05	2,4E-04	4,5E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
1oo3	**0 %**	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03
	60 %	1,8E-05	8,8E-05	1,8E-04	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05

Architecture	*DC*	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	>1E-01			>1E-01			>1E-01		
	60 %	4,4E-02			8,8E-02			>1E-01		
	90 %	1,1E-02			2,2E-02			>1E-01		
	99 %	1,1E-03			2,2E-03			1,1E-02		
1oo2	**0 %**	1,8E-02	2,4E-02	3,2E-02	6,6E-02	7,4E-02	8,5E-02	>1E-01	>1E-01	>1E-01
	60 %	3,4E-03	6,6E-03	1,1E-02	1,2E-02	1,8E-02	2,5E-02	>1E-01	>1E-01	>1E-01
	90 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,8E-03	4,9E-03	1,8E-02	2,5E-02	3,5E-02
	99 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
2oo2 (voir la Note 2)	**0 %**	>1E-01			>1E-01			>1E-01		
	60 %	8,8E-02			>1E-01			>1E-01		
	90 %	2,2E-02			4,4E-02			>1E-01		
	99 %	2,2E-03			4,5E-03			2,2E-02		
1oo2D (voir la Note 3)	**0 %**	1,8E-02	2,5E-02	3,3E-02	6,6E-02	7,7E-02	9,0E-02	1,6E+00	1,5E+00	1,4E+00
	60 %	3,9E-03	7,1E-03	1,1E-02	1,3E-02	1,9E-02	2,6E-02	2,6E-01	2,7E-01	2,8E-01
	90 %	5,7E-04	1,4E-03	2,5E-03	1,5E-03	3,1E-03	5,2E-03	2,0E-02	2,7E-02	3,5E-02
	99 %	4,6E-05	1,3E-04	2,4E-04	9,5E-05	2,7E-04	4,9E-04	6,0E-04	1,5E-03	2,5E-03
2oo3	**0 %**	4,8E-02	5,0E-02	5,3E-02	1,9E-01	1,8E-01	1,7E-01	4,6E+00	4,0E+00	3,3E+00
	60 %	8,3E-03	1,1E-02	1,4E-02	3,2E-02	3,5E-02	4,0E-02	7,6E-01	7,1E-01	6,6E-01
	90 %	6,9E-04	1,5E-03	2,6E-03	2,3E-03	3,9E-03	5,9E-03	4,9E-02	5,4E-02	6,0E-02
	99 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03

Architecture	*DC*	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo3	0 %	4,7E-03	1,3E-02	2,3E-02	2,4E-02	3,7E-02	5,5E-02	2,5E+00	2,0E+00	1,6E+00
	60 %	1,0E-03	4,5E-03	8,9E-03	3,0E-03	9,8E-03	1,8E-02	1,7E-01	1,8E-01	1,9E-01
	90 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,8E-03	1,3E-02	2,4E-02
	99 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFD_G est équivalent respectivement à PFD_S, PFD_L ou PFD_{FE} (voir B.3.2.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la probabilité moyenne de défaillance.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

B.3.2.4 Exemple pour un mode de fonctionnement faible sollicitation

Soit une fonction de sécurité nécessitant un système de niveau SIL 2. Supposons que l'évaluation initiale de l'architecture du système, fondée sur une pratique antérieure, tienne compte d'un groupe de trois capteurs de pression analogiques, à logique majoritaire 2oo3. Le sous-système logique est un PES redondant configuré 1oo2D pilotant une soupape d'arrêt ainsi qu'une seule soupape de mise à l'air libre. La soupape d'arrêt et la soupape de mise à l'air libre doivent fonctionner de telle sorte que la fonction de sécurité s'accomplisse. L'architecture est illustrée à la Figure B.14. Pour l'évaluation initiale, on suppose une période d'essai périodique d'un an.

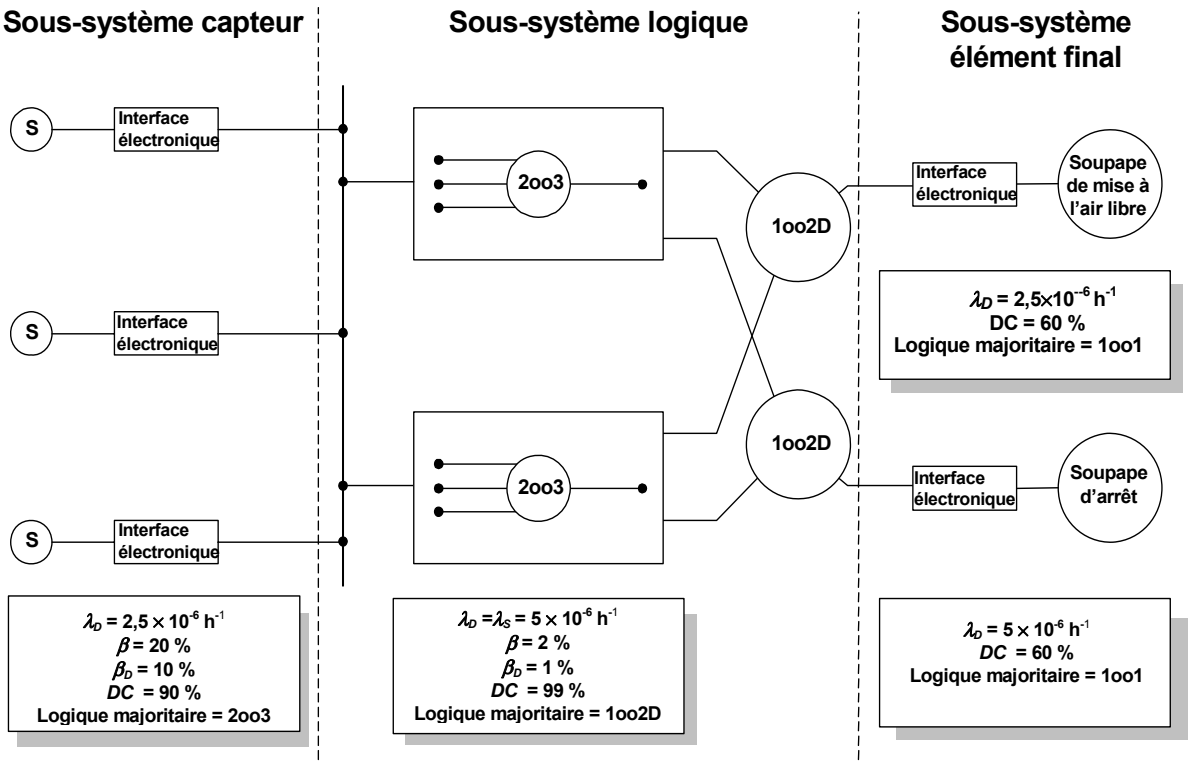


Figure B.14 – Architecture d'un exemple de fonctionnement en mode faible sollicitation

Tableau B.6 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système capteur dans l'exemple de fonctionnement en mode faible sollicitation (intervalle entre essais périodiques d'un an et *MTTR* de 8 h)

Architecture	*DC*	λ_D = 2,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0 %	6,8E-04	1,5E-03	2,5E-03
	60 %	1,6E-04	5,1E-04	9,4E-04
	90 %	2,7E-05	1,2E-04	2,3E-04
	99 %	2,5E-06	1,2E-05	2,4E-05
NOTE Ce tableau est extrait du Tableau B.3.				

Tableau B.7 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système logique de l'exemple de fonctionnement en mode faible sollicitation (intervalle entre essais périodiques d'un an et *MTTR* de 8 h)

Architecture	*DC*	λ_D = 0,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2D	0 %	1,1E-03	2,7E-03	4,8E-03
	60 %	2,0E-04	9,0E-04	1,8E-03
	90 %	4,5E-05	2,2E-04	4,4E-04
	99 %	4,8E-06	2,4E-05	4,8E-05
NOTE Ce tableau est extrait du Tableau B.3.				

Tableau B.8 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système élément final de l'exemple de fonctionnement en mode faible sollicitation (intervalle entre essais périodiques d'un an et durée *MTTR* de 8 h)

Architecture	*DC*	λ_D = 2,5E-06	λ_D = 0,5E-05
1oo1	0 %	1,1E-02	2,2E-02
	60 %	4,4E-03	8,8E-03
	90 %	1,1E-03	2,2E-03
	99 %	1,3E-04	2,6E-04
NOTE Ce tableau est extrait du Tableau B.3.			

Les valeurs suivantes sont déduites des Tableaux B.6 à B.8.

Pour le sous-système capteur,

$$PFD_S = 2{,}3 \times 10^{-4}$$

Pour le sous-système logique,

$$PFD_L = 4{,}8 \times 10^{-6}$$

Pour le sous-système élément final,

$$PFD_{FE} = 4{,}4 \times 10^{-3} + 8{,}8 \times 10^{-3}$$

$$= 1{,}3 \times 10^{-2}$$

Ainsi, pour la fonction de sécurité,

PFD_{SYS} = $2{,}3 \times 10^{-4} + 4{,}8 \times 10^{-6} + 1{,}3 \times 10^{-2}$

= $1{,}3 \times 10^{-2}$

≡ **niveau 1 d'intégrité de sécurité**

Pour améliorer le système de manière à satisfaire au niveau 2 d'intégrité de sécurité, l'une des opérations suivantes peut être effectuée:

a) modifier l'intervalle entre essais périodiques à six mois

PFD_S = $1{,}1 \times 10^{-4}$

PFD_L = $2{,}6 \times 10^{-6}$

PFD_{FE} = $2{,}2 \times 10^{-3} + 4{,}4 \times 10^{-3}$

= $6{,}6 \times 10^{-3}$

PFD_{SYS} = $6{,}7 \times 10^{-3}$

≡ **niveau 2 d'intégrité de sécurité**

b) remplacer la soupape d'arrêt 1oo1 (qui est le dispositif de sortie ayant la plus faible fiabilité) par la soupape 1oo2 (en prenant pour hypothèse que β = 10 % et β_D = 5 %)

PFD_S = $2{,}3 \times 10^{-4}$

PFD_L = $4{,}8 \times 10^{-6}$

PFD_{FE} = $4{,}4 \times 10^{-3} + 9{,}7 \times 10^{-4}$

= $5{,}4 \times 10^{-3}$

PFD_{SYS} = $5{,}6 \times 10^{-3}$

≡ **niveau 2 d'intégrité de sécurité**

B.3.2.5 Effets d'un essai périodique imparfait

Les anomalies dans le système de sécurité qui ne sont détectées ni par des essais de diagnostic ni par des essais périodiques peuvent être détectées par d'autres événements tels qu'un incident nécessitant l'exécution de la fonction de sécurité, ou au cours de la révision de l'équipement. Si les anomalies ne sont pas détectées au moyen de ces méthodes, il convient de supposer qu'elles demeureront pendant toute la durée de vie de l'équipement. Soit une période d'essai périodique T_1 avec une couverture d'essai périodique (PTC) et les anomalies détectées par les autres moyens (1-PTC), avec le temps prévu entre les sollicitations de T_2 sur le système de sécurité. Ces deux temps régissent le temps d'indisponibilité effectif.

Un exemple est donné ci-dessous pour une architecture 1oo2. T_2 est le temps entre les sollicitations sur le système:

$$t_{CE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(PTC)\left(\frac{T_1}{2} + MRT\right) +$$

$$\beta\lambda_{DU}(1-PTC)\left(\frac{T_2}{2} + MRT\right)$$

Le Tableau B.9 ci-dessous donne les résultats numériques d'un système 1oo2 avec un essai périodique de 100 % sur un an (T_1 = 1 an) comparé à un essai périodique de 90 % où la période de sollicitation T_2 est supposée être de 10 ans. Cet exemple a été calculé en prenant pour hypothèse un taux de défaillance de $0,5 \times 10^{-5}$ par heure, une valeur β de 10 % et une valeur β_D de 5 %.

Tableau B.9 – Exemple d'un essai périodique imparfait

Architecture	*DC*	λ_D = 0,5E-05	
		Essai périodique 100 %	Essai périodique 90 %
		β = 10 % β_D = 5 %	β = 10 % β_D = 5 %
1oo2	0 %	2,7E-03	6,0E-03
	60 %	9,7E-04	2,0E-03
	90 %	2,3E-04	4,4E-04
	99 %	2,4E-05	4,4E-05

B.3.3 Fréquence moyenne de défaillance dangereuse par heure (pour un mode de fonctionnement sollicitation élevée ou mode continu)

B.3.3.1 Procédure des calculs

La méthode de calcul de la probabilité de défaillance pour une fonction de sécurité d'un système E/E/PE relatif à la sécurité fonctionnant en mode sollicitation élevée ou mode continu est identique à celle utilisée pour le calcul d'un mode de fonctionnement faible sollicitation (voir B.2.1); la probabilité moyenne de non fonctionnement en cas de sollicitation (PFD_{SYS}) est cependant remplacée par la fréquence moyenne de défaillance dangereuse par heure (PFH_{SYS}).

La probabilité globale d'une défaillance dangereuse pour une fonction de sécurité du système E/E/PE relatif à la sécurité, PFH_{SYS} est déterminée en calculant les taux de défaillances dangereuses pour tous les sous-systèmes assurant la fonction de sécurité et en additionnant ces valeurs individuelles. Cela peut être exprimé par la formule suivante, puisque dans cette annexe les probabilités sont faibles:

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE}$$

où

– PFH_{SYS} est la fréquence moyenne de défaillance dangereuse par heure d'une fonction de sécurité du système E/E/PE relatif à la sécurité;

– PFH_S est la fréquence moyenne de défaillance dangereuse par heure du sous-système capteur;

– PFH_L est la fréquence moyenne de défaillance dangereuse par heure du sous-système logique; et

– PFH_{FE} est la fréquence moyenne de défaillance dangereuse par heure du sous-système élément final.

B.3.3.2 Architectures pour un mode de fonctionnement sollicitation élevée ou continu

NOTE 1 Il convient de considérer ce paragraphe de façon séquentielle, les équations applicables à plusieurs architectures n'étant données que lors de leur première utilisation. Voir également B.3.2.2.

NOTE 2 Les calculs sont basés sur les hypothèses données en B.3.1.

B.3.3.2.1 1oo1

Les Figures B.4 et B.5 montrent les diagrammes de blocs pertinents.

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\lambda_{DU} = \lambda_D(1 - DC); \qquad \lambda_{DD} = \lambda_D DC$$

Si l'on suppose que le système de sécurité met l'EUC en état de sécurité en cas de détection d'une éventuelle défaillance, on obtient pour une architecture 1oo1

$$PFH_G = \lambda_{DU}$$

B.3.3.2.2 1oo2

Les Figures B.6 et B.7 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est donnée en B.3.3.2.1. Si l'on suppose que le système de sécurité met l'EUC en état de sécurité une fois qu'une défaillance a été détectée dans les deux canaux, et en appliquant une approche prudente, on obtient

$$PFH_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})(1 - \beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU}$$

B.3.3.2.3 2oo2

Les Figures B.8 et B.9 illustrent les diagrammes de blocs pertinents. Si l'on suppose que chacun des canaux est mis en état de sécurité en cas de détection d'une éventuelle défaillance, on obtient pour une architecture 2oo2

$$PFH_G = 2\lambda_{DU}$$

B.3.3.2.4 1oo2D

Les Figures B.10 et B.11 montrent les diagrammes de blocs pertinents.

$$\lambda_{SD} = \frac{\lambda}{2} DC$$

$$t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$PFH_G = 2(1 - \beta)\lambda_{DU}((1 - \beta)\lambda_{DU} + (1 - \beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}' + 2(1 - K)\lambda_{DD} + \beta\lambda_{DU}$$

B.3.3.2.5 2oo3

Les Figures B.12 et B.13 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est donnée en B.3.3.2.1. Si l'on suppose que le système de sécurité met l'EUC en état de sécurité une fois qu'une défaillance a été détectée dans l'un des deux canaux, et en appliquant une approche prudente, on obtient

$$PFH_G = 6((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})(1 - \beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU}$$

B.3.3.2.6 1oo3

Les Figures B.12 et B.13 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} et la valeur de t_{GE} sont données en B.3.3.2.1 et B.3.2.2.2. Si l'on suppose que le système de

sécurité met l'EUC en état de sécurité une fois qu'une défaillance a été détectée dans l'un des trois canaux, et en appliquant une approche prudente, on obtient

$$PFH_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 (1-\beta)\lambda_{DU} t_{CE} t_{GE} + \beta\lambda_{DU}$$

B.3.3.3 Tableaux détaillés pour mode de fonctionnement sollicitation élevée ou mode continu

Tableau B.10 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques d'un mois et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (voir la Note 2)	**0 %**	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (voir la Note 3)	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	*DC*	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %
1oo1 (voir la Note 2)	**0 %**	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	**0 %**	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	2.1E-08	1.0E-07	2.0E-07	4.3E-08	2.0E-07	4.0E-07	2.7E-07	1.1E-06	2.1E-06
	90 %	5.1E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.5E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08
2oo2 (voir la Note 2)	**0 %**	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (voir la Note 3)	**0 %**	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	8.1E-08	1.6E-07	2.6E-07	1.6E-07	3.2E-07	5.2E-07	8.7E-07	1.7E-06	2.7E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	**0 %**	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.5E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90 %	5.2E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07	6.6E-08	2.6E-07	5.1E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08
1oo3	**0 %**	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.1E-07	2.5E-06	5.0E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.3 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFH_G est équivalent respectivement à PFH_S, PFH_L ou PFH_{FE} (voir B.3.3.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la fréquence moyenne d'une défaillance dangereuse.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

Tableau B.11 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques de trois mois et une durée moyenne de rétablissement de 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (voir la Note 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (voir la Note 3)	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2.5E-06			λ_D = 0.5E-05			λ_D = 2.5E-05		
		β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %
1oo1 (voir la Note 2)	0 %	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90 %	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07	6.4E-08	2.6E-07	5.1E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.2E-09	2.5E-08	5.0E-08
2oo2 (voir la Note 2)	0 %	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (voir la Note 3)	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	8.2E-08	1.6E-07	2.6E-07	1.7E-07	3.3E-07	5.3E-07	1.0E-06	1.8E-06	2.8E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	0 %	9.0E-08	2.8E-07	5.3E-07	2.6E-07	6.3E-07	1.1E-06	4.5E-06	5.9E-06	7.6E-06
	60 %	2.6E-08	1.1E-07	2.0E-07	6.6E-08	2.2E-07	4.2E-07	8.5E-07	1.6E-06	2.5E-06
	90 %	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07	9.3E-08	2.9E-07	5.3E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.7E-09	2.6E-08	5.1E-08
1oo3	0 %	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.5E-07	2.5E-06	5.0E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.3 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFH_G est équivalent respectivement à PFH_S, PFH_L ou PFH_{FE} (voir B.3.3.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la fréquence moyenne d'une défaillance dangereuse.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

Tableau B.12 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques de six mois et une durée moyenne de rétablissement de 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.2E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (voir la Note 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (voir la Note 3)	0 %	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07
	60 %	4.1E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.5E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2.5E-06			λ_D = 0.5E-05			λ_D = 2.5E-05		
		β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %
1oo1 (voir la Note 2)	0 %	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	2.4E-08	1.0E-07	2.0E-07	5.7E-08	2.1E-07	4.1E-07	6.3E-07	1.4E-06	2.3E-06
	90 %	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07	7.8E-08	2.7E-07	5.2E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08
2oo2 (voir la Note 2)	0 %	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (voir la Note 3)	0 %	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	8.4E-08	1.6E-07	2.6E-07	1.8E-07	3.3E-07	5.3E-07	1.2E-06	2.0E-06	2.9E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.8E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	0 %	1.3E-07	3.2E-07	5.5E-07	4.2E-07	7.7E-07	1.2E-06	8.4E-06	9.2E-06	1.0E-05
	60 %	3.3E-08	1.1E-07	2.1E-07	9.1E-08	2.4E-07	4.4E-07	1.5E-06	2.1E-06	2.9E-06
	90 %	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07	1.3E-07	3.2E-07	5.6E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	6.1E-09	2.6E-08	5.1E-08
1oo3	0 %	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	7.1E-07	2.7E-06	5.1E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.1E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.3 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFH_G est équivalent respectivement à PFH_S, PFH_L ou PFH_{FE} (voir B.3.3.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la fréquence moyenne d'une défaillance dangereuse.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

Tableau B.13 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques d'un an et une durée moyenne de rétablissement de 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (voir la Note 2)	**0 %**	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (voir la Note 2)	**0 %**	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (voir la Note 3)	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.1E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	**0 %**	1.1E-09	5.1E-09	1.0E-08	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.5E-08	1.0E-07
	60 %	4.1E-10	2.0E-09	4.0E-09	2.3E-09	1.0E-08	2.0E-08	5.0E-09	2.1E-08	4.1E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	**0 %**	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %
1oo1 (voir la Note 2)	**0 %**	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	**0 %**	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	2.9E-08	1.1E-07	2.1E-07	7.4E-08	2.3E-07	4.2E-07	1.1E-06	1.7E-06	2.6E-06
	90 %	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07	1.0E-07	3.0E-07	5.4E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.6E-09	2.6E-08	5.0E-08
2oo2 (voir la Note 2)	**0 %**	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (voir la Note 3)	**0 %**	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	8.9E-08	1.7E-07	2.7E-07	1.9E-07	3.5E-07	5.4E-07	1.7E-06	2.3E-06	3.2E-06
	90 %	9.6E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	1.0E-06	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	**0 %**	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-06	1.4E-06	1.6E-05	1.6E-05	1.6E-05
	60 %	4.6E-08	1.2E-07	2.2E-07	1.4E-07	2.9E-07	4.7E-07	2.8E-06	3.2E-06	3.8E-06
	90 %	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.6E-08	1.0E-07	2.1E-07	3.9E-07	6.2E-07
	99 %	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08	6.9E-09	2.7E-08	5.1E-08
1oo3	**0 %**	5.1E-08	2.5E-07	5.0E-07	1.1E-07	5.1E-07	1.0E-06	1.4E-06	3.2E-06	5.5E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.6E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.1E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

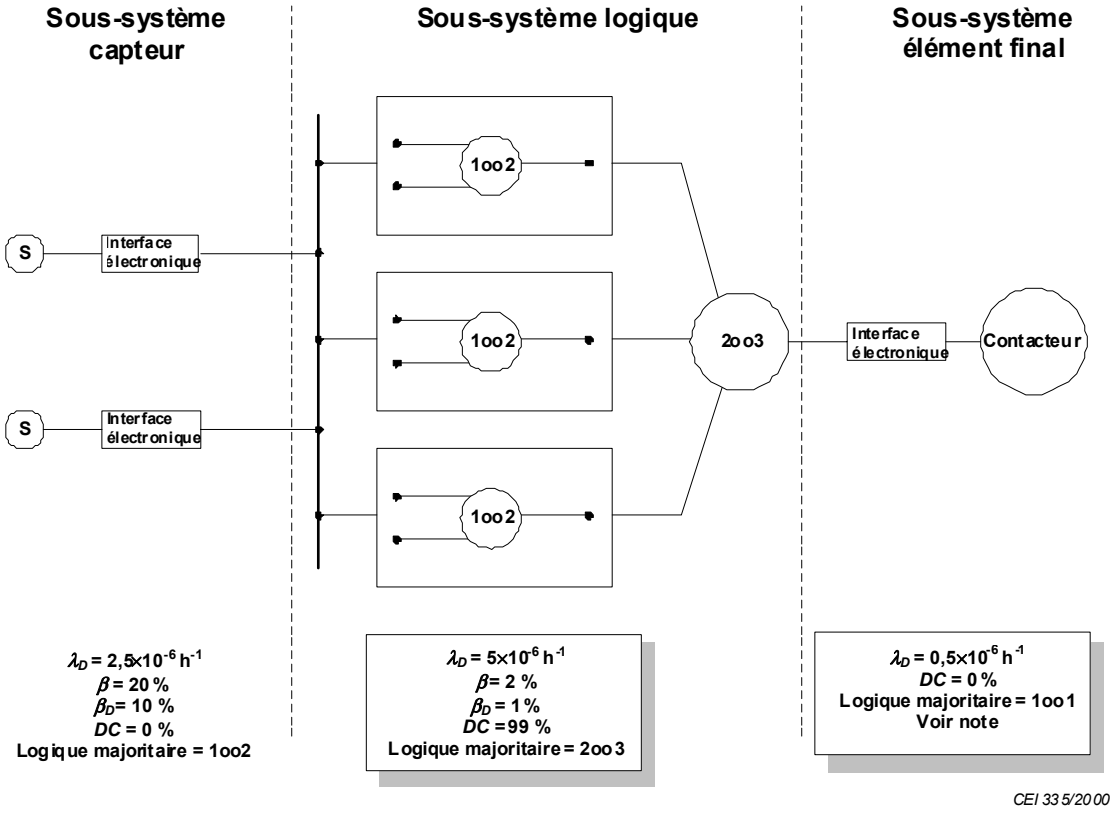
NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.3 et en fonction des hypothèses énoncées en B.3.1. Si le sous-système capteur, logique ou élément final comprend seulement un groupe de canaux à logique majoritaire, alors PFH_G est équivalent respectivement à PFH_S, PFH_L ou PFH_{FE} (voir B.3.3.1).

NOTE 2 Le tableau suppose que $\beta = 2 \times \beta_D$. Pour les architectures 1oo1 et 2oo2, les valeurs de β et de β_D n'affectent pas la fréquence moyenne d'une défaillance dangereuse.

NOTE 3 Le taux de défaillance en sécurité est supposé égal au taux de défaillance dangereuse et K = 0,98.

B.3.3.4 Exemple pour mode de fonctionnement sollicitation élevée ou mode continu

Soit une fonction de sécurité exigeant un système de niveau SIL 2. Supposons que l'évaluation initiale pour l'architecture du système, fondée sur une pratique antérieure, tient compte d'un groupe de deux capteurs à logique majoritaire 1oo2. Le sous-système logique est un système redondant 2oo3 configuré en système électronique programmable pilotant un seul contacteur d'arrêt. Ceci est illustré dans la Figure B.15. On suppose un essai périodique de six mois pour l'évaluation initiale.



NOTE Le sous-système élément final a une proportion globale de défaillance en sécurité supérieure à 60 %.

Figure B.15 – Architecture d'un exemple de fonctionnement en mode sollicitation élevée ou continu

Tableau B.14 – Fréquence moyenne d'une défaillance dangereuse du sous-système capteur dans l'exemple de mode de fonctionnement sollicitation élevée ou continu (intervalle entre essais périodiques de six mois et *MTTR* de 8 h)

Architecture	*DC*	λ_D =2,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2	0 %	7,6E-08	2,7E-07	5,2E-07
	60 %	2,4E-08	1,0E-07	2,0E-07
	90 %	5,3E-09	2,5E-08	5,0E-08
	99 %	5,0E-10	2,5E-09	5,0E-09
NOTE Ce tableau est extrait du Tableau B.12.				

Tableau B.15 – Fréquence moyenne d'une défaillance dangereuse du sous-système logique dans l'exemple de mode de fonctionnement sollicitation élevée ou continu (intervalle entre essais périodiques de six mois et *MTTR* de 8 h)

Architecture	*DC*	λ_D = 0,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0 %	4,2E-07	7,7E-07	1,2E-06
	60 %	9,1E-08	2,4E-07	4,4E-07
	90 %	1,3E-08	5,3E-08	1,0E-07
	99 %	1,0E-09	5,0E-09	1,0E-08
NOTE Ce tableau est extrait du Tableau B.12.				

Tableau B.16 – Fréquence moyenne d'une défaillance dangereuse du sous-système élément final dans l'exemple de mode de fonctionnement sollicitation élevée ou continu (intervalle entre essais périodiques de six mois et *MTTR* de 8 h)

Architecture	*DC*	λ_D = 0,5E-06
1oo1	0 %	5,0E-07
	60 %	2,0E-07
	90 %	5,0E-08
	99 %	5,0E-09
NOTE Ce tableau est extrait du Tableau B.12.		

A partir des Tableaux B.14 à B.16, on obtient les valeurs suivantes.

Pour le sous-système capteur,

$PFH_S = 5{,}2 \times 10^{-7}$ / h

Pour le sous-système logique,

$PFH_L = 1{,}0 \times 10^{-9}$ / h

Pour le sous-système élément final,

$PFH_{FE} = 5{,}0 \times 10^{-7}$ / h

Ainsi, pour la fonction de sécurité,

$PFH_{SYS} = 5{,}2 \times 10^{-7} + 1{,}0 \times 10^{-9} + 5{,}0 \times 10^{-7}$

$= 1{,}02 \times 10^{-6}$ / h

≡ **niveau 1 d'intégrité de sécurité**

Pour améliorer le système de manière à répondre au niveau 2 d'intégrité de sécurité, l'une des opérations suivantes peut être effectuée:

a) remplacer le type de capteur d'entrée et le monter de façon à améliorer la protection contre les défaillances de cause commune, et améliorer ainsi β de 20 % à 10 % et β_D de 10 % à 5 %;

$PFH_S = 2{,}7 \times 10^{-7}$ / h

PFH_L = $1{,}0 \times 10^{-9}$ / h

PFH_{FE} = $5{,}0 \times 10^{-7}$ / h

PFH_{SYS} = $7{,}7 \times 10^{-7}$ / h

≡ **niveau 2 d'intégrité de sécurité**

b) remplacer l'unique dispositif de sortie par deux dispositifs dans le système 1oo2 (β = 10 % et β_D = 5 %).

PFH_S = $5{,}2 \times 10^{-7}$ / h

PFH_L = $1{,}0 \times 10^{-9}$ / h

PFH_{FE} = $5{,}1 \times 10^{-8}$ / h

PFH_{SYS} = $5{,}7 \times 10^{-7}$ / h

≡ **niveau 2 d'intégrité de sécurité**

B.4 Approche booléenne

B.4.1 Généralités

L'approche booléenne comprend les techniques représentant la fonction logique qui relie les défaillances des composants individuels à la défaillance globale du système. Les principaux modèles booléens utilisés dans le domaine de la fiabilité sont les diagrammes de fiabilité (RBD), les arbres de panne (FT), les arbres d'événement et les diagrammes cause-conséquence. Le présent document ne traite que des deux premiers modèles. Toutes ces méthodes ont pour objet de représenter la structure logique du système. Toutefois, son comportement dans la durée n'est pas inclus dans ces techniques de modèle. Une attention toute particulière doit par conséquent être accordée aux caractéristiques de comportement (par exemple, les caractéristiques dépendant du temps telles que les essais périodiques) prises en compte dans les calculs. La première approche lorsqu'on utilise des modèles booléens consiste à séparer la représentation graphique des calculs. Ceci a été décrit dans l'article précédent où les diagrammes de fiabilité sont utilisés pour modéliser la structure et les calculs markoviens permettant d'évaluer *PFD* ou *PFH*. Il s'agit à présent de considérer de manière plus approfondie les calculs probabilistes sur diagramme de fiabilité et arbre de panne.

Cette approche se limite aux composants ayant un comportement suffisamment indépendant les uns des autres.

B.4.2 Modèle de diagramme de fiabilité

De nombreux exemples de diagramme de fiabilité ont déjà été donnés et la Figure B.1 représente, par exemple, une boucle de sécurité complète constituée de trois capteurs (A, B, C) fonctionnant en logique majoritaire 1oo3, un solveur logique (D) et deux éléments finaux (E, F) fonctionnant en logique majoritaire 1oo2.

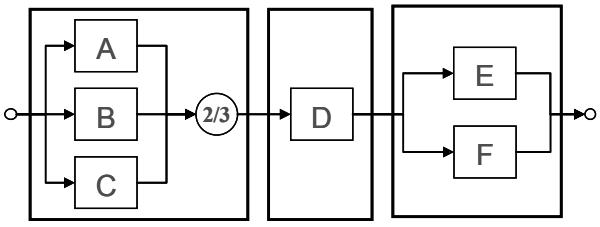


Figure B.16 – Diagramme de fiabilité d'une boucle complète simple avec capteurs fonctionnant en logique majoritaire 2oo3

La Figure B.16 illustre une boucle similaire avec des capteurs fonctionnant en logique majoritaire 2oo3. Cette représentation graphique présente trois principaux intérêts: elle reste

très proche de la structure physique du système étudié, elle est largement utilisée par les ingénieurs et elle constitue un bon support à l'examen.

Le principal inconvénient réside dans le fait que le diagramme de fiabilité constitue en lui-même davantage une méthode de représentation qu'une méthode d'analyse.

Pour de plus amples informations sur le diagramme de fiabilité, voir C.6.4 de la CEI 61508-7 et la CEI 61078.

B.4.3 Modèle d'arbres de panne

Les arbres de panne présentent exactement les mêmes propriétés que le diagramme de fiabilité avec la caractéristique supplémentaire de constituer une méthode d'analyse déductive efficace (du haut vers le bas) qui permet aux fiabilistes de développer des modèles étape par étape, de l'événement de tête (événement non souhaité ou indésirable) jusqu'aux défaillances des composants individuels.

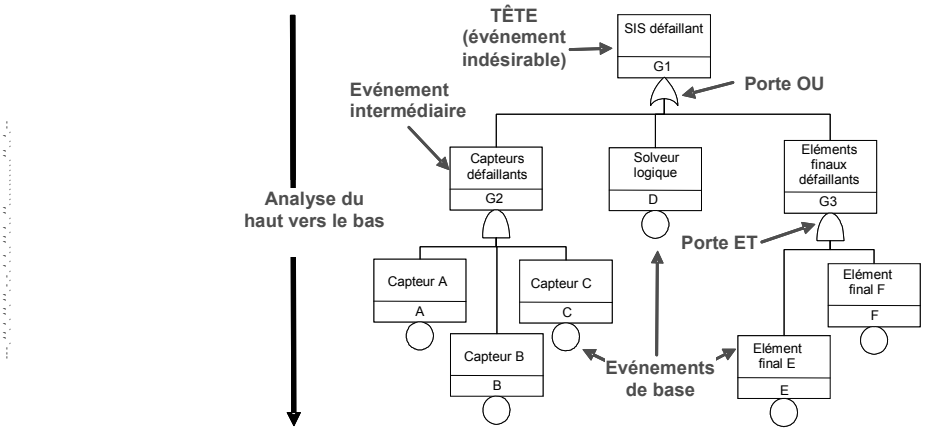


Figure B.17 – Arbre de panne simple équivalent au diagramme de fiabilité présenté à la Figure B.1

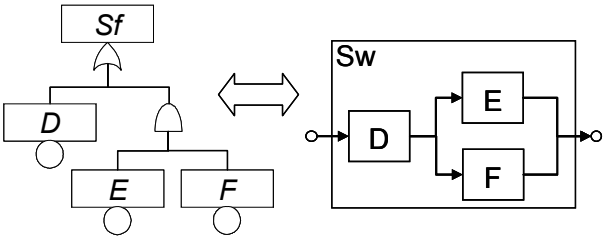
La Figure B.17 illustre un arbre de panne parfaitement équivalent au diagramme de fiabilité présenté à la Figure B.1 mais qui identifie les étapes de l'analyse du haut vers le bas (par exemple: système E/E/PE relatif à la sécurité défaillant => capteur défaillant => capteur A défaillant). Dans l'arbre de panne, les éléments en série sont reliés par des « portes OU » et les éléments en parallèle (c'est-à-dire redondants) sont reliés par des « portes ET ».

Pour de plus amples informations sur l'arbre de panne, voir B.6.6.5 et B.6.6.9 de la CEI 61508-7 et la CEI 61025.

B.4.4 Calculs de *PFD*

B.4.4.1 Présentation générale

Dans la mesure où le diagramme de fiabilité et l'arbre de panne représentent exactement les mêmes éléments, il est possible de réaliser les calculs de la même manière. La Figure B.18 illustre un petit arbre de panne et un petit diagramme de fiabilité équivalents à utiliser pour indiquer les principaux principes des calculs.



NOTE Sur cette figure, les lettres en italique indiquent les éléments défaillants et les lettres non en italique indiquent les éléments en fonctionnement.

Figure B.18 – Équivalence arbre de panne / diagramme de fiabilité

Le petit arbre de panne représente la fonction logique *Sf* = *D* ∪ (*E*∩*F*) où *Sf* est la défaillance du système et *D, E, F* les défaillances des composants individuels. Le petit diagramme de fiabilité représente la fonction logique Sw = D ∩ (E∪F) où Sw est le bon fonctionnement du système et *D, E, F* le bon fonctionnement des composants individuels. Alors, *Sf* = NON Sw, et *Sf* et Sw représentent exactement la même information (c'est-à-dire, la fonction logique et son double).

La principale utilisation de l'arbre de panne et du diagramme de fiabilité consiste à identifier les combinaisons des différentes défaillances des composants donnant lieu à la défaillance globale du système. Elles constituent les coupes d'ordre minimal ainsi désignées car elles indiquent l'endroit où procéder à la coupe du diagramme de fiabilité de sorte qu'un signal transmis à l'entrée ne puisse atteindre la sortie. Dans le cas présent, il y a deux ensembles de coupes: la défaillance simple (*D*) et la défaillance double (*E, F*).

L'application de calculs mathématiques probabilistes de base sur les fonctions logiques donne directement lieu à la probabilité de défaillance P_{Sf} du système et l'on obtient

$$P_{Sf} = P(D) + P(E \cap F) - P(D \cap E \cap F).$$

Lorsque les composants sont indépendants, cette formule devient:

$$P_{Sf} = P_D + P_E P_F - P_D P_E P_F$$

où

P_i est la probabilité de défaillance du composant i.

Cette formule ne dépend pas du temps et ne reflète que la structure logique du système.

Par conséquent, le diagramme de fiabilité et l'arbre de panne sont fondamentalement statiques, c'est-à-dire des modèles indépendants du temps.

Cependant, si la probabilité de défaillance de chaque composant individuel au temps *t* est indépendante de ce qui se produit sur l'autre composant sur le temps *[0, t]*, la formule ci-dessus reste valable à tout moment et peut s'écrire:

$$P_{Sf}(t) = P_D(t) + P_E(t)P_F(t) - P_D(t)P_E(t)P_F(t)$$

Il convient que l'analyste vérifie si les approximations requises sont acceptables ou non, pour finalement obtenir l'indisponibilité instantanée $U_{Sf}(t)$ du système:

$$U_{Sf}(t) = U_D(t) + U_E(t)U_F(t) - U_D(t)U_E(t)U_F(t)$$

Il est donc possible de conclure que les arbres de panne ou les diagrammes de fiabilité permettent de calculer directement l'indisponibilité instantanée U_{Sf} *(t)* des systèmes E/E/PE relatifs à la sécurité et que des calculs supplémentaires sont nécessaires, conformément à B.2.2:

$$PFD_{avg}(T) = \frac{1}{T} MDT(T) = \frac{1}{T}\int_0^T U_{Sf}(t)dt$$

Ce principe peut s'appliquer aux coupes d'ordre minimal:

– défaillance simple (*D*): $PFD^{D}(\tau) = \frac{1}{\tau}\int_0^{\tau} \lambda_D t.dt = \lambda_D \tau / 2$

– défaillance double (*E, F*): $PFD^{EF}(\tau) = \frac{1}{\tau}\int_0^{\tau} \lambda_E . \lambda_F . t^2 dt = \lambda_E \lambda_F \tau^2 / 3$

B.4.4.2 Calculs basés sur les outils d'arbre de panne ou de diagramme de fiabilité

La formule U_{Sf} *(t)* = U_D*(t)* + U_E*(t)*U_F*(t)* - U_D*(t)*U_E*(t)*U_F*(t)* décrite ci-dessus ne représente qu'un cas particulier de la formule dite de Poincaré. Plus généralement, si $Sf = \bigcup_i C_i$ où (C_i) représente les coupes d'ordre minimal du système, on obtient:

$$P(\bigcup_{i-1}^{n} C_i) = \sum_{j=1}^{n} P(C_j) - \sum_{j=1}^{n}\sum_{i=1}^{j-1} P(C_j \bigcap C_i) + \sum_{j=3}^{n}\sum_{i=2}^{j-1}\sum_{k=1}^{j-1} P(C_j \bigcap C_i \bigcap C_k) - \ldots$$

Le nombre de coupes d'ordre minimal augmente de manière exponentielle en fonction du nombre croissant de composants individuels. La formule de Poincaré donne alors lieu à une explosion combinatoire de termes très rapidement insoluble manuellement. Ce problème a heureusement été analysé depuis une quarantaine d'années et de nombreux algorithmes ont été développés pour gérer ces calculs. A l'heure actuelle, les développements les plus récents et les plus puissants sont basés sur les Diagrammes de décision binaire (BDD) qui sont déduits d'une décomposition de Shannon sophistiquée de la fonction logique.

De nombreux progiciels du commerce principalement basés sur des modèles d'arbre de panne sont quotidiennement utilisés par les fiabilistes dans de nombreux secteurs de l'industrie (nucléaire, pétrole, aéronautique, automobile, etc.). Ils peuvent être utilisés pour le calcul de la PFD_{avg} mais les analystes doivent rester très vigilants à cet égard car certains d'entre eux réalisent des calculs de la PFD_{avg} erronés. La principale faute constatée est la combinaison conventionnelle de la $PFD_{avg,i}$ des composants individuels (généralement obtenue tout simplement par $\lambda_i \tau/2$) pour produire un résultat qui est supposé représenter la PFD_{avg}. du système global. Comme spécifié ci-dessus, il s'agit d'un résultat erroné et non prudent.

Dans tous les cas, il est possible d'utiliser les progiciels à arbre de panne pour calculer l'indisponibilité instantanée du système U_{Sf}*(t)* à partir des indisponibilités instantanées de ses composants U_i*(t)*. La moyenne de U_{Sf}*(t)* peut ensuite être calculée sur la période considérée pour évaluer la PFD_{avg}. En fonction du logiciel utilisé, ceci peut être réalisé par le logiciel lui-même ou par des calculs latéraux.

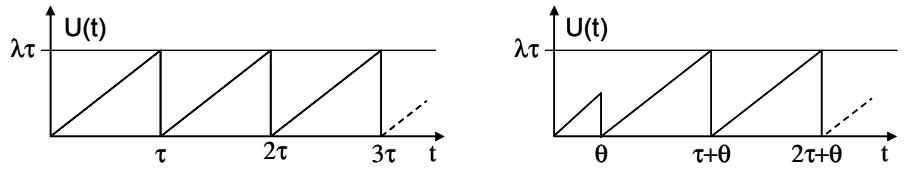


Figure B.19 – Indisponibilité instantanée *U(t)* de composants individuels soumis à essais périodiques

Le cas idéal décrit précédemment est représenté du côté gauche de la Figure B.19:

$$U_i\ (t) = \lambda\ \zeta \text{ et } \zeta = t \text{ modulo } \tau.$$

Il s'agit d'une courbe en dents de scie qui augmente de manière linéaire de 0 à $\lambda\tau$ et repart de 0 après un essai ou une réparation (considéré comme instantané dans la mesure où l'EUC est arrêté pendant ce temps).

Lorsque plusieurs composants sont utilisés dans des structures redondantes, les essais peuvent être étalés dans le temps comme illustré du côté droit de la Figure B.19 où le premier intervalle entre essais est différent des autres. Ceci n'a aucun effet sur la PFD_{avg} ou sur la valeur maximale qui sont égales à $\lambda\tau$/2 et $\lambda\tau$ dans les deux cas.

Bien entendu, dans des cas moins parfaits, ces courbes peuvent se révéler plus compliquées. Le paragraphe B.5.2 donne des lignes directrices sur la conception de courbes en dents de scie plus précises, mais pour les besoins du présent article, les courbes représentées à la Figure B.19 sont suffisantes.

Ceci peut s'appliquer au petit arbre de panne représenté à la Figure B.18 comme illustré à la Figure B.20 (où DU signifie Dangereuse Non détectée et CCF signifie Défaillance de Cause Commune). Le système est considéré comme constitué de deux composants redondants (E et F) et (D) est considérée comme une défaillance de cause commune sur ces composants. Le calcul a été réalisé avec les chiffres suivants:

$$\lambda_{DU} = 3{,}5 \times 10^{-6}/\text{h},\ \tau = 4\ 380 \text{ h et } \beta = 1\ \%$$

Un petit facteur β a été choisi pour éviter que la défaillance de cause commune ne prédomine pas dans le résultat au niveau supérieur et pour mieux en comprendre le fonctionnement.

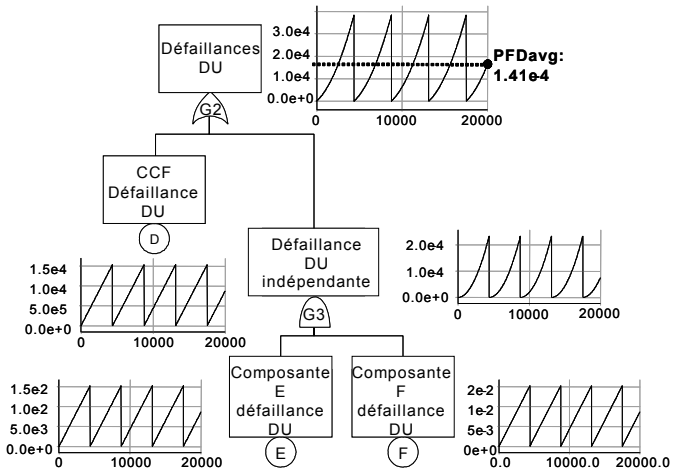


Figure B.20 – Principe des calculs de PFD_{avg} utilisant les arbres de panne

Le type de courbes en dents de scie représentées du côté gauche de la Figure B.19 est facilement identifiable comme entrées pour *D, E* et *F*. La CCF (*D*) est soumise à essai à chaque fois que *E* ou *F* est soumis à essai. Etant donné que *E* et *F* sont soumis à essai en même temps tous les 6 mois, la CCF (*D*) est également soumise à essai tous les 6 mois.

L'utilisation de l'un des algorithmes développés pour les calculs par arbre de panne permet de facilement tracer les courbes en dents de scie aux sorties de toutes les portes logiques. La PFD_{avg} est calculée en moyennant le résultat obtenu pour l'événement de tête. Ceci peut être réalisé par le logiciel à arbre de panne lui-même ou par des calculs manuels. On obtient $PFD_{avg} = 1{,}4 \times 10^{-4}$ et conformément à la présente norme, ce système satisfait à l'objectif chiffré de défaillance pour un niveau SIL 3 pour un mode de fonctionnement à faible sollicitation.

Comme illustré à la Figure B.20, les courbes présentent des pentes faibles entre les essais. Par conséquent, l'évaluation de la moyenne n'est pas difficile à réaliser, à condition d'avoir identifié et pris en compte le moment des essais.

Il est intéressant de noter que dès la mise en œuvre de la redondance, les courbes en dents de scie au niveau de l'événement de tête ne sont plus linéaires entre les essais (c'est-à-dire que le taux de défaillance global du système n'est plus constant).

Il est également intéressant de mesurer l'effet sur la PFD_{avg} de l'étalement dans le temps des essais des composants redondants plutôt que de les réaliser en même temps. Ceci est illustré à la Figure B.21 où les essais du composant F ont été décalés par rapport à ceux du composant E de 3 mois.

Ceci donne lieu à plusieurs effets importants:

– les CCF sont désormais soumises à essai tous les 3 mois (c'est-à-dire à chaque fois que E et F sont soumis à essai). Cette fréquence d'essai périodique est égale au double de celle appliquée dans le cas précédent.

– la courbe en dents de scie au niveau de l'événement de tête a également une fréquence d'essai périodique égale au double de celle appliquée précédemment.

– la courbe en dents de scie est moins étendue autour de sa moyenne que dans le cas précédent.

– la PFD_{avg} a été réduite à $8{,}3 \times 10^{-5:}$ avec cette nouvelle politique d'essai, le système est de niveau SIL 4.

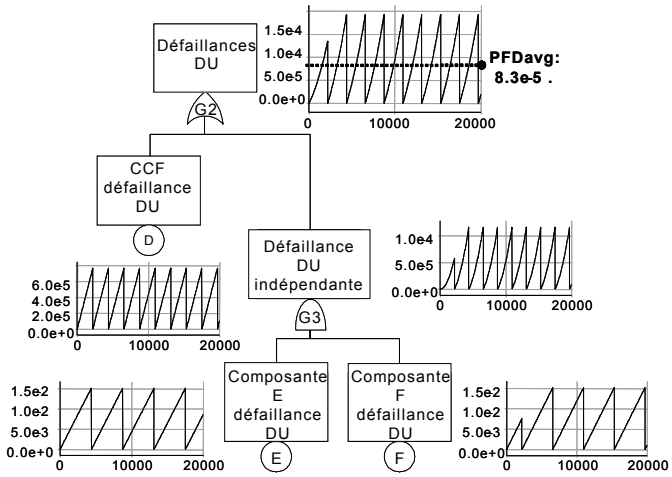


Figure B.21 – Effet du décalage des essais

Le décalage des essais et les procédures adéquates mises en œuvre augmentent la probabilité de détection de CCF et constituent un bon moyen de réduire la CCF pour les systèmes fonctionnant en mode faible sollicitation. Dans le cas présent, le système est passé du niveau SIL 3 à SIL 4 (du point de vue des défaillances du matériel et si d'autres exigences de la série CEI 61508 sont satisfaites).

La Figure B.22 représente la courbe en dents de scie obtenue en ajoutant un composant G (λ_{DU} = 7 × 10^{-9}/h jamais soumis à essai) et un composant H (λ_{DU} = 4 × 10^{-8}/h soumis à essai tous les 2 ans) montés en série avec le système modélisé à la Figure B.20.

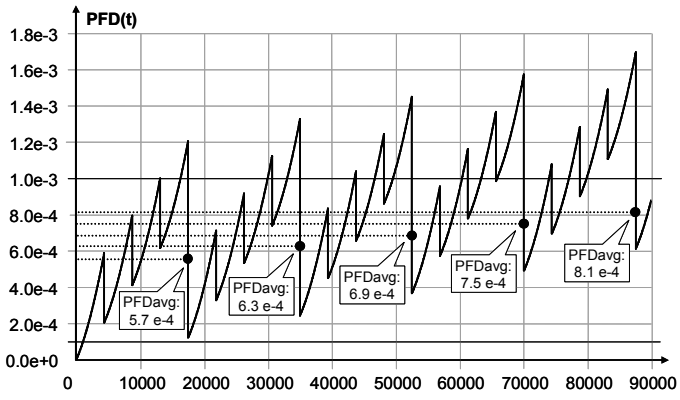


Figure B.22 – Exemple de modèle d'essai complexe

L'effet du composant G jamais soumis à essai est de deux ordres: la *PFD(t)* ne revient jamais à zéro après l'essai réalisé tous les deux ans et la PFD_{avg} augmente de manière continue (les cercles noirs correspondant à la PFD_{avg} sur la période couverte par la ligne en pointillé associée).

Même si les courbes en dents de scie élémentaires (telles que celles représentées à la Figure B.19) sont très simples, les résultats au niveau de l'événement de tête peuvent se révéler plus compliqués sans toutefois poser de problèmes particuliers.

Le présent article n'a pour objet que d'illustrer le principe du calcul utilisant des modèles booléens. Le paragraphe B.5.2 concernant les approches de Markov donne des lignes directrices sur la conception de courbes en dents de scie d'entrée plus sophistiquées pour les composants élémentaires.

Il est donc possible de conclure que lorsque les composants individuels sont suffisamment indépendants, il n'y a aucun problème pour calculer la PFD_{avg} des systèmes E/E/PE relatifs à la sécurité en utilisant des techniques booléennes classiques. Ceci n'est pas aussi simple du point de vue théorique et il convient que l'analyste dispose d'une solide connaissance des calculs probabilistes pour identifier et écarter les mises en œuvre erronées de la PFD_{avg} susceptibles d'être observées. Sous réserve de prendre ces précautions, il est possible d'utiliser tout progiciel à arbre de panne pour réaliser les calculs sus-mentionnés.

Les techniques booléennes peuvent également être utilisées pour les calculs de *PFH*; les développements théoriques à cet égard ne font cependant pas l'objet de la présente annexe informative.

B.5 Approches de transition d'état

B.5.1 Généralités

Les modèles booléens sont fondamentalement indépendants du temps, l'introduction du temps n'est possible que dans des cas particuliers spécifiques. Ceci relève davantage de l'ordre de l'artificiel et nécessite une bonne connaissance des calculs probabilistes pour éviter toute erreur. Par conséquent, il est possible d'utiliser en lieu et place d'autres modèles probabilistes, par nature dynamiques. Dans le domaine de la fiabilité, ils sont fondamentalement basés sur l'approche suivante en deux étapes:

– identification de tous les états du système étudié;

– analyse des transitions du système d'un état à l'autre, selon l'occurrence des événements et pendant sa durée de vie.

C'est la raison pour laquelle ils sont regroupés dans la catégorie des modèles de transition d'état.

En réalité, l'approche générale consiste à construire un type d'automate se comportant comme le système étudié lorsque des événements (défaillances, réparations, essais, etc.) se produisent. Selon la présente norme, les systèmes E/E/PE relatifs à la sécurité ne présentent que des états discrets, ce qui équivaut à construire un automate d'état fini. Ces modèles sont de nature dynamique et peuvent être mis en œuvre de différentes manières: représentations graphiques, langages formels spécifiques ou langages de programmation communs. La présente annexe spécifie deux de ces modèles qui sont très différents mais cependant complémentaires:

– le modèle markovien développé au tout début du siècle dernier. Il est relativement bien connu et géré de manière analytique;

– le modèle du réseau de Pétri développé dans les années soixante. Il est moins connu (mais de plus en plus utilisé du fait de sa flexibilité) et géré par la simulation de Monte Carlo.

Les deux modèles sont basés sur des représentations graphiques très utiles pour les utilisateurs. D'autres techniques basées sur la modélisation en langage formel sont analysées de manière succincte à la fin de cet article.

B.5.2 Approche de Markov

B.5.2.1 Principe de modélisation

L'approche de Markov est la plus ancienne de toutes les approches dynamiques utilisées dans le domaine de la fiabilité. Les processus de Markov sont divisés en deux types: ceux qui sont « amnésiques » (processus de Markov homogènes où tous les taux de transition sont constants) et les autres (processus semi-markovien). Dans la mesure où le futur d'un processus de Markov homogène ne dépend pas de son passé, il est plus facile de réaliser des calculs analytiques. Ceci se révèle plus difficile pour les processus semi-markoviens pour lesquels il est possible d'utiliser une simulation de Monte Carlo. La présente partie de la série

CEI 61508 ne considère que les processus de Markov homogènes et utilise le terme « processus de Markov » pour des raisons de simplicité (voir C.6.4 de la CEI 61508-7 et la CEI 61165).

La formule de base fondamentale des processus de Markov est la suivante:

$$P_i(t+dt) = \sum_{k \neq i} P_k(t)\lambda_{ki}dt + P_i(t)(1 - \sum_{k \neq i} \lambda_{ik}dt)$$

Dans cette formule, λ_{ki} est le taux de transition (par exemple, taux de défaillance ou de réparation) de l'état *i* à l'état *k*. Il s'explique de lui-même: la probabilité d'être dans l'état *i* à *t+dt* est la probabilité de passer à l'état *i* (lorsqu'il est dans un autre état *k*) ou de rester à l'état *i* (s'il est déjà dans cet état) entre *t* et *t* + *dt*.

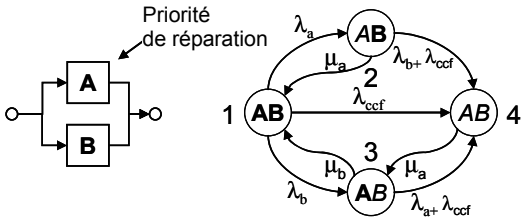


Figure B.23 – Diagramme de Markov modélisant le comportement d'un système à deux composants

Il existe une relation directe entre l'équation ci-dessus et une représentation graphique telle que celle de la Figure B.23 qui modélise un système constitué de deux composants avec une seule équipe de réparation (composant A ayant priorité pour réparation) et une défaillance de cause commune. Dans cette figure, **A** indique que A fonctionne et *A* qu'il est défaillant. Etant donné que les temps de détection doivent être pris en considération, μ_a et μ_b donnés à la Figure B.23 représentent les taux de rétablissement des composants (c'est-à-dire μ_a*=1/MTTR*$_a$ et μ_b*=1/MTTR*$_b$*)*.

Par exemple, la probabilité d'être à l'état 4 est tout simplement calculée comme suit:

$$P_4(t+dt) = [P_1(t)\lambda_{ccf} + P_2(t)(\lambda_b + \lambda_{ccf}) + P_3(t)(\lambda_a + \lambda_{ccf})]dt + P_4(t)(1 - \mu_a dt)$$

Ceci donne lieu à une équation différentielle vectorielle,

$d\vec{P}(t)/dt = [M]\vec{P}(t)$, qui est résolue de manière classique par:

$$\vec{P}(t) = e^{t[M]}\vec{P}(0)$$

où

[*M*] est la matrice de Markov comprenant les taux de transition et $\vec{P}(0)$ le vecteur des conditions initiales (généralement un vecteur-colonne avec 1 pour l'état parfait et 0 pour les autres).

Même si l'exponentielle d'une matrice n'a pas exactement les mêmes propriétés qu'une exponentielle normale, il est possible d'écrire:

$$\vec{P}(t) = e^{(t-t1)[M]} e^{t1[M]} \vec{P}(0) = e^{(t-t1)[M]} \vec{P}(t1)$$

Ceci démontre la propriété de base des processus de Markov: la connaissance des probabilités des états à un instant donné *t1* récapitule tous les états passés et suffit à calculer la manière dont le système évolue dans le futur à partir de *t1*. Ceci se révèle très utile pour les calculs de *PFD*.

Depuis très longtemps, des algorithmes efficaces ont été développés et mis en œuvre dans les progiciels pour résoudre les équations sus-mentionnées. Ainsi, lorsqu'il utilise cette approche, l'analyste n'a plus qu'à s'intéresser à la construction des modèles sans se soucier des calculs mathématiques sous-jacents, même si, dans tous les cas, il doit au moins comprendre ce qui est décrit dans la présente annexe.

La Figure B.24 illustre le principe des calculs de *PFD*:

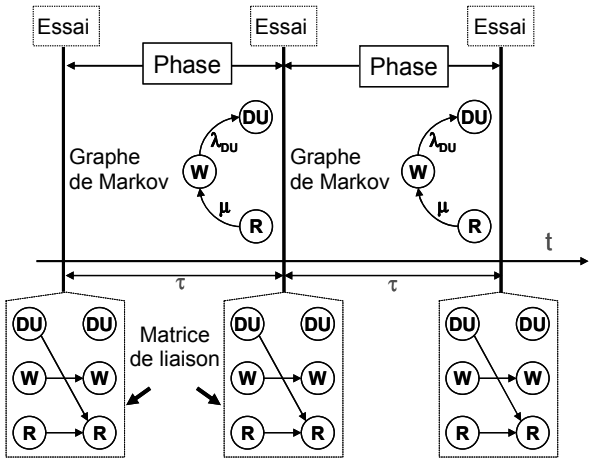


Figure B.24 – Principe de la modélisation de Markov multiphase

Les calculs de *PFD* concernent les systèmes E/E/PE relatifs à la sécurité fonctionnant en mode faible sollicitation et soumis régulièrement à essai (périodique). Pour ces systèmes, les réparations ne peuvent être commencées que lorsque les essais sont réalisés. Les essais sont des points singuliers dans le temps ce qui ne représente pas un problème puisqu'il est possible d'utiliser une approche de Markov multiphase pour les traiter.

Par exemple, un système simple constitué d'un seul composant soumis à essai périodique présente trois états tel qu'illustré à la Figure B.24: en fonctionnement (W), défaillance dangereuse non détectée (DU) et en réparation (R).

Entre les essais, son comportement est modélisé par le processus de Markov à la partie supérieure de la Figure B.24: il peut être défaillant (W→ DU) ou en cours de réparation (R→ W). Dans la mesure où aucune réparation ne peut être commencée pendant un intervalle entre essais, il n'y a pas de transition de DU à R. Etant donné que le diagnostic de la défaillance a été effectué avant de passer à l'état R, μ représente le taux de réparation du composant (c'est-à-dire μ=1/*MRT*) à la Figure B.24.

Lorsqu'un essai est réalisé (voir matrice de liaison à la Figure B.14), une réparation est commencée en cas de défaillance (DU→ R), le composant reste en état de fonctionnement s'il était à l'état de bon fonctionnement (W→ W) et dans le cas très hypothétique qu'une réparation commencée à l'essai précédent ne soit pas terminée, il reste à l'état en réparation (R→ R). Une matrice de liaison [*L*] peut être utilisée pour calculer les conditions initiales au début de l'état *i+1* à partir des probabilités des états à la fin de l'essai *i*. Ceci donne l'équation suivante:

$$\begin{bmatrix} P_{DU}(0) \\ P_w(0) \\ P_R(0) \end{bmatrix}_{i+1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} P_{DU}(\tau) \\ P_w(\tau) \\ P_R(\tau) \end{bmatrix}_i \equiv \vec{P}_{i+1}(0) = [L]\vec{P}_i(\tau)$$

En remplaçant $\vec{P}_i(\tau)$ par sa valeur, on obtient une équation de récurrence qui permet de calculer les conditions initiales au début de chaque intervalle entre essais:

$$\vec{P}_{i+1}(0) = [L]e^{t[M]}\vec{P}_i(0)$$

Ceci peut être appliqué pour calculer les probabilités à tout moment $t = i\tau + \zeta$. Par exemple, pendant l'intervalle entre essais *i*, on obtient:

$$\vec{P}(t) = \vec{P}_i(\zeta) = e^{\zeta[M]}\,\vec{P}_i(0), \quad (i-1)\tau \le t < i\tau, \quad \zeta = t \bmod \tau$$

L'indisponibilité instantanée est obtenue directement en faisant la somme des probabilités des états dans lesquels le système est indisponible. Un vecteur-ligne (q_k) est utile pour exprimer cette opération:

$$U(t) = \sum_{k=1}^{n} q_k P_k(t)$$

où $q_k = 1$ si le système est indisponible à l'état k, et $q_k = 0$ dans les autres cas.

Pour le modèle simple, $PFD(t) = U(t) = P_{DU}(t) + P_R(t)$ est obtenue et l'aspect de la courbe en dents de scie obtenue avec ce modèle est illustré à la Figure B.25.

La PFD_{avg} est calculée comme précédemment au moyen du *MDT* qui pour sa part est facile à calculer à partir des temps moyens cumulés écoulés dans ces états:

$$\vec{MCT}(T) = \int_0^T \vec{P}(t)dt$$

Comme pour $\vec{P}(t)$, des algorithmes efficaces sont réputés pour réaliser ce calcul sur la période *[0, T]* pour obtenir: $PFD_{avg}(T) = \frac{1}{T}\sum_{k=1}^{n} q_k MCT_k(T)$

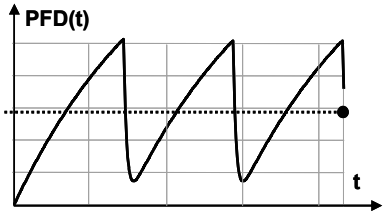


Figure B.25 – Courbe en dents de scie obtenue par l'approche de Markov multiphase

L'application de cette formule au modèle représenté à la Figure B.24 donne:

$$PFD_{avg}(T) = \frac{1}{T}\left[MCT_{DU}(T) + MCT_{R}(T)\right]$$

Ceci peut être ramené au premier terme si l'EUC est arrêté pendant la réparation.

Le cercle noir sur la Figure B.25 représente la PFD_{avg} de la courbe en dents de scie pendant toute la période de calcul.

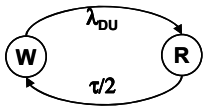


Figure B.26 – Approximation du modèle markovien

A noter que les calculs ci-dessus sont souvent réalisés en utilisant le modèle d'approximation représenté à la Figure B.26 où l'état DU et l'état R ont été fusionnés et où $\tau/2$ (c'est-à-dire le temps moyen de détection de la défaillance) a été utilisé comme temps de rétablissement équivalent. Ceci ne s'applique que si les équations de Markov ont été préalablement résolues par un autre moyen pour trouver cette équivalence. Ceci peut se révéler très difficile pour des systèmes plus importants et ne s'applique que si le temps de réparation est négligeable.

Le modèle simple de la Figure B.24 peut être facilement amélioré pour des composants plus réalistes. Sur la Figure B.27, la matrice de liaison modélise un composant qui a une probabilité, γ, de défaillance par l'essai (c'est-à-dire, une défaillance réelle en cas de sollicitation) et une probabilité, σ,que la défaillance n'ait pas été détectée par l'essai (par erreur humaine).

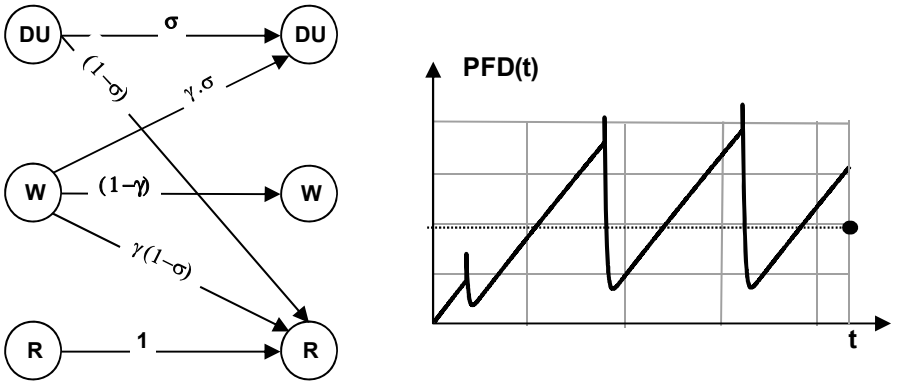


Figure B.27 – Effet des défaillances dues à la sollicitation même

L'aspect de la courbe en dents de scie a changé et les transitions observées pour chaque essai correspondent à la probabilité de non fonctionnement en cas de sollicitation γ. Ici encore, le cercle noir représente la PFD_{avg}.

Lorsqu'un composant (redondant) est déconnecté pour essai, il devient indisponible pendant toute l'exécution de l'essai et ceci contribue à sa PFD_{avg}. Par conséquent, la durée de l'essai, π, doit être prise en compte et une phase supplémentaire doit être introduite entre les intervalles d'essais. Ceci est illustré à la Figure B.28 où les états R et W ne sont modélisés dans cette phase que pour des raisons d'exhaustivité.

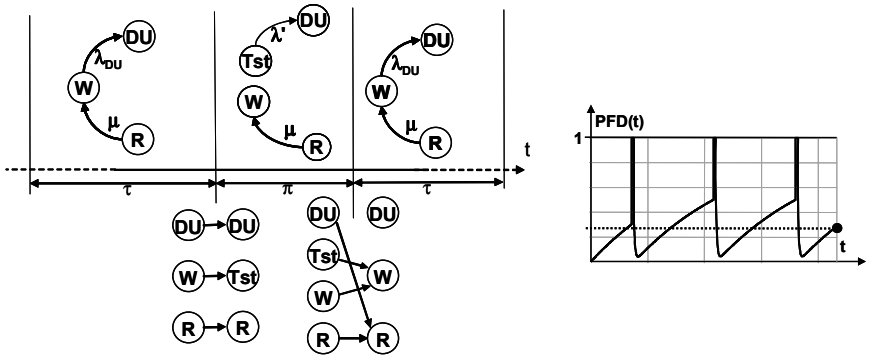


Figure B.28 – Modélisation de l'effet de la durée d'essai

Dans ce modèle markovien, le système est indisponible dans les états R, DU et Tst. Ce cas est plus compliqué que précédemment mais le principe des calculs reste exactement le même. Le comportement de la courbe en dents de scie est représenté à droite. Le système est indisponible pendant les durées d'essai et ceci peut constituer la contribution de tête à PFD_{avg}.

Les précédents diagrammes de Markov ne tenaient compte que des défaillances dangereuses non détectées, mais il est également possible de représenter les défaillances dangereuses détectées. La différence réside dans le fait que la réparation commence une fois tel que représenté à la Figure B.29. Par conséquent, μ_{DD} est le taux de rétablissement du composant (μ_{DD} =*1/MTTR*), où μ_{DU} est le taux de réparation (μ_{DU}=1*/MRT).*

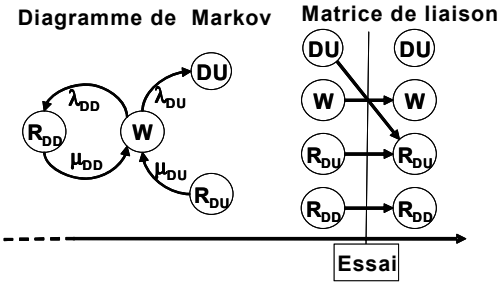


Figure B.29 – Modèle markovien multiphase avec des défaillances DD et DU

Il convient, si nécessaire, de représenter des défaillances en sécurité, mais les diagrammes de Markov choisis dans le cas présent sont des représentations les plus simples possible.

Le principal problème posé par les diagrammes de Markov réside dans le fait que le nombre d'états augmente de manière exponentielle en fonction du nombre croissant de composants du système étudié. Par conséquent, la construction de diagrammes de Markov et la réalisation des calculs ci-dessus sans appliquer des approximations drastiques deviennent des opérations très rapidement insolubles manuellement.

L'utilisation d'un progiciel de Markov efficace permet de pallier les difficultés de calcul. De nombreux progiciels de ce type sont disponibles même s'il n'est pas toujours possible de les utiliser directement pour les calculs de PFD_{avg}: la plupart réalisent des calculs d'indisponibilité instantanée, mais seuls certains d'entre eux calculent les temps moyens cumulés écoulés dans ces états et un petit nombre seulement permet de réaliser une modélisation multiphase. Dans tous les cas, il n'est pas réellement difficile de les adapter aux calculs de PFD_{avg}.

S'agissant de la modélisation proprement dite et lorsque les dépendances entre composants sont faibles, il est possible d'associer les approches de Markov et booléennes:

– les modèles markoviens sont utilisés pour établir les indisponibilités instantanées de chacun des composants;

– les arbres de panne ou les diagrammes de fiabilité sont utilisés pour combiner les indisponibilités individuelles permettant de calculer l'indisponibilité instantanée *PFD(t)* du système complet;

– PFD_{avg} est obtenue en moyennant *PFD(t)*.

Cette approche mixte a été décrite en B.4 et les courbes en dents de scie telles que celles illustrées aux Figures B.25, B.27 et B.28 peuvent être utilisées comme entrée des arbres de panne.

Lorsque les dépendances entre composants ne sont pas négligeables, certains outils sont disponibles pour construire automatiquement les diagrammes de Markov. Ils sont basés sur des modèles de niveau supérieur aux modèles markoviens (par exemple, réseaux de Pétri, langage formel). L'explosion combinatoire du nombre d'états peut toujours entraîner des difficultés.

Cette approche mixte est très efficace pour modéliser des systèmes complexes.

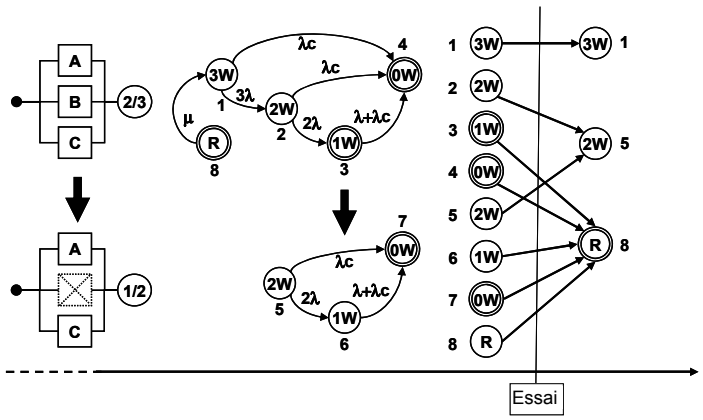


Figure B.30 – Changement de logique (2oo3 à 1oo2) au lieu de réparer une première défaillance

La Figure B.30 illustre la modélisation d'un système constitué de trois composants soumis à essai en même temps et fonctionnant en logique majoritaire 2oo3. Lorsqu'une défaillance est détectée, la logique passe de 2oo3 à 1oo2 car une logique 1oo2 est meilleure qu'une logique 2oo3 du point de vue de la sécurité (mais représente le cas le plus défavorable du point de vue d'une défaillance parasite). La réparation n'intervient que lorsqu'une deuxième défaillance est détectée; la réparation consiste à remplacer les trois éléments par trois nouveaux éléments. Ceci introduit des contraintes systémiques qui rendent impossible la construction du comportement du système complet en combinant tout simplement les comportements indépendants de ses composants.

B.5.2.2 Principe des calculs de *PFH*

Pour les calculs de *PFH*, il est possible d'utiliser le même type de modélisation de Markov multiphase pour les défaillances DU détectées par des essais périodiques. Pour des raisons de simplicité, n'est représenté que le principe des calculs de *PFH* pour des défaillances DD ne nécessitant que des modèles markoviens conventionnels (monophase). Bien entendu, pour des systèmes E/E/PE relatifs à la sécurité fonctionnant en mode continu et présentant des défaillances DU détectées par les essais périodiques, il convient d'utiliser l'approche de Markov multiphase, ce qui ne modifie cependant pas le principe exposé ci-après.

La Figure B.31 présente deux diagrammes de Markov modélisant le même système constitué de deux composants redondants avec une défaillance de cause commune. Du côté gauche, les composants (A et B) sont réparables. Du côté droit, ils ne sont pas réparables.

Sur les deux diagrammes, l'état 4 (*AB*) est absorbant. Le système reste à l'état défaillant après une défaillance globale et *P(t) = P1(t) + P2(t) + P3(t)* est la probabilité d'absence de défaillance sur la période *[0, t]*. Alors *R(t) = P(t)* est la fiabilité du système et *F(t) = 1 - R(t) = P4(t)* est sa non fiabilité.

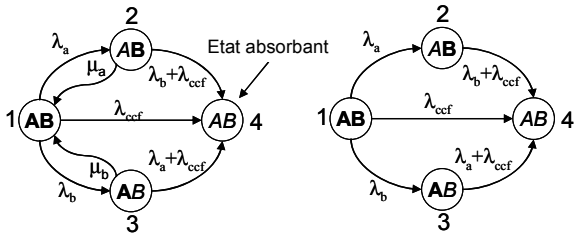


Figure B.31 – Diagrammes de Markov de « fiabilité » avec un état absorbant

Comme abordé en B.2.3, ce modèle de fiabilité constitue le modèle de traitement approprié lorsque la défaillance des systèmes E/E/PE relatifs à la sécurité donne immédiatement lieu à une situation dangereuse. Une nouvelle fois, μ_a et μ_b représentent les taux de rétablissement des composants (c'est-à-dire μ_a=1/*MTTR*$_a$ et μ_b=1/*MTTR*$_b$).

Ce type de diagramme de Markov de fiabilité fournit directement la *PFH* par *PFH = F(T)/T*. Par exemple, à partir de la Figure B.31, $PFH(T) = P4(T)/T$ (à condition que *P4(T)* << 1), est directement obtenue.

Ce type de diagramme de Markov de fiabilité permet également de calculer le *MTTF* du système au moyen de la formule suivante:

$$MTTF = \lim_{t\to\infty} \sum_{k=1}^{n} a_k MCT_k(t)$$

Dans cette formule, *MCT*$_k$*(t)* est le temps moyen cumulé écoulé à l'état *k,* et a_k = 1 si *k* est un état de bon fonctionnement et a_k = 0 dans les autres cas.

Une limite supérieure est obtenue par:

$$PFH \approx 1/MTTF$$

Des algorithmes efficaces ont été développés et pratiquement tous les progiciels de Markov peuvent être utilisés pour les calculs de *F(T)* et de *MTTF*.

Les estimations de *PFH* sus-mentionnées s'appliquent dans tous les cas même en l'absence de taux de défaillance global constant du système (comme pour le diagramme du côté droit de la Figure B.31). La seule contrainte est d'utiliser un diagramme de Markov de fiabilité avec un (ou plusieurs) état(s) absorbant(s). Bien entendu, ceci s'applique lorsqu'on utilise un modèle multiphase.

Lorsque tous les états sont totalement et rapidement réparables, le taux de défaillance global du système $\Lambda(t)$ tend rapidement vers une valeur asymptotique Λ_{as} = 1/*MTTF*. Dans ces diagrammes, à l'exception des états parfaits et absorbants, tous les états sont quasi instantanés (car les *MTTR* des composants sont courts comparés à leurs *MTTF*). Ceci permet d'évaluer directement les taux de défaillance globaux constants du système de chaque

scénario en commençant de l'état parfait pour aboutir à l'état absorbant. Le diagramme de Markov du côté gauche de la Figure B.31 modélise ce type de système totalement et rapidement réparable. Ce qui donne:

– $1 \rightarrow 4$: $\Lambda_{14}=\lambda_{ccf}$

– $1 \rightarrow 2 \rightarrow 4$: $\Lambda_{124}=\lambda_a . (\lambda_b+ \lambda_{ccf})/[(\lambda_b+ \lambda_{ccf})+\mu_a] \approx \lambda_a . (\lambda_b+ \lambda_{ccf})/ \mu_a$

– $1 \rightarrow 3 \rightarrow 4$: $\Lambda_{134}=\lambda_b . (\lambda_a+ \lambda_{ccf})/[(\lambda_a+ \lambda_{ccf})+\mu_b] \approx \lambda_b . (\lambda_a+ \lambda_{ccf})/ \mu_b$

Pour le scénario $1 \rightarrow 3 \rightarrow 4$ dans les formules ci-dessus, λ_b est le taux de transition régissant la transition de l'état parfait et $(\lambda_a+ \lambda_{ccf})/ \mu_b$ est la probabilité de passage à 4 plutôt que du retour à 1 lorsqu'il est à l'état 3.

En définitive: $\Lambda_{as}= \Lambda_{12}+ \Lambda_{124}+ \Lambda_{134}=1/MTTF$

Ceci peut être facilement généralisé aux diagrammes de Markov complexes mais ne s'applique qu'aux systèmes totalement et rapidement réparables, c'est-à-dire des défaillances DD.

Le diagramme de Markov du côté droit de la Figure B.31 n'est pas totalement et rapidement réparable. Par conséquent, l'application du calcul ci-dessus conduirait à des résultats erronés.

Lorsque le système E/E/PE relatif à la sécurité fonctionnant en mode continu est utilisé conjointement à d'autres barrières de sécurité, sa disponibilité doit être prise en compte. Ceci est représenté sur les deux diagrammes de la Figure B.32 ci-dessous: absence d'état absorbant et réparation du système après une défaillance globale. *P(t) = P1(t) + P2(t) + P3(t)* est la probabilité que le système fonctionne à *t*. Alors, *A(t) = P(t)* est sa disponibilité et *U(t)* = 1 - *A(t) = P4(t)* est son indisponibilité.

Ce cas est très différent de l'exemple représenté à la Figure B.31. Il convient d'utiliser *R(t)* et *A(t)* correctement, tout comme *U(T)* et *F(T)* si des résultats corrects doivent être obtenus.

En cas de défaillances DD, le moyen le plus simple de résoudre ce problème consiste à calculer la limite supérieure de *PFH* au moyen de *MDT* et *MUT* comme expliqué en B.2.3.

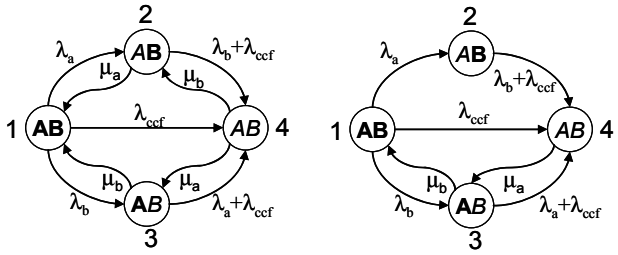


Figure B.32 – Diagrammes de Markov de « disponibilité » sans état absorbant

L'une des propriétés intéressantes des diagrammes de Markov de disponibilité est le fait qu'ils atteignent un équilibre asymptotique lorsque la probabilité d'entrer dans un état donné est égale à la probabilité d'en sortir. Soit l'expression:

– $P_{i,as} = \lim_{t \to \infty} P_i(t)$ la valeur asymptotique de $P_i(t)$

– $\lambda_i = \sum_{j \neq i} \lambda_{ij}$ le taux de transition de *i* à tout autre état

A chaque fois que le système passe à l'état *i*, le temps moyen de séjour dans cet état est de $Mst_i = 1/\lambda_i$.

Ceci permet de calculer $MUT = \sum_i (1 - q_i) P_{i,as} Mst_i$ et $MDT = \sum_i q_i P_{i,as} Mst_i$

où

q_i = 0, si *i* est un état de fonctionnement, et égal à 1 dans les autres cas.

En définitive est obtenue: $PFH = 1/(MUT + MDT) = 1/\sum_i P_{i,as} Mst_i = 1/\sum_i \frac{P_{i,as}}{\lambda_i}$

Il convient de noter que le nombre de défaillances observées sur la période *[0, T]* est donné par: $n = T/\sum_i \frac{P_{i,as}}{\lambda_i}$.

Dans la mesure où la plupart des progiciels de Markov sont en mesure de déterminer les probabilités asymptotiques, la réalisation de ces calculs ne présente aucune difficulté particulière.

Lorsque la période considérée est trop courte pour atteindre la convergence du processus de Markov, *PFH* peut être calculée au moyen de: $w(t) = \sum_{i \neq f} \lambda_{if} P_i(t)$.

On obtient: $PFH(T) = \sum_{i \neq f} \lambda_{if} \frac{\int_0^T P_i(t) dt}{T} = \frac{\sum_{i \neq f} \lambda_{if} MCT_i(T)}{T}$

Ici encore, il n'existe aucune difficulté pour réaliser ces calculs avec un progiciel de Markov, fournissant le temps de séjour cumulé dans chacun des états.

Dans le cas de systèmes totalement et rapidement réparables (défaillances DD), le taux de Vesely $\Lambda_V(t)$ tend très rapidement vers une valeur asymptotique, Λ_{as},qui représente une bonne approximation du taux de défaillance global constant du système. Par conséquent, dans ce cas la *PFH* peut être calculée de la même manière que dans le cas de fiabilité.

En cas de défaillances DU, ceci se révèle plus compliqué en raison de la modélisation multiphase. La formule ci-dessus peut être généralisée pour obtenir:

$$PFH(T) = \frac{\sum_{\varphi=1}^{n} \sum_{i \neq f} \lambda_{if} MCT_i(T_\varphi)}{\sum_{\varphi=1}^{n} T_\varphi}$$

Dans cette formule, T_φ est la durée de la phase φ.

En règle générale, les processus de Markov multiphase atteignent également l'équilibre lorsque la probabilité de sortir d'un état donné est égale à la probabilité d'y entrer. Les valeurs asymptotiques n'ont aucun rapport avec celles décrites ci-dessus mais elles peuvent être utilisées dans la formule ci-dessus.

Il est possible de conclure que l'approche de Markov fournit un certain nombre de possibilités pour calculer la *PFH* d'un système E/E/PE relatif à la sécurité fonctionnant en mode continu. Il est cependant nécessaire d'avoir une bonne compréhension des calculs mathématiques sous-jacents pour les utiliser correctement.

B.5.3 Approche par réseaux de Pétri et simulation de Monte Carlo

B.5.3.1 Principe de modélisation

Un moyen efficace de modéliser des systèmes dynamiques consiste à construire un automate d'état fini ayant un comportement aussi proche que possible de celui des systèmes E/E/PE relatifs à la sécurité étudiés. Les réseaux de Pétri (voir B.2.3.3 et B.6.6.10 de la CEI 61508-7) se sont révélés très efficaces à cet égard pour les raisons suivantes:

– ils sont faciles à traiter de manière graphique;

– la taille des modèles augmente de manière linéaire selon le nombre de composants à modéliser;

– ils sont très souples et permettent de modéliser pratiquement tous les types de contraintes;

– ils représentent un support parfait pour la simulation de Monte Carlo (voir B.6.6.8 de la CEI 61508-7).

Développés à l'origine dans les années soixante pour réaliser des essais formels sur des automates, ils ont rapidement été détournés en deux étapes par les fiabilistes, dans les années soixante-dix, pour la construction automatique de gros diagrammes de Markov et dans les années quatre-vingt, pour la simulation de Monte Carlo.

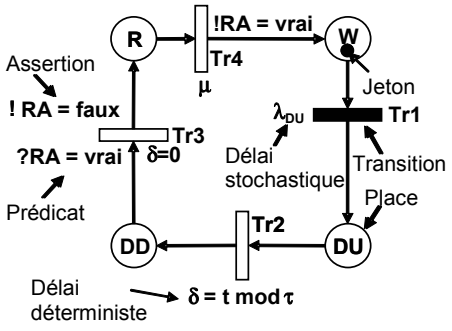


Figure B.33 – Réseau de Pétri pour modélisation d'un composant simple soumis à essai périodique

Le sous-réseau de Pétri type pour un composant simple soumis à essai périodique est constitué de trois parties:

1) la partie statique (c'est-à-dire un dessin):
   a) places (cercles) correspondant à des états potentiels;
   b) transitions (rectangles) correspondant à des événements potentiels;
   c) flèches ascendantes (des places vers les transitions) validant les transitions;
   d) flèches descendantes (des transitions vers les places) indiquant ce qui se passe en cas de déclenchement de transitions.
2) la partie ordonnancement:
   a) délais stochastiques représentant les délais aléatoires s'écoulant avant l'occurrence des événements;
   b) délais déterministes représentant les délais connus s'écoulant avant l'occurrence des événements.
3) la partie dynamique:
   a) jetons (petits cercles noirs) se déplaçant lorsque les événements se produisent pour indiquer les états potentiels réellement accomplis;
   b) prédicats (toute formule pouvant être vraie ou fausse) validant les transitions;

c) assertions (toute équation) mettant à jour certaines variables en cas de déclenchement d'une transition.

En outre, certaines règles permettent la validation et le déclenchement d'une transition:

4) validation d'une transition (c'est-à-dire, les conditions dans lesquelles l'événement correspondant peut survenir):
   a) toutes les places en amont ont au moins un jeton;
   b) tous les prédicats doivent être « vrai ».
5) déclenchement d'une transition (c'est-à-dire, ce qui se passe lorsque l'événement correspondant se produit):
   a) un jeton est retiré des places en amont;
   b) un jeton est ajouté dans les places en aval;
   c) les assertions sont mises à jour.

La plupart des notions relatives aux réseaux de Pétri sont présentées ci-dessus et les autres sont introduites si nécessaire.

B.5.3.2 Principe de la simulation de Monte Carlo

La simulation de Monte Carlo consiste à animer des modèles de comportement au moyen de nombres aléatoires pour évaluer le temps pendant lequel le système reste dans les états régis par des délais aléatoires ou déterministes (voir également B.6.6.8 de la CEI 61508-7).

Ceci peut être expliqué en utilisant le réseau de Pétri présenté à la Figure B.33:

– Au début le jeton est à la place *W* et le composant est en bon ordre de fonctionnement.
– Un seul événement peut se produire à partir de cet état - une défaillance dangereuse non détectée - (la transition *Tr1* est valide et tracée en noir).
– Le temps écoulé dans cet état est stochastique et régi par une distribution exponentielle du paramètre λ_{DU}. La simulation de Monte Carlo consiste à déclencher un nombre aléatoire (voir ci-après) pour calculer le délai *d1* avant l'occurrence de la défaillance (c'est-à-dire *Tr1* est en cours de déclenchement).
– Lorsque *d1* est écoulé, *Tr1* est déclenchée et le jeton se déplace vers la place *DU* (plus précisément, un jeton est retiré de la place *W* et un jeton est ajouté à la place *DU*).
– Le composant atteint l'état dangereux non détecté et la transition *Tr2* devient valide.
– La défaillance dangereuse est détectée après un délai déterministe *d2* (*d*2 = *t modulo* τ lorsque *t* est le temps réel et τ l'intervalle entre essais). Ceci simule l'intervalle entre essais.
– Lorsque *t*2 est écoulé, c'est-à-dire lorsque la défaillance dangereuse est détectée, le jeton entre dans la place *DD*. Le composant est à présent en attente de réparation et *Tr*3 devient valide.
– Le délai *d*3 pour le déclenchement de *Tr*3 (début de la réparation) ne dépend pas du composant lui-même mais de la disponibilité des ressources de réparation représentées par le message *RA*. Ceci est régi par l'occurrence des événements dans une autre partie du réseau de Pétri dans son ensemble non représentée à la Figure B.33.
– La réparation commence dès que l'équipe de réparation est disponible (c'est-à-dire que le prédicat *?RA = true* devient vrai) et le jeton entre dans la place *R*. Les ressources de réparation sont immédiatement indisponibles pour une autre intervention et l'assertion *!RA = false* est utilisée pour mettre à jour la valeur de *RA*. Ceci évite toute autre réparation en même temps.
– La transition stochastique *Tr*4 (c'est-à-dire la fin de la réparation) devient valide et le délai *d4* peut être calculé en déclenchant un nombre aléatoire selon le taux de réparation μ.

– Lorsque *d*4 est écoulé, *Tr*4 est déclenchée et le composant revient à son état de bon fonctionnement (le jeton entre dans la place *W*). Les ressources de réparation sont de nouveau disponibles et *RA* est mis à jour par l'assertion *!RA = true*.
– Et ainsi de suite... tant que le déclenchement de la transition valide suivante appartient à la période considérée *[0, T]*.

Lorsque le déclenchement suivant n'est plus dans la période *[0, T]*, la simulation est arrêtée et une histoire du composant est obtenue. Pendant le déroulement de l'histoire, les paramètres pertinents peuvent être enregistrés, comme le marquage moyen des places (c'est-à-dire le rapport du temps écoulé avec un jeton dans la place pendant la durée T), les fréquences de déclenchement de transition, le temps écoulé jusqu'à la première occurrence d'un événement donné, etc.

Le principe de la simulation de Monte Carlo est de réaliser un grand nombre d'histoires et d'appliquer des statistiques classiques aux résultats afin d'évaluer les paramètres pertinents.

A l'inverse des calculs analytiques, la simulation de Monte Carlo permet d'associer facilement les délais déterministes et aléatoires qui peuvent être simulés à partir de leur distribution de probabilité cumulée *F(d)* et nombres aléatoires z_i distribués de manière uniforme sur *[0, 1]*. Ces nombres aléatoires sont disponibles dans pratiquement tous les langages de programmation et des algorithmes puissants existent à cet effet.

Un échantillon (d_i), distribué selon *F(d),* est ensuite obtenu à partir d'un échantillon (z_i) par l'opération: $d_i = F^{-1}(z_i)$. Ceci est très facile à réaliser lorsque la formule analytique de $F^{-1}(z)$ est disponible sous la forme, par exemple, de délais distribués de manière exponentielle: $d_i = -\frac{1}{\lambda_{DU}} Log(z_i)$.

S'agissant de l'exactitude des calculs relatifs à un paramètre simulé donné *X*, les statistiques de base permettent de calculer facilement la moyenne, la variance, l'écart type et la confiance de l'échantillon (X_i) simulé:

– moyenne: $\overline{X} = \frac{\sum_i x_i}{N}$
– variance: $\sigma^2 = \frac{\sum_i (x_i - \overline{X})^2}{N}$ et écart type: σ
– intervalle de confiance de 90 % autour de $\overline{X}$: $Conf = 1{,}64 \frac{\sigma}{\sqrt{N}}$

Par conséquent, l'utilisation de la simulation de Monte Carlo permet de toujours estimer l'exactitude des résultats. Par exemple, considérons 90 % de chance que le résultat vrai $\hat{X}$ appartient à l'intervalle $\left[\overline{X} - 1{,}64\sigma / \sqrt{N},\quad \overline{X} + 1{,}64\sigma / \sqrt{N}\right]$.

Cet intervalle est réduit lorsque le nombre d'histoires augmente et lorsque la fréquence d'occurrence de *X* augmente.

Les ordinateurs personnels actuels permettent de réaliser les calculs sans réelle difficulté, même pour des systèmes E/E/PE relatifs à la sécurité de niveau SIL 4.

B.5.3.3 Principe des calculs de *PFD*

Le sous-réseau de Pétri de la Figure B.33 peut être utilisé pour évaluer directement la PFD_{avg} du composant dans la mesure où le marquage moyen de la place *W* qui est égal au rapport du

temps écoulé dans *W* (c'est-à-dire avec *W* marquée par un jeton) à la durée *T*, représente en fait la disponibilité moyenne *A* du composant. On obtient $PFD_{avg} = 1 - A$.

L'exactitude du calcul peut être estimée comme expliqué ci-dessus.

Des comportements plus complexes peuvent être représentés en utilisant des sous-réseaux de Pétri spécifiques. La Figure B.34 donne un exemple d'application de la modélisation de composants soumis à essais périodiques, de défaillances de cause commune (CCF) et de ressources de réparation.

La partie gauche présente la modélisation d'un composant soumis à essais périodiques qui passe par les états en fonctionnement (*W*), défaillance dangereuse non détectée (*DU*), en essai (DUT), défaillance dangereuse détectée (*DD*), prêt pour réparation (*RR*) et en réparation (*R*).

En cas de défaillance (*DU*), le message *!-Ci* (équivalent à *!Ci = false*) est émis pour informer de la défaillance du composant. Il attend ensuite jusqu'au début d'un essai périodique (DUT). L'intervalle entre essais périodiques est τ et le décalage θ. L'essai est alors réalisé pendant une durée égale à π et l'état *DD* est atteint. Si une pièce de rechange est disponible (au moins un jeton en *SP*), le composant passe à l'état prêt pour réparation (*RR*) et la variable *NbR* est augmentée de 1 pour informer les ressources de réparation du nombre de composants devant être réparés. Lorsque les ressources de réparation sont en place (un jeton en *OL*), la réparation commence (*R*) et le jeton est retiré de *OL*. A l'issue de la réparation, le composant revient à l'état de bon fonctionnement, le message *!Ci* est émis (c'est-à-dire !*Ci = true*), *NbR* est réduite de 1 et le jeton est remis en *OL* pour permettre des réparations ultérieures. Et ainsi de suite.

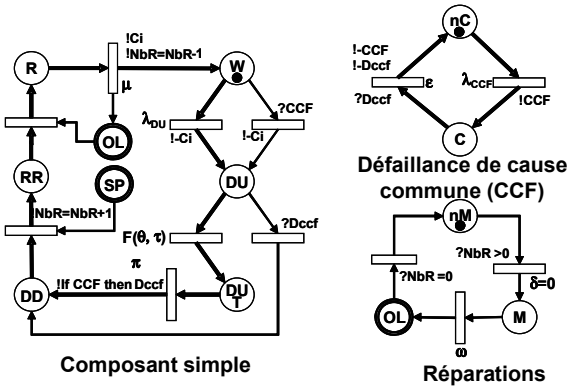


Figure B.34 – Réseau de Pétri pour modélisation de défaillance de cause commune et des ressources de réparation

La variable *NbR* est utilisée par le sous-réseau de Pétri dédié aux réparations. Lorsqu'elle devient positive, la mobilisation des ressources commence (*M*) et après un certain délai, elles sont prêtes à fonctionner à la place (*OL*). Le jeton en *OL* est utilisé pour valider le début de la réparation d'un composant défaillant. Par conséquent, il n'est possible de ne réaliser qu'une seule réparation en même temps. Lorsque toutes les réparations sont réalisées (c'est-à-dire *NbR* = 0), les ressources de réparation sont démobilisées.

La Figure B.34 présente également la modélisation d'une défaillance de cause commune (CCF). Lorsqu'elle se produit (λ_{DCC}), le message *!CCF* devient vrai et est utilisé pour mettre tous les composants affectés dans leurs états *DU*. Les messages pertinents C_i deviennent faux et les composants sont réparés indépendamment les uns des autres. A l'issue de l'essai d'un

composant, l'assertion *!IF CCF then Dccf* permet d'informer tous les autres composants qu'une DCC a été détectée. Ce message est utilisé pour les mettre immédiatement dans leurs états *DD*. Ce message est également utilisé pour réinitialiser le sous-réseau de Pétri pour CCF mais ceci n'est réalisé qu'après un certain temps (ε) pour garantir que tous les composants ont été mis dans leur état *DD* avant la réinitialisation.

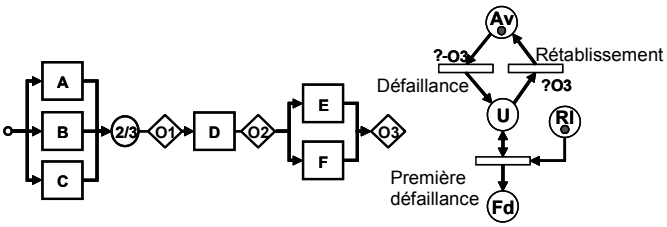


Figure B.35 – Utilisation des diagrammes de fiabilité pour construire le réseau de Pétri et le réseau de Pétri auxiliaire pour les calculs de *PFD* et de *PFH*

Les sous-réseaux de Pétri de la Figure B.34 sont destinés à être utilisés comme parties de modèles plus complexes. La Figure B.35 en donne une utilisation qui reprend le diagramme de fiabilité de la Figure B.16 qui a été légèrement adapté avec l'introduction des sorties intermédiaires *Oi*.

Les composants A, B, C, D, E, F peuvent être modélisés par un ensemble de sous-réseaux de Pétri tels que ceux représentés à la Figure B.34 avec, par exemple, une CCF pour (A, B, C) et une autre pour (E, F), et les mêmes ressources de réparation pour tous les composants. Il reste à résoudre le problème de la liaison des composants entre eux selon la logique du diagramme de fiabilité et de calculer la PFD_{avg} considérée.

La liaison des composants est très simple à réaliser en utilisant les messages C_i et en construisant les assertions suivantes:

- $O_1 = C_a.C_b + C_a.C_c + C_b.C_c$
- $O_2 = O_1.C_d$
- $O_3 = O_2.(C_e + C_f)$

Par conséquent, lorsque O_3 est vrai, le système E/E/PE relatif à la sécurité complet fonctionne correctement et il est indisponible dans les autres cas. Ce message est utilisé dans le sous-réseau de Pétri du côté droit afin de modéliser les différents états des systèmes E/E/PE relatifs à la sécurité: disponible (*Av*), indisponible (*U*), fiable (*RI*) et non fiable (*Fd*).

Pour le calcul de *PFD,* ne sont pris en compte que *Av* et *U:* lorsque O_3 devient faux, le système est défaillant et passe à l'état indisponible et lorsque O_3 devient vrai, le système est rétabli et repasse à l'état disponible. Ceci est très simple et le marquage moyen de *Av* est la disponibilité moyenne du système et le marquage moyen de *U* est son indisponibilité moyenne, c'est-à-dire sa PFD_{avg}.

Par conséquent, la simulation de Monte Carlo réalise automatiquement l'intégrale de l'indisponibilité instantanée qu'il n'est donc pas nécessaire de calculer sauf si la courbe en dents de scie est souhaitée. Ceci serait facilement réalisé en évaluant le marquage moyen de *U* à un moment donné plutôt que sur toute la période *[0, T]*.

La présentation faite ci-dessus n'est qu'une illustration des grandes lignes de l'utilisation des réseaux de Pétri pour des calculs de SIL mais les possibilités de modélisation potentielle sont virtuellement infinies.

B.5.3.4 Principe des calculs de *PFH*

Pour le calcul de *PFH,* les principes sont exactement les mêmes que ceux indiqués précédemment et les mêmes sous-modèles peuvent être utilisés pour les défaillances DU. La Figure B.36 illustre un sous-réseau de Pétri modélisant une défaillance DD qui est détectée et réparée dès que possible.

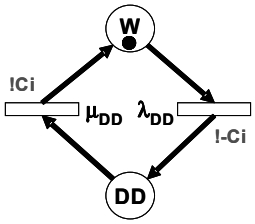


Figure B.36 – Réseau de Pétri simple pour un composant simple avec défaillances détectées et réparations

Ces modèles de composants peuvent être utilisés comme expliqué ci-dessus en relation avec un diagramme de fiabilité représentant tout le système tel qu'illustré à la Figure B.35.

Lorsque le système E/E/PE relatif à la sécurité fonctionnant en mode continu constitue la dernière barrière de sécurité, un accident se produit dès qu'il est défaillant et la *PFH* doit être évaluée au moyen de la fiabilité du système. Ceci est réalisé par la partie inférieure du sous-réseau de Pétri représentée du côté droit de la Figure B.35: la fréquence moyenne de la première défaillance du système sur la période *[0, T]* représente sa non fiabilité *F(T)*. Ensuite, lorsque *F(T)* est courte par rapport à 1, et selon la définition de *PFH*, on obtient *PFH* = *F(T)/T*.

Du fait que le jeton est en *RI*, la première défaillance est une transition en un seul passage. A condition que toutes les histoires donnent lieu à une défaillance (c'est-à-dire, T est suffisamment long), le temps moyen écoulé avec un jeton en *RI* est le *MTTF* du système. Alors, *PFH* ≈ 1/*MTTF* donne une limite supérieure de *PFH*.

Lorsque le système E/E/PE relatif à la sécurité fonctionnant en mode continu ne constitue pas la dernière barrière de sécurité, sa défaillance ne provoque pas directement un accident. Il est alors réparé après une défaillance globale et sa *PFH* doit être calculée au moyen de l'indisponibilité du système. Elle est obtenue directement à partir de la fréquence *Nbf* de la défaillance de transition. Ceci donne la durée de la défaillance du système sur une période donnée, par conséquent on obtient *PFH(T)* = *Nbf/T*.

Il est intéressant de noter que lorsque *T* est suffisamment long, le *MUT* peut être calculé par le temps de séjour moyen cumulé MCT_{Av} à l'état *Av* et le *MDT* par le temps de séjour moyen cumulé MCT_U à l'état *U*. Les temps de séjour moyens cumulés MCT_A et MCT_U sont très simples à calculer dans le cadre de la simulation de Monte Carlo et ce en cumulant tout simplement les temps pendant lesquels un jeton est présent en *Av* ou en *U*. On obtient $MUT = MCT_A / Nbf$ et $MUT = MCT_u / Nbf$. Ceci peut être utilisé pour évaluer *PFH* = 1/*(MUT* + *MDT)* = 1/*MTBF* = *Nbf/T.*

Tous ces résultats sont obtenus directement car la simulation de Monte Carlo fournit normalement les valeurs moyennes. La présentation faite ci-dessus n'est qu'une illustration des grandes lignes de l'utilisation des réseaux de Pétri pour des calculs de SIL mais les possibilités de modélisation potentielle sont virtuellement infinies.

B.5.4 Autres approches

La relation entre la taille des modèles et le nombre de composants du système étudié varie énormément en fonction du type d'approche utilisé. Elle est linéaire pour les arbres de panne et les réseaux de Pétri mais exponentielle pour les processus de Markov. Par conséquent, les

approches par arbre de panne et réseau de Pétri facilitent grandement le traitement de systèmes beaucoup plus importants contrairement à l'approche de Markov. C'est la raison pour laquelle les réseaux de Pétri sont parfois utilisés pour produire des diagrammes de Markov de grande taille.

Les langages formels sous-jacents aux représentations graphiques décrites ci-dessus produisent des modèles plats: chaque composant est décrit séparément, au même niveau. De ce fait, les modèles de grande taille sont parfois difficiles à maîtriser et à maintenir. Un moyen de pallier ce problème consiste à utiliser des langages structurés fournissant des modèles hiérarchiques compacts. Plusieurs langages formels de ce type ont été récemment développés et certains progiciels sont disponibles. On peut citer par exemple le langage AltaRica Data Flow publié en 2000 destiné à être librement utilisé dans le domaine de la fiabilité et conçu pour modéliser avec exactitude les propriétés fonctionnelles et dysfonctionnelles des systèmes industriels (voir références en B.7).

La Figure B.37 est équivalente au diagramme de fiabilité représenté à la Figure B.1. Ce modèle est hiérarchique car les modules simples ne sont modélisés qu'une seule fois, puis réutilisés autant de fois que nécessaire au niveau du système (c'est-à-dire dans le nœud principal). Ceci permet de réaliser des modèles très compacts.

Pour des raisons de simplification de la présentation, deux transitions seulement sont représentées pour les composants: défaillance et réparation (c'est-à-dire, défaillances DD détectées et réparées dès leur occurrence).

Les opérateurs logiques (*or*, *and*) (ou, et) sont utilisés pour décrire la logique du système. Ceci est réalisé en relation directe avec le diagramme de fiabilité et le flux Out modélise l'état du système: il fonctionne lorsque *Out* est *true* (vrai) et il est défaillant lorsque *Out* est *false* (faux).

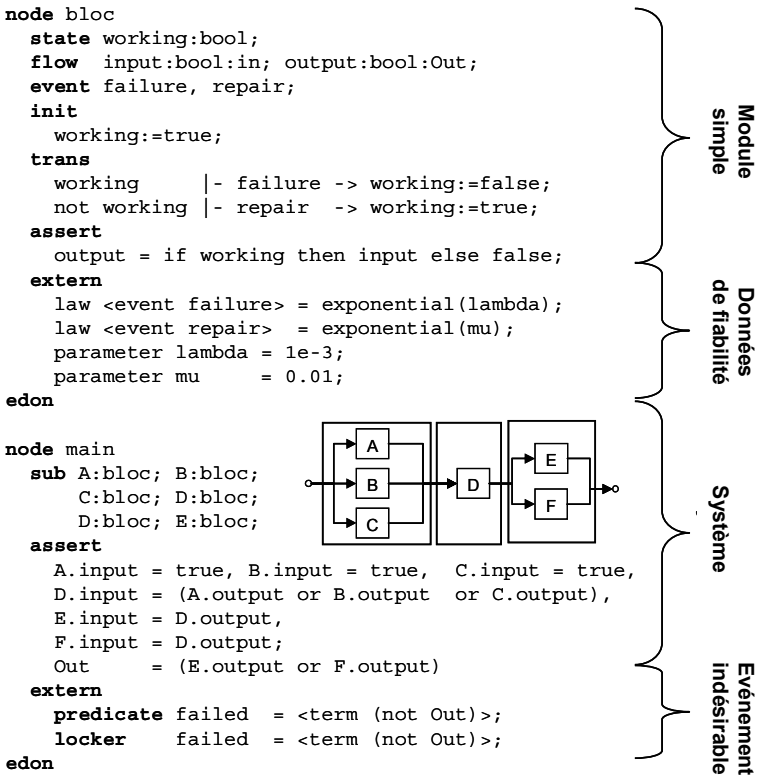


Figure B.37 – Exemple de modélisation fonctionnelle et dysfonctionnelle avec un langage formel

Ceci fournit de bons modèles de comportement pour une simulation de Monte Carlo efficace. Tous les éléments décrits ci-dessus pour le réseau de Pétri s'appliquent également dans ce cas pour les calculs de PFD_{avg} ou de *PFH*. Par conséquent, ce cas n'est pas développé plus en détail.

Ce langage formel possède des propriétés mathématiques similaires à celles des réseaux de Pétri, ce qui permet de compiler un modèle vers un autre sans aucune difficulté. Il généralise également les propriétés des langages sous-jacents aux arbres de panne ou aux processus de Markov. Par conséquent, sous réserve que la description ait été limitée aux propriétés des processus de Markov ou des arbres de panne, il est possible de compiler le modèle dans des diagrammes de Markov ou arbres de panne équivalents. Les mots clé "predicate" et "locker" à la fin du modèle fournissent des directives pour la génération des arbres de panne ou les modèles markoviens ainsi que pour la simulation de Monte Carlo directe.

L'utilisation d'un langage formel conçu pour modéliser correctement le comportement du système tant du point de vue fonctionnel que dysfonctionnel, permet de réaliser les opérations suivantes:

– Les simulations de Monte Carlo à réaliser directement sur les modèles;
– Les diagrammes de Markov à générer et les calculs analytiques à réaliser comme indiqué précédemment (lorsque le langage a été limité aux propriétés de Markov);
– Les arbres de panne équivalents à générer et les calculs analytiques à réaliser comme indiqué précédemment (lorsque le langage a été limité aux propriétés booléennes).

Ces langages formels fonctionnels et dysfonctionnels sont d'usage général. Leur utilisation ne pose aucun problème dans le cas particulier des systèmes E/E/PE relatifs à la sécurité. Ils constituent un moyen efficace de maîtriser les calculs de PFD_{avg} et de *PFH* des systèmes E/E/PE relatifs à la sécurité en présence de plusieurs couches de protection, divers types de modes de défaillance, des modèles d'essai périodique complexes, des dépendances de composants, des ressources de maintenance, etc., c'est-à-dire, lorsque les autres méthodes ont montré qu'elles avaient atteint leurs limites.

B.6 Traitement des incertitudes

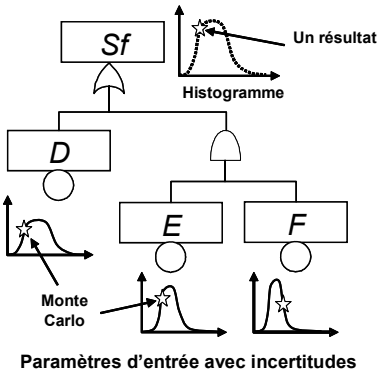


Figure B.38 – Principe de la propagation de l'incertitude

L'un des principaux problèmes posés par la réalisation de calculs probabilistes est lié aux incertitudes associées aux paramètres de fiabilité. Par conséquent, pour les calculs de *PFD* ou de *PFH*, il est utile d'évaluer l'effet correspondant sur l'incertitude des résultats.

Pour traiter cette question des précautions doivent être prises, l'utilisation de la simulation de Monte Carlo constituant à cet égard un moyen efficace pour résoudre le problème, comme illustré à la Figure B.38.

Sur cette figure, les paramètres de fiabilité d'entrée (par exemple, les taux de défaillances dangereuses non détectées) ne sont plus valables, ils sont donc remplacés par des variables aléatoires. La densité de probabilité de cette variable aléatoire est plus ou moins prononcée ou plate selon le degré d'incertitude: la densité de probabilité de F est plus prononcée que celle de E ou de D, ce qui indique que F présente une incertitude moindre que pour E ou D, par exemple.

Le principe du calcul est le suivant:

1) génération d'un ensemble de paramètres d'entrée au moyen de nombres aléatoires selon les distributions probabilistes de ces paramètres (similaire aux explications données en B.3.2);
2) réalisation du calcul en utilisant l'ensemble généré de paramètres d'entrée ci-dessus;
3) enregistrement du résultat de sortie (ceci constitue une valeur utilisée à l'étape 4);
4) réalisation toujours renouvelée des étapes 1 à 3 jusqu'à l'obtention d'un nombre suffisant de valeurs (par exemple 100 ou 1 000) afin de constituer un histogramme (ligne en pointillé à la Figure B.38);
5) analyse statistique de cet histogramme pour obtenir la moyenne et l'écart type du résultat de sortie.

La moyenne de cet histogramme est la PFD_{avg} ou la *PFH* selon le type de calcul réalisé, et l'écart type mesure l'incertitude sur ces résultats. Plus l'écart type est petit, plus le calcul de PFD_{avg} ou de *PFH* est précis.

Le principe illustré sur l'arbre de panne est très général et peut être appliqué à n'importe laquelle des méthodes de calcul spécifiées dans la présente annexe: formules simplifiées, processus de Markov, voire approches par réseaux de Pétri ou en langages formels. Lorsque le calcul a déjà été réalisé par simulation de Monte Carlo, une simulation de Monte Carlo en deux étapes doit être utilisée.

La distribution probabiliste pour un paramètre de fiabilité d'entrée donné doit être choisie en fonction de la connaissance acquise en la matière. Il peut s'agir:

– d'une distribution uniforme entre les limites inférieure et supérieure;
– d'une distribution triangulaire avec la valeur la plus probable;
– d'une loi log-normale avec un facteur d'erreur donné;
– d'une loi de Khi-Deux, etc.

Les premières distributions peuvent être évaluées par raisonnement théorique lorsque le retour d'expérience est insuffisant. Les dernières distributions peuvent être utilisées lorsque le retour d'expérience est plus conséquent car ce dernier fournit des valeurs moyennes de paramètre ainsi que les intervalles de confiance sur ces valeurs moyennes.

Par exemple, si *n* défaillances ont été observées sur un temps d'observation cumulé *T*, on obtient:

– $\hat{\lambda} = n/T$ est l'estimateur de probabilité maximum du taux de défaillance

– $\lambda_{Inf,\alpha} = \frac{1}{2T}\chi^2_{(1-\alpha),2n}$ limite inférieure avec une probabilité α % inférieure à $\lambda_{\text{Inf},\alpha}$

– $\lambda_{Sup,\alpha} = \frac{1}{2T}\chi^2_{\alpha,2(n+1)}$ limite supérieure avec une probabilité α % supérieure à $\lambda_{\text{Sup},\alpha}$

Lorsque α = 5 %, la valeur vraie de λ a alors 90 chances sur 100 d'appartenir à l'intervalle $[\lambda_{\text{Inf},\alpha}, \lambda_{\text{Sup},\alpha}]$. Plus cet intervalle est petit, plus la valeur vraie de λ est sûre. Normalement, les bonnes bases de données de fiabilité fournissent ces informations. Il convient cependant

que les analystes considèrent avec une grande prudence les données de fiabilité fournies sans intervalle de confiance (ou les informations permettant de les calculer).

Les valeurs de $\hat{\lambda}$, $\lambda_{\mathrm{Inf},\alpha}$ et $\lambda_{\mathrm{Sup},\alpha}$ peuvent être utilisées pour générer une distribution appropriée permettant de modéliser le taux de défaillance λ d'un mode de défaillance donné et ses incertitudes. Ceci est évident pour la distribution χ^2 mais la loi log-normale s'est révélée très efficace à cet égard. Une loi log-normale de ce type est définie par sa moyenne $\hat{\lambda}$ ou sa valeur médiane $\lambda_{50\ \%}$ et par son facteur d'erreur.

Cette loi présente une propriété très intéressante: $\lambda_{\mathrm{Inf},\alpha} = \lambda_{50\ \%}/ef_{\alpha}$ et $\lambda_{\mathrm{Sup},\alpha} = \lambda_{50\ \%}.ef_{\alpha}$.

Elle est ensuite définie par seulement deux paramètres: $\hat{\lambda}$ *and* $ef_{\alpha} \approx \sqrt{\frac{\lambda_{Sup,\alpha}}{\lambda_{Inf,\alpha}}}$

Lorsque $ef_{\alpha} = 1$, il n'y a pas d'incertitudes, lorsque $ef_{\alpha} = 3{,}3$, il existe un facteur d'environ 10 entre les limites de confiance inférieure et supérieure, etc.

Ces lois peuvent à leur tour être utilisées dans les simulations de Monte Carlo afin de tenir compte des effets des valeurs moyennes et des incertitudes sur PFD_{avg} ou *PFH*. Par conséquent, il est toujours possible de maîtriser les incertitudes dans le cadre des calculs probabilistes. Certains progiciels mettent directement en œuvre ce type de calculs.

S'agissant de l'analyse de systèmes redondants, il convient de tenir compte non seulement de l'incertitude du taux de défaillance de l'élément de base mais également de l'exactitude du taux de défaillance CCF. Même lorsque les données de retour d'expérience sont suffisamment fiables pour chacun des éléments, les données d'expérience CCF sont rarement suffisantes ce qui constitue de ce fait la plus grande source d'incertitude.

B.7 Références

Voir les références [4] à [9] et [22] à [24] dans la Bibliographie pour des détails complémentaires sur l'évaluation des probabilités de défaillance.

Annexe C
(informative)

Calcul de la couverture de diagnostic et de la proportion de défaillance en sécurité – exemple élaboré

Une méthode de calcul de la couverture de diagnostic et de la proportion de défaillance en sécurité est donnée à l'Annexe C de la CEI 61508-2. La présente annexe décrit de manière concise l'utilisation de cette méthode pour calculer la couverture de diagnostic. On suppose que toutes les informations données dans la CEI 61508-2 sont disponibles et ont été utilisées pour obtenir les valeurs indiquées dans le Tableau C.1. Le Tableau C.2 donne les limites de la couverture de diagnostic qui peuvent être revendiquées pour certains éléments de systèmes E/E/PE relatifs à la sécurité. Les valeurs du Tableau C.2 se fondent sur un raisonnement théorique.

Pour comprendre toutes les valeurs du Tableau C.1, un schéma détaillé du matériel est nécessaire pour permettre de déterminer l'effet de tous les modes de défaillance. Ces valeurs ne sont données qu'à titre d'exemple, et certains composants du Tableau C.1 ne supportent pas de couverture de diagnostic car il est pratiquement impossible de détecter tous les modes de défaillance pour tous les composants.

Le Tableau C.1 a été déterminé comme suit:

a) Une analyse de mode de défaillance et de leurs effets a été effectuée pour déterminer l'effet de chaque mode de défaillance pour chaque composant sur le comportement du système sans essai de diagnostic. Les proportions du taux global de défaillance associées à chaque mode de défaillance sont indiquées pour chaque composant, et entre défaillances non dangereuses (S) et défaillances dangereuses (D). La répartition entre défaillances non dangereuses et défaillances dangereuses peut être déterministe pour des composants simples, et dans le cas contraire elle se fonde sur un raisonnement théorique. Pour des composants complexes, dont il n'est pas possible d'effectuer une analyse détaillée de chaque mode de défaillance, une répartition des défaillances en 50 % de non dangereuses et 50 % de dangereuses est généralement acceptée. Pour ce tableau, les modes de défaillance donnés dans la référence a) ont été utilisés, bien que d'autres répartitions entre modes de défaillance soient réalisables et éventuellement souhaitables.

b) La couverture de diagnostic pour chaque essai de diagnostic spécifique réalisé sur chaque composant est donnée (dans la colonne intitulée «DC_{comp}»). Des couvertures de diagnostic spécifiques sont données pour la détection des deux types de défaillance, non dangereuse et dangereuse. Bien qu'il soit montré que des défaillances de circuit ouvert ou de court-circuit pour composants simples (par exemple des résistances, des condensateurs et des transistors) sont détectées avec une couverture de diagnostic spécifique de 100 %, l'utilisation du Tableau C.2 limite à 90 % la couverture de diagnostic pour l'élément U16, composant complexe de type B.

c) Les colonnes (1) et (2) indiquent les taux de défaillances en sécurité et dangereuses, en l'absence d'essais de diagnostic, pour chaque composant (respectivement λ_S et λ_{DD} + λ_{DU}).

d) On peut considérer une défaillance dangereuse détectée comme étant en fait une défaillance en sécurité et ainsi définir la répartition entre défaillances effectivement non dangereuses (c'est-à-dire les défaillances non dangereuses détectées, soit non dangereuses non détectées, soit les défaillances dangereuses détectées) et les défaillances dangereuses non détectées. Le taux de défaillances effectivement en sécurité est calculé en multipliant le taux de défaillances dangereuses par la couverture de diagnostic spécifique pour une défaillance dangereuse et en additionnant le résultat obtenu au taux de défaillances en sécurité (voir colonne (3)). De la même manière, le taux de défaillances dangereuses non détectées est calculé en soustrayant la couverture de diagnostic spécifique pour défaillances dangereuses de un et en multipliant le résultat obtenu par le taux de défaillances dangereuses (voir colonne (4)).

e) La colonne (5) donne le taux de défaillances en sécurité détectées et la colonne (6) donne le taux de défaillances dangereuses détectées, calculées en multipliant la couverture de diagnostic spécifique respectivement par le taux de défaillances en sécurité et par le taux de défaillances dangereuses.

f) Ce tableau produit les résultats suivants:

– taux global de défaillance en sécurité $\sum \lambda_S + \sum \lambda_{Dd} = 9{,}9 \times 10^{-7}$
(y compris défaillances dangereuses détectées)

– taux global de défaillances dangereuses non détectées $\sum \lambda_{Du} = 5{,}1 \times 10^{-8}$

– taux global de défaillance $\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du} = 1{,}0 \times 10^{-6}$

– taux global de défaillances en sécurité non détectées $\sum \lambda_{Su} = 2{,}7 \times 10^{-8}$

– couverture de diagnostic pour des défaillances en sécurité $\dfrac{\sum \lambda_{Sd}}{\sum \lambda_S} = \dfrac{3{,}38}{3{,}65} = 93\ \%$

– couverture de diagnostic des défaillances dangereuses
$\dfrac{\sum \lambda_{Dd}}{\sum \lambda_{Dd} + \sum \lambda_{Du}} = \dfrac{6{,}21}{6{,}72} = 92\ \%$ (en général simplement désignée par l'expression «couverture de diagnostic»)

– proportion de défaillances en sécurité $\dfrac{\sum \lambda_S + \sum \lambda_{Dd}}{\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}} = \dfrac{986}{365 + 672} = 95\ \%$

g) La répartition du taux de défaillance sans essai de diagnostic est de 35 % de défaillances en sécurité et de 65 % de défaillances dangereuses.

Tableau C.1 – Exemples de calcul de la couverture de diagnostic et de la proportion de défaillances en sécurité

Elément	n°	Type	Répartition entre défaillances en sécurité et dangereuses pour chaque mode de défaillance								Répartition entre défaillances en sécurité et dangereuses dans le cas d'une couverture de diagnostic et calcul des taux de défaillance ($\times 10^{-9}$)							
			OC		SC		Ecart		Fonction		DC_{comp}		(1)	(2)	(3)	(4)	(5)	(6)
			S	D	S	D	S	D	S	D	S	D	λ_S	$\lambda_{DD}+\lambda_{DU}$	$\lambda_S+\lambda_{DD}$	λ_{DU}	λ_{SD}	λ_{DD}
Print	1	Print	0,5	0,5	0,5	0,5	0	0	0	0	0,99	0,99	11,0	11,0	21,9	0,1	10,9	10,9
CN1	1	Con96pin	0,5	0,5	0,5	0,5					0,99	0,99	11,5	11,5	22,9	0,1	11,4	11,4
C1	1	100nF	1	0	1	0	0	0	0	0	1	0	3,2	0,0	3,2	0,0	3,2	0,0
C2	1	10µF	0	0	1	0	0	0	0	0	1	0	0,8	0,0	0,8	0,0	0,8	0,0
R4	1	1M	0,5	0,5	0,5	0,5					1	1	1,7	1,7	3,3	0,0	1,7	1,7
R6	1	100k									0	0	0,0	0,0	0,0	0,0	0,0	0,0
OSC1	1	OSC24 MHz	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	1	16 0	16,0	32,0	0,0	16,0	16,0
U8	1	74HCT85	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U16	1	MC68000-12	0	1	0	1	0,5	0,5	0,5	0,5	0,90	0,90	260,4	483,6	695,6	48,4	234,4	435,2
U26	1	74HCT74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U27	1	74F74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	14,4	14,4	28,7	0,1	14,3	14,3
U28	1	PAL16L8A	0	1	0	1	0	1	0	1	0,98	0,98	0,0	88,0	86,2	1,8	0,0	86,2
T1	1	BC817	0	0	0	0,67	0	0,5	0	0	1	1	0,0	0,2	0,4	0,0	0,0	0,2
Total													365	672	986	50,9	338	621

NOTE Aucun des modes de défaillance de l'élément R6 n'est détecté, mais une défaillance donnée n'affecte ni la sécurité ni la disponibilité.

Légende

S	Défaillance en sécurité
D	Défaillance dangereuse
OC	Circuit ouvert
SC	Court-circuit
Ecart	Modification de valeur
Fonction	Défaillances fonctionnelles
DC_{comp}	Couverture de diagnostic spécifique pour le composant

Voir également le Tableau B.1, bien que les taux de défaillance y soient donnés pour chacun des composants concernés plutôt que pour chaque composant dans un canal.

Tableau C.2 – Couverture de diagnostic et efficacité pour différents éléments

Composant	Couverture de diagnostic faible	Couverture de diagnostic moyenne	Couverture de diagnostic élevée
CPU (voir Note 3) - Unité centrale	total inférieur à 70 %	total inférieur à 90 %	
registre, RAM (mémoire vive interne)	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
codage et exécution y compris les registres d'indicateurs (voir Note 3)	50 % - 60 %	75 % - 95 %	-
	50 % - 70 %	85 % - 98 %	-
calcul d'adresse (voir Note 3)	50 % - 60 %	60 % - 90 %	85 % - 98 %
registre d'adresse d'instruction, pointeur de pile	50 % - 70 %		
	40 % - 60 %		
Bus			
unité de gestion de la mémoire	50 %	70 %	90 % - 99 %
arbitrage du bus	50 %	70 %	90 % - 99 %
Traitement des interruptions	40 % - 60 %	60 % - 90 %	85 % - 98 %
Horloge (quartz) (voir Note 4)	50 %	-	95 % - 99 %
Surveillance du programme			
temporelle (voir Note 3)	40 % - 60 %	60 % - 80 %	-
logique (voir Note 3)	40 % - 60 %	60 % - 90 %	-
temporelle et logique (voir Note 5)	-	65 % - 90 %	90 % - 98 %
Mémoire invariable	50 % - 70 %	99 %	99,99 %
Mémoire variable	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
Matériel discret			
E/S numériques	70 %	90 %	99 %
E/S analogiques	50 % - 60 %	70 % - 85 %	99 %
alimentation	50 % - 60 %	70 % - 85 %	99 %
Communication et mémoire de masse	90 %	99,9 %	99,99 %
Dispositifs électromécaniques	90 %	99 %	99,9 %
Capteurs	50 % - 70 %	70 % - 85 %	99 %
Eléments finaux	50 % - 70 %	70 % - 85 %	99 %

NOTE 1 Il convient de lire ce tableau conjointement avec le Tableau A.1 de la CEI 61508-2 qui fournit les modes de défaillance à prendre en compte.

NOTE 2 Lorsqu'une plage de couverture de diagnostic est donnée, les limites supérieures de l'intervalle ne peuvent être établies que pour des moyens de surveillance à tolérance étroite, ou pour des mesures d'essai qui appliquent une contrainte dynamique élevée sur la fonction à soumettre à essai.

NOTE 3 Pour les techniques n'ayant pas de valeur élevée de couverture de diagnostic, il n'existe pas à l'heure actuelle de mesures et techniques hautement efficaces connues.

NOTE 4 Il n'existe pas à l'heure actuelle de mesures et techniques de moyenne efficacité pour les horloges à quartz.

NOTE 5 La couverture de diagnostic minimale pour une combinaison de surveillance de déroulement de programme temporelle et logique est d'efficacité moyenne.

Voir les références [10] à [12] de la Bibliographie.

Annexe D
(informative)

Méthodologie permettant de quantifier l'effet des défaillances de cause commune du matériel dans des systèmes E/E/PE

D.1 Généralités

D.1.1 Introduction

La présente norme inclut un certain nombre de mesures ayant trait aux défaillances systématiques. Toutefois, quelle que soit la qualité d'application de ces mesures, il existe une probabilité résiduelle d'apparition de défaillances systématiques. Bien que cela n'affecte pas de manière significative les calculs de fiabilité pour les systèmes à un canal unique, le potentiel de défaillance pouvant affecter plus d'un canal sur des systèmes à plusieurs canaux (ou plusieurs composants dans un système de sécurité redondant), c'est-à-dire des défaillances de cause commune, se traduit en erreurs substantielles lorsque des calculs de fiabilité sont appliqués à des systèmes à plusieurs canaux ou redondants.

Cette annexe informative décrit deux méthodologies qui permettent de prendre en compte les défaillances de cause commune dans l'évaluation de sécurité des systèmes E/E/PE à plusieurs canaux ou redondants. L'utilisation de ces méthodologies permet d'estimer l'intégrité d'un tel système de manière plus précise que si les défaillances de cause commune potentielles sont ignorées.

La première méthodologie est utilisée pour calculer une valeur de β, facteur fréquemment utilisé dans la modélisation des défaillances de cause commune. Ceci permet d'estimer le taux de défaillances de cause commune applicable à deux systèmes ou plus fonctionnant en parallèle à partir du taux de défaillance aléatoire du matériel de l'un de ces systèmes (voir D.5). Il est généralement admis que les chiffres relatifs aux défaillances aléatoires du matériel incluent un nombre de défaillances occasionnées par des défaillances systématiques.

D'autres méthodologies sont dans certains cas préférables, par exemple lorsqu'un facteur β plus précis peut être obtenu grâce à la disponibilité de données relatives aux défaillances de cause commune ou lorsque le nombre d'éléments affectés est supérieur à quatre. La deuxième méthodologie, c'est-à-dire la méthode du taux de défaillance binomiale (également désignée modèle des chocs), peut être utilisée.

D.1.2 Présentation succincte

On considère que les défaillances d'un système ont deux causes différentes:

– les défaillances aléatoires du matériel; et
– les défaillances systématiques.

On estime que les premières apparaissent de manière aléatoire dans le temps pour tout composant et entraînent une défaillance d'un canal au sein du système auquel appartient le composant lorsque les dernières apparaissent immédiatement et de manière déterministe lorsque le système atteint l'état auquel l'erreur systématique sous-jacente s'applique.

Il existe une probabilité restreinte que des défaillances aléatoires indépendantes du matériel puissent avoir lieu sur tous les canaux d'un système à plusieurs canaux de sorte que tous les canaux présentent simultanément un état de défaillance. Les défaillances aléatoires du matériel étant sensées apparaître au hasard dans le temps, la probabilité pour que de telles défaillances affectent simultanément des canaux parallèles est faible comparée à la probabilité de défaillance d'un seul canal. Cette probabilité peut être calculée au moyen de techniques

communément admises mais le résultat peut être très optimiste lorsque les défaillances ne sont pas totalement indépendantes les unes des autres.

Les défaillances dépendantes se décomposent traditionnellement dans les catégories suivantes (voir la référence [18] dans la Bibliographie):

– Défaillance de cause commune (CCF) provoquant plusieurs défaillances à partir d'une cause partagée unique. Les défaillances multiples peuvent se produire simultanément ou sur une période de temps;
– Défaillances de mode commun (CMF) qui représentent un cas particulier de CCF dans lequel plusieurs équipements sont défaillants dans le même mode;
– Défaillances en cascade qui sont des défaillances par propagation.

Le terme CCF est souvent utilisé pour couvrir tous les types de défaillances dépendantes comme appliqué dans la présente annexe. Elles se décomposent également comme suit:

– Défaillances dépendantes dues à des causes déterministes évidentes;
– Evénements de défaillances multiples potentielles résiduelles non pris explicitement en compte dans l'analyse du fait du manque d'exactitude, de causes déterministes pas évidentes ou de l'impossibilité de collecter des données de fiabilité.

Il convient d'analyser, de modéliser et de quantifier la première défaillance de manière conventionnelle et de traiter uniquement la deuxième comme indiqué dans la présente Annexe D informative. Cependant, les défaillances systématiques – qui sont des défaillances parfaitement dépendantes non identifiées pendant l'analyse de sécurité (sinon elles auraient été retirées) – sont traitées de manière spécifique dans la présente norme et cette annexe s'applique principalement aux défaillances dépendantes aléatoires du matériel.

Par conséquent, les défaillances de cause commune résultant d'une cause unique peuvent affecter plusieurs canaux ou plusieurs composants. Celles-ci peuvent avoir pour origine une défaillance systématique (par exemple, une erreur de conception ou de spécification) ou une contrainte extérieure provoquant une défaillance aléatoire précoce du matériel (par exemple une température excessive résultant de la défaillance aléatoire d'un ventilateur de refroidissement commun, qui accélère la durée de vie des composants ou les sort de leur environnement d'exploitation spécifié) ou, éventuellement, une combinaison des deux. Les défaillances de cause commune étant, selon toute vraisemblance, susceptibles d'affecter plusieurs canaux dans un système à plusieurs canaux, la probabilité de défaillance de cause commune est probablement le facteur déterminant d'évaluation de la probabilité globale de défaillance d'un système à plusieurs canaux et si cela n'est pas pris en compte, il est peu probable d'obtenir une estimation réaliste du niveau d'intégrité de sécurité du système à plusieurs canaux.

D.1.3 Protection contre les défaillances de cause commune

Bien que les défaillances de cause commune résultent d'une cause unique, elles ne se manifestent pas toutes simultanément dans tous les canaux. Par exemple, si un ventilateur est défectueux, tous les canaux d'un système E/E/PE à plusieurs canaux peuvent subir une défaillance, et entraîner aussi une défaillance de cause commune. Cependant, il est peu probable que tous les canaux s'échauffent avec la même intensité ou atteignent la même température critique. Les défaillances apparaissent donc à des moments différents dans les différents canaux.

L'architecture des systèmes programmables leur permet d'exécuter des fonctions de diagnostic interne pendant leur exploitation en ligne. Celles-ci peuvent être utilisées de diverses manières, par exemple

– un système électronique programmable à un canal peut vérifier en continu son fonctionnement interne ainsi que la fonctionnalité des dispositifs d'entrée et de sortie. Lorsqu'elle a été prévue dès la conception, une couverture d'essai de l'ordre de 99 % est réalisable (voir [13] dans la Bibliographie). Si 99 % des anomalies internes sont détectées

avant qu'elles ne provoquent une défaillance, la probabilité d'anomalies sur un seul canal qui peut en définitive contribuer à des défaillances de cause commune est réduite de manière significative;

– outre les essais internes, chaque canal d'un système électronique programmable peut surveiller les sorties d'autres canaux dans un système électronique programmable à plusieurs canaux (ou encore chaque dispositif électronique programmable peut surveiller un autre dispositif de même nature dans un système électronique programmable à plusieurs canaux). De cette manière, lorsqu'une défaillance apparaît sur un canal, elle peut être détectée, puis un arrêt de sécurité peut être déclenché par le ou les canaux restants qui n'ont pas subi de défaillance et qui effectuent l'essai de surveillance croisée. (Il convient de noter que la surveillance croisée n'est efficace que si l'état du système de commande change en continu, par exemple le verrouillage d'une protection fréquemment utilisée dans une machine cyclique, ou lorsque de brefs changements peuvent être introduits sans affecter la fonction commandée.) Cette surveillance croisée peut être exécutée à un débit élevé, de sorte que, juste avant une défaillance de cause commune non simultanée, il est probable qu'un essai de surveillance croisée détecte la défaillance du premier canal et soit en mesure de mettre le système en état de sécurité avant qu'un second canal ne soit affecté.

Si l'on reprend l'exemple du ventilateur, le taux d'élévation de la température et la sensibilité de chaque canal sont légèrement différents, entraînant une éventuelle défaillance du second canal plusieurs dizaines de minutes après le premier. Cela permet à l'essai de diagnostic de lancer un arrêt de sécurité avant que le second canal ne succombe à l'anomalie de cause commune.

On peut donc en conclure que

– les systèmes électroniques programmables ont la possibilité d'incorporer des défenses contre les défaillances de cause commune et être ainsi moins sensibles à ces défaillances en comparaison à d'autres technologies;

– un facteur β différent peut être applicable aux systèmes électroniques programmables par comparaison avec d'autres technologies. Ainsi, les estimations réalisées sur le facteur β et fondées sur des données historiques sont susceptibles de ne pas être valides. (Aucun des modèles existants étudiés utilisés pour l'estimation de la probabilité de défaillance de cause commune ne prévoit l'effet de la surveillance croisée automatique);

– étant donné que les défaillances de cause commune sont étalées dans le temps, et peuvent être révélées par les essais de diagnostic avant qu'elles n'affectent tous les canaux, de telles défaillances peuvent ne pas être reconnues ou indiquées comme étant des défaillances de cause commune.

Trois approches peuvent être suivies pour réduire la probabilité des défaillances de cause commune potentiellement dangereuses.

a) Réduire le nombre global de défaillances systématiques et défaillances aléatoires du matériel. (Cela réduit les surfaces des ellipses dans la Figure D.1, entraînant ainsi une réduction de la zone de chevauchement).

b) Assurer une indépendance maximale des canaux (séparation et diversité). (Cela réduit la zone de chevauchement entre les ellipses dans la Figure D.1 tout en conservant la même surface.)

c) Détecter les défaillances de cause commune non simultanées lorsqu'un seul canal est affecté et avant qu'un deuxième ne le soit, c'est-à-dire utiliser les essais de diagnostic ou le décalage des essais périodiques.

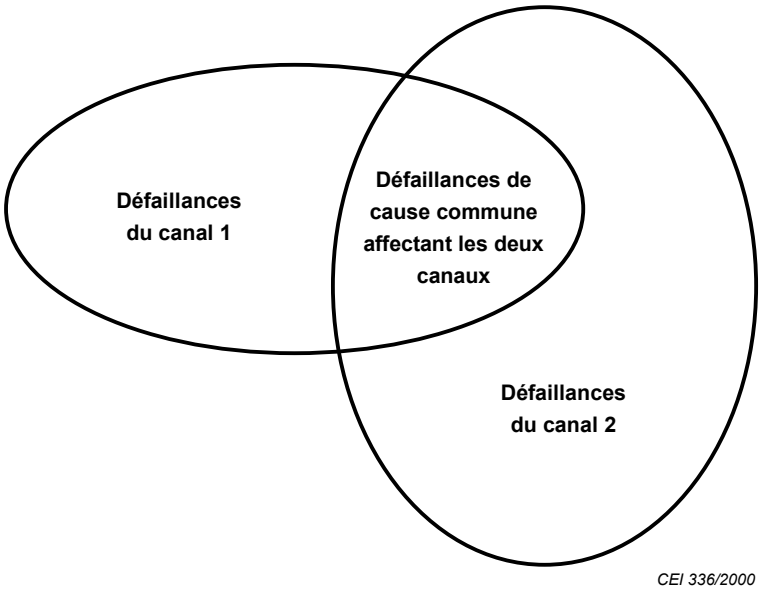


Figure D.1 – Relation entre défaillances de cause commune et défaillances propres à un canal

Pour les systèmes à plus de deux canaux, la défaillance de cause commune peut affecter tous les canaux ou uniquement plusieurs canaux sans toutefois dépendre de la source de mode commun. Ainsi, l'approche retenue dans la présente annexe, selon la première méthode, consiste à calculer la valeur β sur la base d'un système duplex à logique majoritaire 1oo2, puis à appliquer un facteur de multiplication à la valeur calculée β en fonction du nombre total de canaux et des exigences de logique majoritaire. (voir Tableau D.5).

D.1.4 Approche adoptée dans la série CEI 61508

La série CEI 61508 se fonde sur ces trois orientations et nécessite donc une triple approche:

a) Appliquer les techniques spécifiées dans la CEI 61508-2/3 afin de réduire la probabilité globale de défaillance systématique à un niveau correspondant à la probabilité de défaillance aléatoire du matériel.

b) Quantifier les facteurs qui peuvent l'être, en d'autres termes tenir compte de la probabilité de défaillance aléatoire du matériel, comme spécifié dans la CEI 61508-2.

c) Déduire, en utilisant les moyens considérés comme les plus adéquats à l'heure actuelle, un facteur reliant la probabilité de défaillance de cause commune du matériel à la probabilité de défaillances aléatoires du matériel. La méthodologie décrite dans la présente annexe traite de l'obtention de ce facteur.

La plupart des méthodologies permettant d'estimer la probabilité de défaillances de cause commune tentent de faire des prédictions à partir de la probabilité de défaillances aléatoires du matériel. Il est difficile de justifier une relation entre ces probabilités; toutefois, une telle corrélation a été vérifiée dans la pratique et procède probablement d'effets de second ordre. Par exemple, plus la probabilité de défaillances aléatoires du matériel d'un système est élevée,

– plus le volume de la maintenance exigé par le système est important. La probabilité d'introduction d'une anomalie systématique au cours de la maintenance dépend du nombre d'opérations de maintenance réalisé, et cela affecte également le taux d'erreurs humaines, ce qui entraîne des défaillances de cause commune. Cela donne lieu à une relation entre la probabilité de défaillances aléatoires du matériel et la probabilité de défaillance de cause commune. Par exemple:

  - une réparation, suivie d'essais et éventuellement d'un réétalonnage, est nécessaire à chaque fois qu'une défaillance aléatoire du matériel a lieu;

- pour un niveau d'intégrité de sécurité donné, un système ayant une probabilité de défaillances aléatoires du matériel plus élevée nécessite des essais périodiques plus fréquents et plus approfondis/complexes, entraînant une intervention humaine supplémentaire.

– plus complexe est le système. La probabilité de défaillances aléatoires du matériel dépend du nombre de composants, et donc de la complexité d'un système. Un système complexe est plus difficilement compris et donc plus vulnérable à l'introduction d'anomalies systématiques. De plus, la complexité rend difficile la détection des anomalies, que ce soit par une analyse ou des essais, et peut alors utiliser des parties de la logique d'un système peu éprouvées dans la pratique, si ce n'est en de rares circonstances. A nouveau, cela entraîne une relation entre la probabilité de défaillances aléatoires du matériel et la probabilité de défaillance de cause commune.

Plusieurs approches sont couramment utilisées pour traiter les CCF (facteur β, lettres grecques multiples, facteur α, taux de défaillance binomiale ...) [20]. La présente annexe informative propose deux des modèles courants pour la troisième partie de la triple approche déjà décrite. Malgré les limites des modèles courants, ils sont reconnus comme étant à l'heure actuelle les meilleurs moyens de fournir une estimation de la probabilité de défaillance de cause commune:

– le modèle bien établi du facteur β qui est largement utilisé et constitue un moyen réaliste de traiter un système à plusieurs canaux, comportant généralement jusqu'à quatre éléments dépendants.

– le taux de défaillance binomiale [21] (également désigné modèle des chocs) qui peut être utilisé lorsque le nombre d'éléments dépendants est supérieur à quatre.

On se heurte aux deux difficultés suivantes lorsque l'on utilise le facteur β ou les modèles des chocs sur un système E/E/PE.

– Quelle valeur convient-il de choisir pour les paramètres? De nombreuses sources (par exemple la référence [10]) suggèrent des fourchettes probables de la valeur du facteur β mais aucune valeur réelle n'est donnée, et le choix est laissé à l'appréciation subjective de l'utilisateur. Pour résoudre ce problème, la méthodologie du facteur β de la présente annexe se fonde sur le système décrit en premier lieu dans la référence [11] et récemment redéfinie dans la référence [12].

– Ni le modèle du facteur β ni le modèle des chocs ne tiennent compte des capacités d'essai de diagnostic sophistiquées des systèmes électroniques programmables modernes, qui peuvent être utilisées pour la détection de défaillances de cause commune non simultanées avant qu'elles n'aient eu suffisamment de temps pour se manifester pleinement. Pour combler cette lacune, l'approche décrite dans les références [11] et [12] a été modifiée afin de refléter l'effet des essais de diagnostic sur l'estimation de la valeur probable de β.

Les fonctions d'essai de diagnostic d'un système électronique programmable effectuent continuellement une comparaison entre le fonctionnement du système et des états prédéfinis. Ces états peuvent être prédéfinis sur logiciel ou sur matériel (par exemple au moyen d'un chien de garde). Envisagées ainsi, les fonctions d'essai de diagnostic peuvent être considérées comme un canal supplémentaire assurant partiellement une certaine diversité et tournant parallèlement au système électronique programmable.

Une surveillance croisée entre les canaux peut également être réalisée. Cette technique a été utilisée pendant de nombreuses années dans des systèmes à deux canaux interverrouillés uniquement à base de relais. Cependant, avec une technologie à relais, il n'est généralement possible de réaliser des vérifications croisées que lorsque les canaux changent d'état, rendant ces essais inadaptés pour la détection de défaillances de cause commune non simultanées dans lesquelles les systèmes restent dans le même état (par exemple ON) sur de longues périodes. Avec la technologie des systèmes électroniques programmables, la surveillance croisée peut être réalisée à une fréquence de répétition élevée.

D.2 Domaine d'application de la méthodologie

Le domaine d'application de cette méthodologie se limite aux défaillances de cause commune dans le matériel et ce, pour les raisons suivantes:

– le modèle du facteur β et le modèle des chocs relient la probabilité de défaillance de cause commune à la probabilité de défaillance aléatoire du matériel. La probabilité de défaillances de cause commune qui implique le système dans son ensemble dépend de la complexité du système (qui s'explique éventuellement par le logiciel de l'utilisateur) et non du matériel uniquement. Tout calcul fondé sur la probabilité de défaillance aléatoire du matériel ne peut manifestement pas prendre en compte la complexité du logiciel;

– les comptes rendus sur les défaillances de cause commune se limitent généralement aux défaillances du matériel, le domaine le plus préoccupant pour les fabricants du matériel;

– la modélisation des défaillances systématiques (par exemple les défaillances de logiciel) n'est pas considérée comme réalisable dans la pratique;

– les mesures spécifiées dans la CEI 61508-3 sont destinées à réduire la probabilité de défaillance de cause commune liée au logiciel à un niveau acceptable compte tenu du niveau d'intégrité de sécurité cible.

Ainsi, l'estimation de la probabilité de défaillance de cause commune issue de cette méthodologie est liée uniquement aux défaillances relatives au matériel. Il convient de NE PAS considérer que cette méthodologie puisse être utilisée pour obtenir un taux de défaillance global prenant en compte la probabilité de défaillance relative au logiciel.

D.3 Éléments pris en compte dans la méthodologie

Dans la mesure où les capteurs, les sous-systèmes logiques et éléments finaux sont sujets, par exemple, à des conditions environnementales différentes et des essais de diagnostic ayant des niveaux de capacité variables, il convient que la méthodologie soit appliquée à chacun des sous-systèmes séparément. Par exemple, le sous-système logique est plus vraisemblablement destiné à un environnement contrôlé, alors que les capteurs peuvent être montés à l'extérieur sur une tuyauterie exposée aux intempéries.

Les canaux électroniques programmables ont la capacité requise pour exécuter des fonctions d'essai de diagnostic sophistiquées. Ces fonctions peuvent

– disposer d'une couverture de diagnostic élevée au sein des canaux;

– surveiller des canaux de redondance supplémentaires;

– avoir une fréquence de répétition élevée; et

– dans certains cas de plus en plus nombreux, surveiller également des capteurs et/ou des éléments finaux.

Pour une grande part, les défaillances de cause commune n'affectent pas en même temps tous les canaux. Ainsi, lorsque la fréquence de répétition des essais de diagnostic est suffisamment élevée, une grande partie de défaillances de cause commune peut être détectée et donc être évitée avant d'affecter tous les canaux disponibles.

Les caractéristiques d'un système à plusieurs canaux, qui ont une incidence sur son immunité aux défaillances de cause commune, ne peuvent pas être toutes évaluées par les essais de diagnostic. Cependant, les caractéristiques ayant trait à la diversité ou à l'indépendance sont rendues plus effectives. Toute caractéristique destinée à prolonger la durée entre défaillances de canal pour une défaillance de cause commune non simultanée (ou réduire la proportion de défaillances de cause commune simultanées) augmente la probabilité de détection de la défaillance par les essais de diagnostic et de mise en sécurité du site. Les caractéristiques liées à l'immunité aux défaillances de cause commune sont donc divisées entre celles dont l'effet est supposé être accru par l'utilisation des essais de diagnostic et celles dont l'effet n'est pas supposé être accru. Cela conduit aux deux colonnes, respectivement X et Y, du Tableau D.1.

Toutefois, pour un système à trois canaux, la probabilité que des défaillances de cause commune affectent les trois canaux est légèrement inférieure à la probabilité de défaillances affectant deux canaux; on suppose, pour simplifier la méthodologie du facteur β, que la probabilité est indépendante du nombre de canaux affectés; en d'autres termes, on suppose que lorsqu'une défaillance de cause commune se produit, elle affecte tous les canaux. Une autre méthode est le modèle des chocs.

Il n'existe pas de données disponibles connues sur les défaillances de cause commune relatives au matériel permettant l'étalonnage de la méthodologie. Les tableaux de la présente annexe ont donc été élaborés à partir d'un raisonnement théorique.

Parfois, les programmes d'essai de diagnostic ne jouent pas un rôle direct de sécurité et peuvent donc ne pas faire l'objet du même niveau de garantie de qualité que ceux qui assurent les principales fonctions de commande. Cette méthodologie a été développée en se fondant sur l'hypothèse selon laquelle les essais de diagnostic possèdent une intégrité qui correspond au niveau d'intégrité de sécurité cible. Il convient donc de développer tout programme d'essai de diagnostic lié au logiciel en utilisant des techniques adaptées au niveau d'intégrité de sécurité cible.

D.4 Utilisation du facteur β pour le calcul de probabilité de défaillance due à des défaillances de cause commune dans un système E/E/PE relatif à la sécurité

Considérons l'effet de défaillances de cause commune sur un système à plusieurs canaux disposant d'essais de diagnostic dans chacun de ses canaux.

Si l'on utilise le modèle du facteur β, le taux de défaillance dangereuse de cause commune est:

$$\lambda_D \beta$$

où

λ_D est le taux de défaillance dangereuse aléatoire du matériel pour chaque canal individuel et β est le facteur β en l'absence d'essais de diagnostic, c'est-à-dire la proportion de défaillances d'un canal individuel qui affectent tous les canaux.

Supposons maintenant que les défaillances de cause commune affectent tous les canaux et que la période de temps entre la défaillance sur le premier canal et la défaillance de tous les canaux est relativement courte en comparaison de l'intervalle de temps entre des défaillances de cause commune successives.

Supposons qu'il existe des essais de diagnostic exécutés dans chaque canal que détecte et révèle une partie des défaillances. On peut répartir toutes les défaillances dans deux catégories: celles qui ne s'inscrivent pas dans la couverture des essais de diagnostic (et qui ne peuvent donc jamais être détectées) et celles qui s'inscrivent dans cette couverture (qui sont en fin de compte détectées par les essais de diagnostic).

Le taux global de défaillance provoqué par des défaillances dangereuses de cause commune est donc donné par:

$$\lambda_{DU} \beta + \lambda_{DD} \beta_D$$

où

– λ_{DU} est le taux de défaillance dangereuse non détectée d'un canal unique, c'est-à-dire le taux de défaillance des défaillances qui ne s'inscrivent pas dans la couverture des essais

de diagnostic; toute réduction dans le facteur β induite par la fréquence de répétition des essais de diagnostic n'affecte manifestement pas cette proportion des défaillances;

– β est le facteur de défaillance de cause commune pour les anomalies dangereuses non détectables, égal au facteur β global applicable en l'absence d'essai de diagnostic;

– λ_{DD} est le taux de défaillance dangereuse détectée d'un canal unique, c'est-à-dire le taux de défaillance des défaillances d'un seul canal qui s'inscrivent dans la couverture des essais de diagnostic. Si la fréquence de répétition des essais de diagnostic est élevée, une proportion des défaillances est découverte, entraînant ainsi une réduction de la valeur de β, c'est-à-dire $\beta_{D;}$

– β_D est le facteur de défaillance de cause commune pour les anomalies dangereuses détectables. Plus la fréquence de répétition des essais de diagnostic est augmentée, plus la valeur de β_D descend en dessous de celle de β;

– β est obtenu à partir du Tableau D.5, en utilisant les résultats de D.4 tel que, $S = X + Y$ (voir D.5);

– β_D est obtenu à partir du Tableau D.5, en utilisant les résultats de D.4 tel que, $S_D = X(Z+1)+Y$.

D.5 Utilisation des tableaux pour l'estimation de β

Il convient de calculer séparément le facteur β pour les capteurs, le sous-système logique et les éléments finaux.

Afin de réduire au minimum la probabilité d'occurrence de défaillances de cause commune, il convient d'établir en premier lieu les mesures qui permettent une défense efficace contre l'apparition de ces défaillances. La mise en oeuvre des mesures appropriées dans le système entraîne une réduction de la valeur du facteur β utilisée pour l'estimation de la probabilité de défaillance due à des défaillances de cause commune.

Le Tableau D.1 énumère les mesures et comprend des valeurs associées, basées sur une approche théorique (estimation d'ingénierie), qui représentent la contribution de chacune des mesures à la réduction des défaillances de cause commune. Les capteurs et éléments finaux étant traités différemment des composants électroniques programmables, des colonnes distinctes sont utilisées dans le tableau pour énumérer ces composants ainsi que les capteurs ou éléments finaux.

Des essais de diagnostic étendus peuvent être inclus dans des systèmes électroniques programmables pour détecter des défaillances de cause commune non simultanées. Pour pouvoir prendre en compte les essais de diagnostic dans l'estimation du facteur β, la contribution globale de chaque mesure du Tableau D.1 est répartie, en utilisant une approche théorique, entre deux ensembles de valeurs, X et Y. Pour chaque mesure, le ratio X:Y représente l'importance de l'amélioration de la contribution de cette mesure à l'élimination des défaillances de cause commune par les essais de diagnostic.

Il convient que l'utilisateur du Tableau D.1 détermine les mesures applicables au système en question, et fasse la somme des valeurs correspondantes indiquées dans chacune des colonnes X_{LS} et Y_{LS} pour le sous-système logique, ou X_{SF} et Y_{SF} pour les capteurs ou éléments finaux, les sommes étant respectivement notées X et Y.

Il est admis d'utiliser les Tableaux D.2 et D.3 pour déterminer un facteur Z à partir de la fréquence et de la couverture des essais de diagnostic, en tenant compte de la Note 4 (importante) qui limite les cas où il convient d'utiliser une valeur non nulle de Z. Le résultat S est alors calculé en utilisant les équations suivantes, selon le cas (voir l'article précédent):

– $S = X + Y$ pour obtenir la valeur de β_{int} (facteur β pour les défaillances non détectées); et

– $S_D = X(Z+1)+Y$ pour obtenir la valeur de $\beta_{D\ int}$ (facteur β pour les défaillances détectées).

Ici, S ou S_D est le résultat utilisé dans le Tableau D.4 pour déterminer le facteur β_{int} approprié.

β_{int} et $\beta_{D\ int}$ représentent les valeurs de la défaillance de cause commune avant de tenir compte de l'effet de différents degrés de redondance.

Tableau D.1 – Calcul des résultats électroniques programmables ou des capteurs/éléments finaux

Article	Sous-système logique		Capteurs et éléments finaux	
	X_{LS}	Y_{LS}	X_{SE}	Y_{SE}
Séparation/ségrégation				
Tous les câbles de signaux des canaux sont-ils acheminés séparément vers tous les points de connexion ?	1,5	1,5	1,0	2,0
Les canaux du sous-système logique sont-ils sur des cartes de circuits imprimés séparées?	3,0	1,0		
Les canaux du sous-système logique sont-ils séparés efficacement? Par exemple, dans des armoires séparées ?	2,5	0,5		
Si les capteurs/éléments finaux disposent d'une électronique de commande dédiée, l'électronique de chaque canal est-elle sur une carte de circuit imprimé séparée ?			2,5	1,5
Si les capteurs/éléments finaux disposent d'une électronique de commande, l'électronique de chaque canal est-elle sous abri et dans des armoires séparées ?			2,5	0,5
Diversité/redondance				
Les canaux emploient-ils des technologies électriques différentes, par exemple, un canal électronique ou électronique programmable et l'autre à relais ?	8,0			
Les canaux emploient-ils des technologies électroniques différentes, par exemple, un canal électronique et l'autre un canal électronique programmable ?	6,0			
Les dispositifs emploient-ils des principes physiques différents pour les éléments sensibles, par exemple, la pression et la température, un anémomètre à moulinets et un transducteur Doppler, etc. ?			9,0	
Les dispositifs utilisent-ils des principes électriques/conceptions différents par exemple numérique et analogique, fabricant différent (pas simplement de marque différente) ou technologie différente ?			6,5	
Une faible diversité est-elle utilisée par exemple des essais de diagnostic du matériel utilisant la même technologie ?	2,0	1,0		
Une diversité moyenne est-elle utilisée, par exemple des essais de diagnostic du matériel utilisant une technologie différente ?	3,0	2,0		
Les canaux ont-ils été conçus par des concepteurs différents sans communiquer entre eux pendant les activités de conception ?	1,5	1,5		
Des méthodes d'essai et des individus différents sont-ils utilisés pour chaque canal pendant la mise en service ?	1,0	0,5	1,0	2,0
La maintenance de chaque canal est-elle réalisée par des personnes différentes à des moments différents ?	3,0		3,0	
Complexité/conception/application/maturité/expérience				
L'interconnexion entre des canaux prévient-elle l'échange d'informations autres que celles utilisées pour les besoins des essais de diagnostic ou de logique majoritaire ?	0,5	0,5	0,5	0,5
La conception se fonde-t-elle sur des techniques utilisées en équipement qui ont été utilisées de manière satisfaisante dans ce domaine depuis plus de cinq ans ?	0,5	1,0	1,0	1,0
Y a-t-il plus de cinq ans d'expérience avec le même matériel utilisé dans des environnements similaires ?	1,0	1,5	1,5	1,5
Le système est-il simple, par exemple, pas plus de 10 entrées ou sorties par canal ?		1,0		
Les entrées et sorties sont-elles protégées contre les surtensions et les surintensités potentielles ?	1,5	0,5	1,5	0,5
Les caractéristiques assignées de tous les dispositifs/composants sont-elles sélectionnées avec prudence ? (par exemple, par un facteur de 2 ou plus)	2,0		2,0	
Evaluation/analyse et retour d'information				
Les résultats des analyses des modes de défaillance et de leurs effets ou des analyses d'arbre de panne ont-ils été examinés afin d'établir des sources de défaillance de cause commune et éliminer dès la conception les sources prédéterminées de défaillance de cause commune ?		3,0		3,0
Les défaillances de cause commune ont-elles été prises en compte lors des études sur la conception et les résultats ont-ils été répercutés sur la conception ? (Des preuves documentaires des études faites sur la conception sont exigées.)		3,0		3,0
Toutes les défaillances relevées sur le terrain ont-elles été analysées de manière exhaustive avec retour d'expérience vers la conception ? (Des preuves documentaires de la procédure sont exigées.)	0,5	3,5	0,5	3,5

Tableau D.1 *(suite)*

Article	Sous-système logique		Capteurs et éléments finaux	
	X_{LS}	Y_{LS}	X_{SE}	Y_{SE}
Procédures/interface humaine				
Existe-t-il une procédure de travail écrite qui assure que toutes les défaillances (ou dégradations) de composants sont détectées, que les causes initiales sont établies et d'autres éléments similaires inspectés pour déceler les causes potentielles de défaillances similaires ?		1,5	0,5	1,5
Existe-t-il des procédures garantissant que: la maintenance (y compris le réglage ou l'étalonnage) de toute partie des canaux indépendants est échelonnée et, outre les vérifications manuelles réalisées après la maintenance, les essais de diagnostic peuvent-ils être exécutés de manière satisfaisante entre l'achèvement de la maintenance d'un canal donné et le début de la maintenance d'un autre canal ?	1,5	0,5	2,0	1,0
Les procédures écrites de maintenance spécifient-elles que toutes les parties de systèmes redondants (par exemple des câbles, etc.), conçus pour être indépendants les uns des autres, ne sont pas allouées de façons différentes ?	0,5	0,5	0,5	0,5
La maintenance des cartes de circuits imprimés, etc. est-elle effectuée à l'extérieur par un centre de réparation qualifié et tous les éléments réparés sont-ils soumis à des essais de préinstallation complets ?	0,5	1,0	0,5	1,5
Le système a-t-il une couverture de diagnostic faible (60 % à 90 %) et rend-il compte des défaillances au niveau d'un module remplaçable sur site ?	0,5			
Le système a-t-il une couverture de diagnostic moyenne (90 % à 99 %) et rend-il compte des défaillances au niveau d'un module remplaçable sur site ?	1,5	1,0		
Le système a-t-il une couverture de diagnostic élevée (>99 %) et rend-il compte des défaillances au niveau d'un module remplaçable sur site ?	2,5	1,5		
Les essais de diagnostic du système rapportent-ils les défaillances au niveau d'un module remplaçable sur site ?			1,0	1,0
Compétence/formation/culture de sécurité				
Les concepteurs ont-ils été formés (sur la base d'une documentation de formation) pour mesurer les causes et les conséquences de défaillances de cause commune ?	2,0	3,0	2,0	3,0
Les agents de maintenance ont-ils été formés (sur la base d'une documentation de formation) pour mesurer les causes et les conséquences de défaillances de cause commune ?	0,5	4,5	0,5	4,5
Contrôle de l'environnement				
L'accès du personnel est-il limité (par exemple armoires verrouillées, points inaccessibles) ?	0,5	2,5	0,5	2,5
Le système est-il en mesure de fonctionner toujours dans la plage de température, d'humidité, de corrosion, de poussière, de vibrations, etc. pour laquelle il a été soumis à essai, sans utiliser un contrôle extérieur de l'environnement ?	3,0	1,0	3,0	1,0
Tous les câbles de signaux et d'alimentation sont-ils séparés en tous points de connexion ?	2,0	1,0	2,0	1,0
Essais environnementaux				
L'immunité du système a-t-elle été évaluée pour toutes les influences environnementales significatives (par exemple compatibilité électromagnétique (CEM), température, vibrations, chocs, humidité) à un niveau approprié comme spécifié dans les normes reconnues ?	10,0	10,0	10,0	10,0

NOTE 1 Un certain nombre d'éléments dépendent du fonctionnement du système, et il peut être difficile d'effectuer les prévisions correspondantes lors de la conception. Dans ce cas, il convient que les concepteurs posent des hypothèses raisonnables et s'assurent par la suite que l'utilisateur final du système soit informé, par exemple, des procédures à mettre en place pour atteindre le niveau d'intégrité de sécurité prévu à la conception. Cette disposition peut être appliquée en incluant les informations nécessaires dans la documentation d'accompagnement.

NOTE 2 Les valeurs données dans les colonnes *X* et *Y* sont basées sur une approche théorique et prennent en compte les effets directs et indirects des articles énumérés dans la première colonne. Par exemple, l'utilisation de modules remplaçables sur site a les conséquences suivantes:

– les réparations sont effectuées par le constructeur dans des conditions définies et non pas sur le terrain dans des conditions moins favorables (avec les risques d'erreurs que cela comporte). La conséquence en est une contribution dans la colonne *Y* du fait de la réduction des défaillances systématiques potentielles (et, donc, des défaillances de cause commune);

– une réduction du besoin d'interaction manuelle sur le site et la possibilité de remplacer rapidement les modules présentant une anomalie, peut-être même en ligne, ce qui accroît l'efficacité du diagnostic et la possibilité d'identification des défaillances avant qu'elles ne deviennent des défaillances de cause commune. La conséquence en est une contribution de forte valeur dans la colonne *X*.

Tableau D.2 – Valeur de *Z* – électronique programmable

Couverture de diagnostic	Intervalle entre les essais de diagnostic		
	Moins de 1 min	Entre 1 min et 5 min	Plus de 5 min
≥ 99 %	2,0	1,0	0
≥ 90 %	1,5	0,5	0
≥ 60 %	1,0	0	0

Tableau D.3 – Valeur de *Z* – capteurs ou éléments finaux

Couverture de diagnostic	Intervalle entre les essais de diagnostic			
	Moins de 2 h	Entre 2 h et deux jours	Entres deux jours et une semaine	Plus d'une semaine
≥ 99 %	2,0	1,5	1,0	0
≥ 90 %	1,5	1,0	0,5	0
≥ 60 %	1,0	0,5	0	0

NOTE 1 La méthodologie est plus efficace si l'on tient compte de manière homogène de toutes les catégories de la liste donnée dans le Tableau D.1. Il est donc fortement recommandé que le résultat total des colonnes *X* et *Y* pour chaque catégorie ne dépasse pas le résultat total des colonnes *X* et *Y* divisé par 20. Par exemple, si le résultat total (*X* + *Y*) est 80, il convient qu'aucune des catégories (par exemple procédure/interface humaine) n'ait un résultat total (*X* + *Y*) de moins de quatre.

NOTE 2 Lorsque le Tableau D.1 est utilisé, tenir compte des résultats de tous les éléments applicables. Le calcul du résultat a été conçu pour prendre en charge des éléments qui ne sont pas mutuellement exclusifs. Par exemple, un système ayant des canaux de sous-système logique dans des tiroirs séparés a droit aux deux résultats pour « Les canaux du sous-système logique sont-ils dans des armoires séparées ? » et à ceux de « Les canaux du sous-système logique sont-ils sur des cartes de circuits imprimés séparées ? ».

NOTE 3 Lorsque des capteurs ou des éléments finaux sont à base d'électronique programmable, il convient de les considérer comme faisant partie du sous-système logique lorsqu'ils sont contenus dans le même bâtiment (ou véhicule) que le dispositif qui constitue l'élément majeur du sous-système logique, et comme des capteurs ou des éléments finaux dans le cas contraire.

NOTE 4 Pour une valeur non nulle de *Z*, il convient d'assurer que l'équipement commandé est mis dans un état de sécurité avant qu'une défaillance de cause commune non simultanée ne puisse affecter tous les canaux. Il convient que la durée nécessaire de mise en état de sécurité soit inférieure à l'intervalle entre essais de diagnostic revendiqué. Une valeur non nulle pour *Z* ne peut être utilisée que lorsque:

– le système déclenche un arrêt automatique suite à la détection d'une anomalie; ou

– un arrêt en sécurité ne se déclenche pas après une première anomalie [9)], mais les essais de diagnostic:

  - déterminent l'emplacement de l'anomalie et sont capables de localiser l'anomalie; et
  - sont toujours aptes à placer l'EUC en état de sécurité après la détection d'anomalies postérieures; ou

– une procédure de travail formelle est mise en place pour assurer que la cause de toute anomalie détectée est examinée de manière exhaustive pendant l'intervalle entre essais de diagnostic revendiqué; et

  - lorsque l'anomalie peut potentiellement entraîner une défaillance de cause commune, l'installation est immédiatement mise à l'arrêt; ou
  - le canal présentant une anomalie est réparé pendant l'intervalle entre essais de diagnostic revendiqué.

NOTE 5 Dans les industries de transformation, il est peu probable que l'EUC puisse être mis à l'arrêt lorsqu'une anomalie est détectée pendant l'intervalle entre essais de diagnostic tel que décrit dans le Tableau D.2. Il convient de ne pas interpréter cette méthodologie comme une exigence stipulant que les usines de transformation soient mises à l'arrêt lorsque de telles anomalies sont détectées. Cependant, lorsqu'un arrêt n'est pas déclenché, aucune

9) Il convient de prendre en compte le fonctionnement du système pour l'identification d'une anomalie. Par exemple, il convient qu'un système 2oo3 simple soit mis à l'arrêt (ou réparé) dans les délais indiqués dans les Tableaux D.2 ou D.3, après identification d'une défaillance simple. Si cela n'est pas le cas, une défaillance sur un second canal peut entraîner l'exclusion du canal restant (en bon état) par la logique majoritaire des deux canaux défectueux. Un système qui reconfigure automatiquement en un système 1oo2 à logique majoritaire en cas de défaillance d'un canal et se met automatiquement à l'arrêt en cas de deuxième défaillance, dispose d'une probabilité plus élevée de détecter la défaillance sur le second canal et ainsi une valeur non nulle pour *Z* peut être demandée.

réduction du facteur β ne peut être obtenue par l'utilisation des essais de diagnostic pour l'électronique programmable. Dans certaines industries, un arrêt peut être réalisable pendant la durée décrite. Une valeur non nulle de *Z* peut dans ce cas être utilisée.

NOTE 6 Lorsque des essais de diagnostic sont réalisés de manière modulaire, la durée de répétition utilisée dans les Tableaux D.2 ou D.3 est la période comprise entre les exécutions successives de l'ensemble complet des modules d'essais de diagnostic. La couverture de diagnostic est la couverture totale assurée par tous les modules.

Tableau D.4 – Calcul de β_{int} ou de $\beta_{D\ int}$

Résultat (*S* ou S_D)	**Valeur correspondante de β ou de β_D pour:**	
	Sous-système logique	**Capteurs ou éléments finaux**
120 ou supérieur	0,5 %	1 %
70 à 120	1 %	2 %
45 à 70	2 %	5 %
Inférieur à 45	5 %	10 %
NOTE 1 Les niveaux maximaux de $\beta_{D\ int}$ indiqués dans ce tableau sont inférieurs à ceux qui seraient généralement utilisés; cela reflète l'utilisation de techniques spécifiées ailleurs dans la présente norme pour réduire la probabilité de défaillances systématiques dans sa globalité, et la probabilité de défaillances de cause commune en tant que résultat de cette réduction. NOTE 2 Des valeurs de $\beta_{D\ int}$ inférieures à 0,5 % pour le sous-système logique et à 1 % pour les capteurs seraient difficiles à justifier.		

La valeur β_{int} déduite du Tableau D4 est la défaillance de cause commune associée au système 1oo2. Pour d'autres niveaux de redondance (MooN), cette valeur β_{int} est modifiée comme indiqué dans le Tableau D.5 pour obtenir la valeur finale de β.

Le Tableau D.5 peut également être utilisé pour déterminer la valeur finale de β_D mais dans le cas de la valeur $\beta_{int,}$, la valeur $\beta_{D\ int}$ peut lui être substituée.

NOTE 7 Pour les informations pertinentes associées (concernant la méthode PDS), voir [25] dans la Bibliographie.

Tableau D.5 – Calcul de β pour des systèmes à niveaux de redondance supérieurs à 1oo2

MooN		**N**			
		2	3	4	5
M	1	β_{int}	0,5 β_{int}	0,3 β_{int}	0,2 β_{int}
	2	-	1,5 β_{int}	0,6 β_{int}	0,4 β_{int}
	3	-	-	1,75 β_{int}	0,8 β_{int}
	4	-	-	-	2 β_{int}

D.6 Exemples de l'utilisation de la méthodologie du facteur β

Afin de démontrer l'effet de la méthodologie du facteur β, quelques exemples simples ont été extraits du Tableau D.6 pour l'électronique programmable.

Pour les catégories n'ayant aucun rapport avec la diversité ou la redondance, des valeurs typiques pour X et Y ont été utilisées. Elles ont été obtenues en calculant la moitié du résultat maximal pour la catégorie considérée.

Dans les exemples de système divers, les valeurs données pour la catégorie diversité/redondance sont déduites des propriétés suivantes prises en considération dans le Tableau D.1:

– un système est électronique, l'autre utilise une technologie de relais;
– les essais de diagnostic du matériel utilisent des technologies différentes;
– les différents concepteurs n'ont pas communiqué pendant le processus de conception;
– des méthodes et personnels d'essai différents ont été utilisés pour la mise en service des systèmes; et
– la maintenance est effectuée par des équipes différentes à des moments différents.

Dans les exemples de système redondant, les valeurs pour la catégorie diversité/redondance découlent de ce que les diagnostics du matériel sont effectués par un système indépendant qui utilise la même technologie que les systèmes redondants.

Pour les systèmes diversifiés comme pour les systèmes redondants, on a utilisé une valeur maximale et une valeur minimale pour *Z*, ce qui donne au total quatre exemples de systèmes.

Tableau D.6 – Exemples de valeurs pour l'électronique programmable

Catégorie		Diversité du système avec essai de diagnostic satisfaisant	Diversité du système avec essai de diagnostic médiocre	Redondance du système avec essai de diagnostic satisfaisant	Redondance du système avec essai de diagnostic médiocre
Séparation/ségrégation	*X*	3,50	3,50	3,50	3,50
	Y	1,50	1,50	1,50	1,50
Diversité/redondance	*X*	14,50	14,50	2,00	2,00
	Y	3,00	3,00	1,00	1,00
Complexité/conception/.....	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Evaluation/analyse/....	*X*	0,25	0,25	0,25	0,25
	Y	4,75	4,75	4,75	4,75
Procédures/interface humaine	*X*	3,50	3,50	3,50	3,50
	Y	3,00	3,00	3,00	3,00
Compétence/formation/...	*X*	1,25	1,25	1,25	1,25
	Y	3,75	3,75	3,75	3,75
Contrôle de l'environnement	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Essai environnemental	*X*	5,00	5,00	5,00	5,00
	Y	5,00	5,00	5,00	5,00
Couverture de diagnostic	*Z*	2,00	0,00	2,00	0,00
Total *X*		33,5	33,5	21	21
Total *Y*		25,5	25,5	23,5	23,5
Résultat *S*		59	59	44,5	44,5
β		2 %	2 %	5 %	5 %
Résultat S_D		126	59	86,5	44,5
β_D		0,5 %	2 %	1 %	5 %
Système diversifié 1002 (Tableau D.5)		0,5 %	2 %		
Le système non diversifié est triplex avec logique majoritaire 2003 (Tableau D.5)				1,5 %	7,5 %

D.7 Taux de défaillance binomiale (Modèle des chocs) – approche CCF

Le retour d'expérience relatif à la défaillance de cause commune (CCF) indique que si plusieurs défaillances doubles, quelques défaillances triples et voire une défaillance quadruple ont été observées, aucune défaillance multiple au-delà de l'ordre quatre n'a jamais été observée à partir d'une cause unique explicite qui aurait pu ne pas être identifiée pendant l'analyse de sécurité. Par conséquent, la probabilité de défaillances dépendantes multiples

diminue lorsque l'ordre de la CCF augmente. Par conséquent, si le modèle du facteur β est réaliste pour les défaillances doubles, légèrement pessimiste pour les défaillances triples, au-delà il devient beaucoup trop prudent. Considérons l'exemple type d'un système instrumenté de sécurité qui ferme les n puits de production (par exemple n=150) d'un champ pétrolier en cas de blocage de sortie. Bien entendu, 2, 3, voire 4 puits peuvent ne pas se fermer du fait d'une CCF non explicite mais pas tous les n puits tels que modélisés par le facteur β (sinon, la CCF est explicite et il convient de l'analyser comme une défaillance individuelle). Un autre exemple type concerne le traitement de plusieurs couches de protection en même temps. Par exemple, le fait de tenir compte de la CCF potentielle entre capteurs de deux couches de protection peut impliquer de considérer les CCF entre six capteurs (c'est-à-dire 3 capteurs pour chaque couche).

Plusieurs modèles ont été proposés [18] pour pallier cette difficulté mais la plupart d'entre eux nécessitent un tel nombre de paramètres de fiabilité (par exemple, lettres grecques multiples ou modèles α) qu'ils en deviennent non réalistes. Parmi ces modèles, le taux de défaillance binomiale (Modèle des chocs), introduit par Vesely en 1977 et amélioré par Atwood en 1986, fournit une solution pragmatique [18, 19]. Le principe repose sur le fait que lorsqu'une CCF se produit, elle s'apparente à un choc sur les composants associés. Ce choc peut être mortel (c'est-à-dire même effet que dans le modèle du facteur β) ou non mortel, auquel cas il n'existe qu'une certaine probabilité de défaillance d'un composant donné du fait du choc. La probabilité d'occurrence de k défaillances dues au choc non mortel est alors distribuée de manière binomiale.

Ce modèle ne nécessite de mettre en œuvre que 3 paramètres:

– ω taux de chocs mortels;

– ρ taux de chocs non mortels;

– γ probabilité conditionnelle de défaillance d'un composant due à un choc non mortel.

La Figure D.2 donne un exemple de mise en œuvre de cette méthode au moyen d'un arbre de panne.

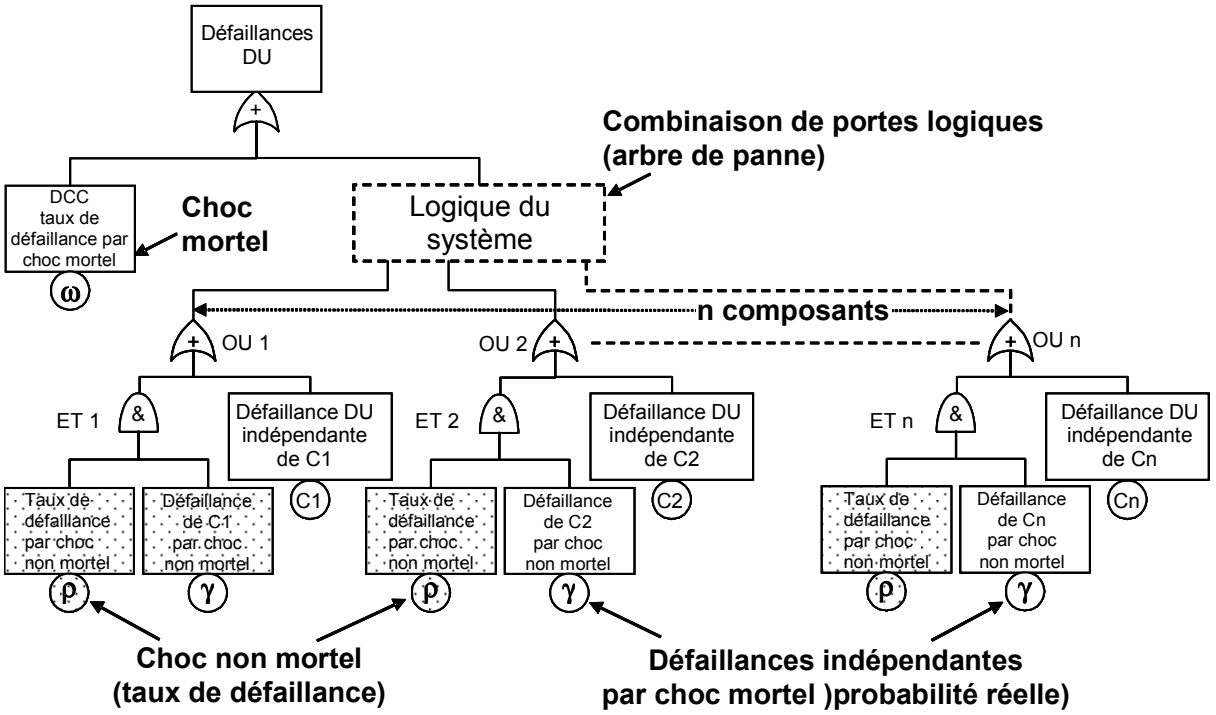


Figure D.2 – Mise en œuvre d'un modèle des chocs avec des arbres de panne

Des composants identiques peuvent être liés au modèle du facteur β en divisant β en deux parties β_L et β_{NL}:

– $\beta = \beta_L + \beta_{NL}$
– taux de défaillance par choc mortel: $\lambda_{DU} \times \beta_L$
– taux de défaillance par choc non mortel: $\lambda_{DU} \times \beta_{NL}$
– taux de défaillance indépendante: $\lambda_{DU}[1 - (\beta_L + \beta_{NL})]$

Dans l'arbre de panne représenté à la Figure D.2, on obtient:

– taux de chocs mortels: $\omega = \lambda_{DU} \times \beta_L$
– taux de chocs non mortels: $\rho = \lambda_{DU} \times \beta_{NL} / \gamma$

Le principal problème réside toujours dans l'évaluation des valeurs des trois paramètres (ω, ρ, γ) ou (β_L, β_{NL}, γ). La référence [19] donne certaines indications et d'autres références sur les traitements statistiques permettant d'évaluer (ω, ρ, γ) à partir du retour d'expérience.

En l'absence de données, il est possible d'utiliser un raisonnement théorique en appliquant des approches pragmatiques. Par exemple, il est possible d'utiliser la procédure suivante avec modélisation par arbre de panne en présence de plus de 3 éléments similaires:

1) estimer β comme dans la méthode du facteur β;
2) considérer que β_L est négligeable ($\beta_{NL} = \beta$);
3) estimer γ pour assurer d'obtenir des résultats prudents. En considérant que les défaillances doubles ont au moins un effet de l'ordre de 10 fois supérieur à la défaillance quadruple (hypothèse de toute évidence prudente), la formule suivante peut être utilisée:

$$\gamma = \sqrt{\frac{C_N^2}{10.C_N^4}}$$

où

N est le nombre d'éléments similaires;

C_N^2 est le nombre de défaillances doubles potentielles; et

C_N^4 est le nombre de défaillances quadruples potentielles

4) calculer ρ en fonction du nombre de N éléments similaires:

$$\rho = \frac{\beta\lambda_{DU}}{C_N^2\gamma^2 + C_N^3\gamma^3}$$

En appliquant cette méthode, les contributeurs de tête sont des défaillances doubles et triples, et les résultats sont prudents comparés à ceux obtenus avec la méthode du facteur β avec seulement 3 composants. La CCF double et les défaillances triples sont correctement prises en compte et les défaillances multiples non réalistes ne sont pas totalement négligées.

Ce modèle est très simple à mettre en œuvre dans les modèles de calcul par arbre de panne tels que ceux présentés dans l'Annexe B, par exemple, arbres de panne en B.4.3. Ceci permet de facilement traiter des systèmes de sécurité comportant de nombreux composants similaires de façon très simple.

D.8 Références

Les références [13] à [15] et [20] et [21] de la Bibliographie donnent des informations utiles en ce qui concerne les défaillances de cause commune.

Annexe E
(informative)

Exemples d'application des tableaux d'intégrité de sécurité logicielle contenus dans la CEI 61508-3

E.1 Généralités

La présente annexe fournit deux exemples de travail pour l'application des tableaux d'intégrité de sécurité logicielle spécifiés à l'Annexe A de la CEI 61508-3:

a) système électronique programmable relatif à la sécurité de niveau 2 d'intégrité de sécurité requis pour un procédé dans une usine chimique;

b) programme d'arrêt réalisé avec un langage de haut niveau, de niveau 3 d'intégrité de sécurité.

Ces exemples illustrent la méthode de sélection potentielle des techniques de développement de logiciels dans différentes circonstances, à partir des tableaux des Annexes A et B de la CEI 61508-3.

Il convient de noter que ces illustrations ne sont pas des applications définitives de la norme à ces exemples. La CEI 61508-3 spécifie clairement en plusieurs points que, compte tenu du grand nombre de facteurs qui affectent la capabilité systématique du logiciel, aucun algorithme de combinaison des techniques et mesures approprié à toute application donnée ne peut être spécifié.

Dans le cas d'un système réel, il convient que toutes les entrées des tableaux soient étayées par une justification documentée de la validité des commentaires et par le fait que ceux-ci constituent une réponse appropriée pour le système en question et l'application. Cette justification est susceptible d'être soutenue par une référence aux recommandations de l'Annexe C de la CEI 61508-3 qui traite des propriétés souhaitables qui, si elles sont réalisées dans la phase du cycle de vie approprié, peuvent justifier la confiance dans le fait que le logiciel définitif a une intégrité de sécurité systématique suffisante.

E.2 Exemple pour le niveau 2 d'intégrité de sécurité

Cet exemple est un système électronique programmable relatif à la sécurité de niveau 2 d'intégrité de sécurité requis pour un procédé dans une usine chimique. Ce système utilise la logique scalaire pour le programme d'application, comme illustration de programmation d'application dans un langage de variabilité limitée.

L'application est composée de plusieurs cuves de réacteur liées par des cuves de stockage intermédiaire qui sont remplies de gaz inerte à certains points du cycle de réaction afin de supprimer inflammation et explosions. Les fonctions du système électronique programmable relatif à la sécurité comprennent: la réception des entrées venant des capteurs, l'alimentation et le verrouillage des vannes, les pompes et les actionneurs, la détection des situations dangereuses et l'activation des alarmes, l'interface avec un système de commande distribué, tel que requis par la spécification des exigences de sécurité.

Hypothèses:

– le contrôleur du système électronique programmable relatif à la sécurité est un PLC;

– l'analyse de danger et de risque a établi qu'un système électronique programmable relatif à la sécurité est exigé, et que le niveau 2 d'intégrité de sécurité est requis dans cette application (par application de la CEI 61508-1 et la CEI 61508-2);
– bien que le contrôleur agisse en temps réel, un temps de réponse seulement relativement faible est nécessaire;
– il y a des interfaces avec un opérateur humain et avec un système de commande distribué;
– le code source du système logiciel et la conception de l'électronique programmable du PLC ne sont pas disponibles pour examen, mais ils ont été qualifiés pour le niveau 2 d'intégrité de sécurité sur la base de la CEI 61508-3;
– le langage utilisé pour la programmation de l'application est une logique scalaire, produit en utilisant le système de développement du fournisseur du PLC;
– le code d'application est nécessaire pour conduire un et un seul type de PLC;
– la totalité du développement du logiciel a été revue par une personne indépendante de l'équipe de développement;
– une personne indépendante de l'équipe logicielle a été témoin et a approuvé les essais de validation;
– les modifications (le cas échéant) nécessitent l'autorisation d'une personne indépendante de l'équipe logicielle.

NOTE 1 Pour la définition d'une personne indépendante, voir la CEI 61508-4.

NOTE 2 Voir les notes de 7.4.2, 7.4.3, 7.4.4 et 7.4.5 de la CEI 61508-3 pour des informations sur la répartition des responsabilités entre le fournisseur et l'utilisateur du PLC lorsqu'une programmation à variabilité limitée est utilisée.

Les tableaux suivants montrent comment l'Annexe A de la CEI 61508-3 peut être interprétée pour cette application.

Tableau E.1 – Spécification des exigences pour la sécurité du logiciel

(voir 7.2 de la CEI 61508-3)

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
1a	Méthodes semi-formelles	Tableau B.7	R	Diagrammes cause-conséquence, diagrammes de séquence, blocs fonctionnels. Typiquement utilisés pour la spécification d'exigences d'application logicielles sur PLC
1b	Méthodes formelles	B.2.2, C.2.4	R	Pas utilisées pour la programmation à variabilité limitée
2	Traçabilité ascendante entre les exigences de sécurité du système et les exigences pour la sécurité du logiciel	C.2.11	R	Vérifier l'exhaustivité: examen pour assurer que toutes les exigences de sécurité du système sont traitées par les exigences pour la sécurité du logiciel
3	Traçabilité descendante entre les exigences de sécurité et les besoins de sécurité perçus	C.2.11	R	Réduire au minimum la complexité et la fonctionnalité: examen pour assurer que toutes les exigences pour la sécurité du logiciel sont réellement nécessaires pour traiter les exigences de sécurité du système
4	Outils de spécification assistée par ordinateur pour prise en charge des techniques/mesures appropriées ci-dessus	B.2.4	R	Outils de développement fournis par le fabricant de PLC

NOTE 1 Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.

NOTE 2 Les exigences pour la sécurité du logiciel ont été spécifiées en langage naturel.

Tableau E.2 – Conception et développement du logiciel – conception de l'architecture du logiciel

(voir 7.4.3 de la CEI 61508-3)

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
1	Détection des anomalies	C.3.1	R	Vérification du domaine de valeur, chien de garde, entrées/sorties, communication. Emettre une alarme en cas d'erreur (voir 3a)
2	Code de détection d'erreurs	C.3.2	R	Inclus dans les options utilisateur - sélection faite avec le soin nécessaire
3a	Programmation d'assertion des défaillances	C.3.3	R	Dédiée à certains programmes PLC à logique scalaire pour soumettre à essai certaines conditions essentielles de sécurité (voir 1)
3b	Techniques de surveillance diversifiées (avec indépendance entre l'ordinateur de surveillance et la fonction surveillée du même ordinateur)	C.3.4	R	Application non préférentielle: plus grande complexité du logiciel pour garantir l'indépendance.
3c	Techniques de surveillance diversifiées (avec indépendance entre l'ordinateur de surveillance et l'ordinateur surveillé)	C.3.4	R	Contrôler les combinaisons d'entrées/sorties autorisées dans un superviseur de sécurité matériel indépendant
3d	Redondance diversifiée, implémentant la même spécification des exigences pour la sécurité du logiciel	C.3.5	---	Application non préférentielle: avantage pour la sécurité insuffisant par rapport à 3c.
3e	Redondance diversifiée sur le plan fonctionnel, implémentant une spécification différente des exigences pour la sécurité du logiciel	C.3.5	---	Application non préférentielle: pratiquement obtenue par 3c.
3f	Récupération par régression	C.3.6	R	Inclus dans les options utilisateur - sélection faite avec le soin nécessaire
3g	Conception de logiciel sans état (ou conception avec état limité)	C.2.12	---	Non utilisée. La commande du processus a besoin des états pour mémoriser l'état de l'installation.
4a	Nouvelle sollicitation des mécanismes de rétablissement après anomalie	C.3.7	R	Utilisés comme requis par l'application (voir 2 et 3c)
4b	Dégradation progressive	C.3.8	R	Pas utilisée pour la programmation à variabilité limitée
5	Intelligence artificielle - correction d'anomalie	C.3.9	NR	Pas utilisée pour la programmation à variabilité limitée
6	Reconfiguration dynamique	C.3.10	NR	Pas utilisée pour la programmation à variabilité limitée
7	Approche modulaire	Tableau B.9	HR	
8	Utilisation de composants logiciels sécurisés/vérifiés (s'ils existent)	C.2.10	HR	Code préexistant de projets antérieurs
9	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et l'architecture du logiciel	C.2.11	R	Vérifier l'exhaustivité: examen pour assurer que toutes les exigences pour la sécurité du logiciel sont traitées par l'architecture du logiciel
10	Traçabilité descendante entre la spécification des exigences pour la sécurité du logiciel et l'architecture du logiciel	C.2.11	R	Réduire au minimum la complexité et la fonctionnalité: examen pour assurer que toutes les exigences de sécurité de l'architecture sont réellement nécessaires pour traiter les exigences pour la sécurité du logiciel.
11a	Méthodes diagrammatiques structurées	C.2.1	HR	Des méthodes de flux de données et des tableaux de données logiques peuvent être utilisés pour représenter au moins l'architecture

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
11b	Méthodes semi-formelles	Tableau B.7	R	Peuvent être utilisées pour l'interface DCS
11c	Méthodes formelles de conception et d'affinement	B.2.2, C.2.4	R	Rarement utilisées pour la programmation à variabilité limitée
11d	Génération automatique de logiciel	C.4.6	R	Non utilisé pour la programmation à variabilité limité
12	Outils de spécification et de conception assistée par ordinateur	B.2.4	R	Outils de développement fournis par le fabricant de PLC
13a	Comportement cyclique, avec temps de cycle maximal garanti	C.3.11	HR	Non utilisé. Surveillance matérielle du temps de cycle du PLC.
13b	Architecture à déclenchement temporel	C.3.11	HR	Non utilisé. Surveillance matérielle du temps de cycle du PLC.
13c	Dirigé par les événements, avec temps de réponse maximal garanti	C.3.11	HR	Non utilisé. Surveillance matérielle du temps de cycle du PLC.
14	Allocation de ressources statiques	C.2.6.3	R	Non utilisée. Aucun problème lié aux ressources dynamiques dans la programmation à variabilité limitée
15	Synchronisation statique de l'accès aux ressources partagées	C.2.6.3	---	Non utilisée. Aucun problème lié aux ressources dynamiques dans la programmation à variabilité limitée

NOTE 1 Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.

NOTE 2 Il n'est pas aisé d'implémenter certaines des techniques ci-dessus lorsqu'on programme dans un langage de variabilité limitée.

Tableau E.3 – Conception et développement du logiciel – outils de support et langages de programmation

(voir 7.4.4 de la CEI 61508-3)

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
1	Langage de programmation approprié	C.4.5	HR	En général logique scalaire, et souvent propriétaire, dépendant du fournisseur du PLC
2	Langage de programmation fortement typé	C.4.1	HR	Non utilisé. Utilisation d'un texte structuré orienté PLC (voir [16] dans la Bibliographie)
3	Sous-ensemble de langage	C.4.2	---	Attention aux instructions «macro» complexes, aux interruptions qui altèrent le cycle de scrutation du PLC, etc.
4a	Outils et traducteurs certifiés	C.4.3	HR	Disponibles chez les fabricants de PLC
4b	Outils et traducteurs dans lesquels on a une confiance accrue résultant de l'utilisation	C.4.4	HR	Kit de développement du fournisseur de PLC; outils maison développés au fil des différents projets

NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.

Tableau E.4 – Conception et développement du logiciel – conception détaillée

(voir 7.4.5 et 7.4.6 de la CEI 61508-3)
(cela comprend la conception du système logiciel,
la conception des modules logiciels et le codage)

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
1a	Méthodes structurées	C.2.1	HR	Pas utilisées pour la programmation à variabilité limitée
1b	Méthodes semi-formelles	Tableau B.7	HR	Diagrammes cause-conséquence, diagrammes de séquence, blocs fonctionnels. Typique de la programmation à variabilité limitée
1c	Méthodes formelles de conception et d'affinement	B.2.2, C.2.4	R	Pas utilisées pour la programmation à variabilité limitée
2	Outils de conception assistée par ordinateur	B.3.5	R	Outils de développement fournis par le fabricant de PLC
3	Programmation défensive	C.2.5	R	Inclus dans le logiciel système
4	Approche modulaire	Tableau B.9	HR	Ordonne et groupe le programme PLC à logique scalaire pour augmenter sa modularité par rapport aux fonctions requises
5	Règles de conception et de codage	C.2.6 Tableau B.1	HR	Conventions maison pour la documentation et la maintenabilité
6	Programmation structurée	C.2.7	HR	Similaire à la modularité dans ce contexte
7	Utilisation de composants sécurisés/ vérifiés (s'ils existent)	C.2.10 C.4.5	HR	Blocs fonctionnels, programmes-pièce
8	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et la conception du logiciel	C.2.11	R	Vérifier l'exhaustivité: examen pour assurer que toutes les exigences pour la sécurité du logiciel sont traitées par la conception du logiciel

NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.

Tableau E.5 – Conception et développement du logiciel – essai et intégration des modules logiciels

(voir 7.4.7 et 7.4.8 de la CEI 61508-3)

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
1	Essai probabiliste	C.5.1	R	Pas utilisé pour la programmation à variabilité limitée
2	Analyse dynamique et essai	B.6.5 Tableau B.2	HR	Utilisé
3	Enregistrement et analyse des données	C.5.2	HR	Enregistrement des cas d'essai et des résultats
4	Essais fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Les données d'entrée sont sélectionnées pour exécuter tous les cas fonctionnels spécifiés, y compris la gestion des erreurs. Cas d'essai issus de diagrammes cause-conséquence, d'analyse des valeurs limites, et du partitionnement des entrées
5	Essais de fonctionnement	Tableau B.6	R	Pas utilisé pour la programmation à variabilité limitée
6	Essais basés sur le modèle	C.5.27	R	Pas utilisé pour la programmation à variabilité limitée
7	Essais d'interface	C.5.3	R	Inclus dans les essais fonctionnels et boîte noire
8	Outils de gestion et d'automatisation des essais	C.4.7	HR	Outils de développement fournis par le fabricant du PLC
9	Traçabilité ascendante entre la spécification de conception du logiciel et les spécifications des modules et de l'essai d'intégration	C.2.11	R	Vérifier l'exhaustivité: examen pour assurer qu'un essai approprié est planifié pour étudier la fonctionnalité de tous les modules et leur intégration aux modules associés de manière appropriée.
10	Vérification formelle	C.5.12	---	Pas utilisée pour la programmation à variabilité
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.6 – Intégration de l'électronique programmable (matériel et logiciel)

(voir 7.5 de la CEI 61508-3)

	Technique/mesure	Réf.	SIL2	Interprétation pour cette application
1	Essais fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Les données d'entrée sont sélectionnées pour exécuter tous les cas fonctionnels spécifiés, y compris la gestion des erreurs. Cas d'essai issus de diagrammes cause-conséquence, d'analyse des valeurs limites, et du partitionnement des entrées
2	Essais de fonctionnement	Tableau B.6	R	Au moment de l'assemblage du système PLC pour l'essai d'acceptation en usine
3	Traçabilité ascendante entre le système et les exigences de conception du logiciel pour l'intégration du matériel/logiciel et les spécifications d'essai d'intégration du matériel/logiciel	C.2.11	R	Examen pour assurer que les essais d'intégration du matériel/logiciel sont appropriés
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.7 – Validation de sécurité du logiciel

(voir 7.7 de la CEI 61508-3)

	Technique/mesure	Réf.	SIL2	Interprétation pour cette application
1	Essai probabiliste	C.5.1	R	Pas utilisé pour la programmation à variabilité limitée
2	Simulation de processus	C.5.18	R	Pas utilisée pour la programmation à variabilité limitée, mais de plus en plus communément utilisée dans le développement des systèmes PLC
3	Modélisation	Tableau B.5	R	Pas utilisée pour la programmation à variabilité limitée, mais de plus en plus communément utilisée dans le développement des systèmes PLC
4	Essais fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Les données d'entrée sont sélectionnées pour exécuter tous les cas fonctionnels spécifiés, y compris la gestion des erreurs. Cas d'essai issus de diagrammes cause-conséquence, d'analyse des valeurs limites, et du partitionnement des entrées
5	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et le plan de validation de la sécurité du logiciel	C.2.11	R	Vérifier l'exhaustivité: examen pour assurer que des essais de validation de logiciel adéquats sont programmés pour traiter les exigences pour la sécurité du logiciel
6	Traçabilité descendante entre le plan de validation de la sécurité du logiciel et la spécification des exigences pour la sécurité du logiciel	C.2.11	R	Réduire au minimum la complexité: examen pour assurer que tous les essais de validation sont adaptés.
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.8 – Modification du logiciel

(voir 7.8 de la CEI 61508-3)

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
1	Analyse d'impact	C.5.23	HR	Une analyse d'impact est effectuée pour étudier comment l'effet des changements proposés est limité par la modularité du système complet
2	Revérification du module logiciel modifié	C.5.23	HR	Répéter les essais déjà faits
3	Revérification des modules logiciels affectés	C.5.23	HR	Répéter les essais déjà faits
4a	Revalidation du système complet	Tableau A.7	R	L'analyse d'impact a montré que la modification est nécessaire. La revalidation est donc effectuée selon les exigences
4b	Validation de non régression	C.5.25	HR	
5	Gestion de configuration logicielle	C.5.24	HR	Référentiels, enregistrement des changements, impact sur d'autres exigences système
6	Enregistrement et analyse de données	C.5.2	HR	Enregistrement des cas d'essai et résultats
7	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et le plan de modification du logiciel (y compris la revérification et la revalidation)	C.2.11	R	Procédures de modification adéquates pour obtenir les exigences pour la sécurité du logiciel
8	Traçabilité descendante entre le plan de modification du logiciel (y compris la revérification et la revalidation) et la spécification des exigences pour la sécurité du logiciel	C.2.11	R	Procédures de modification adéquates pour obtenir les exigences pour la sécurité du logiciel

NOTE Dans les colonnes de références (intitulées Réf.), les références informatives “B.x.x.x”, “C.x.x.x” réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que “Tableau A.x”, “Tableau B.x” réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.

Tableau E.9 – Vérification du logiciel

(voir 7.9 de la CEI 61508-3)

Technique/mesure		Réf.	SIL2	Interprétation pour cette application
1	Preuve formelle	C.5.12	R	Pas utilisée pour la programmation à variabilité limitée
2	Animation de la spécification et de la conception	C.5.26	R	
3	Analyse statique	B.6.4 Tableau B.8	HR	Références croisées écrites de l'utilisation des variables, conditions, etc.
4	Analyse dynamique et essai	B.6.5 Tableau B.2	HR	Banc d'essai automatique pour faciliter les essais de non-régression
5	Traçabilité ascendante entre la spécification de conception du logiciel et le plan de vérification du logiciel (y compris la vérification des données)	C.2.11	R	Vérifier l'exhaustivité: examen pour assurer la réalisation d'un essai de fonctionnalité adéquat.
6	Traçabilité descendante entre le plan de vérification du logiciel (y compris la vérification des données) et la spécification de conception du logiciel	C.2.11	R	Réduire au minimum la complexité: examen pour assurer que tous les essais de vérification sont appropriés.
7	Analyse numérique hors ligne	C.2.13	R	Pas utilisée. La stabilité numérique des calculs n'est pas une préoccupation majeure dans le cas présent
Essai des modules logiciels et intégration		Voir Tableau E.5 de la présente norme		
Essai d'intégration de l'électronique programmable		Voir Tableau E.6 de la présente norme		
Essai du système logiciel (validation)		Voir Tableau E.7 de la présente norme		
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.10 – Evaluation de la sécurité fonctionnelle

(voir Article 8 de la CEI 61508-3)

Evaluation/technique		Réf.	SIL2	Interprétation pour cette application
1	Listes de contrôle	B.2.5	R	Utilisé
2	Tables de décision/de vérité	C.6.1	R	Utilisé à un degré limité
3	Analyse des défaillances	Tableau B.4	R	Diagrammes cause-conséquence au niveau système, mais autrement l'analyse des défaillances n'est pas utilisée pour la programmation à variabilité limitée
4	Analyse des défaillances de cause commune d'un logiciel diversifié (si un logiciel diversifié est effectivement utilisé)	C.6.3	R	Pas utilisée pour la programmation à variabilité limitée
5	Diagramme de blocs de fiabilité	C.6.4	R	Pas utilisé pour la programmation à variabilité limitée
6	Traçabilité ascendante entre les exigences de l'Article 8 et le plan pour l'évaluation de la sécurité fonctionnelle du logiciel	C.2.11	R	Vérifier l'exhaustivité de la couverture de l'évaluation de la sécurité fonctionnelle
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3				

E.3 Exemple pour le niveau 3 d'intégrité de sécurité

Ce second exemple est un programme d'arrêt réalisé avec un langage de haut niveau, de niveau 3 d'intégrité de sécurité.

Le système logiciel est relativement volumineux pour un système de sécurité: plus de 30 000 lignes de code source ont été développées spécifiquement pour le système. Les fonctions intrinsèques usuelles sont également utilisées: au moins deux systèmes d'exploitation différents et le code préexistant de projets antérieurs (éprouvé par une utilisation antérieure). Au total, le système correspond à plus de 100 000 lignes de code source, si celles-ci pouvaient être disponibles en tant que telles.

L'ensemble du matériel (y compris les capteurs et actionneurs) correspond à un système double canal avec ses sorties vers les éléments finaux connectés avec des ET logiques.

Hypothèses:

– bien qu'une réponse rapide ne soit pas exigée, un temps de réponse maximal est garanti;
– il y a des interfaces avec des capteurs, des actionneurs et des signaux vers les opérateurs;
– les codes sources des systèmes d'exploitation, des librairies graphiques et des librairies mathématiques du commerce ne sont pas disponibles;
– le système est susceptible de subir des modifications ultérieures;
– le logiciel développé spécifiquement utilise un des langages procéduraux communs;
– il est partiellement orienté objet;
– toutes les parties dont le code source n'est pas disponible sont diversifiées, les composants logiciels venant de différents fournisseurs, et leur code objet est généré par des traducteurs différents;
– le logiciel s'exécute sur plusieurs processeurs disponibles dans le commerce qui remplissent les exigences de la CEI 61508-2;

– toutes les exigences de la CEI 61508-2 pour maîtriser et éviter les pannes matérielles sont respectées par le système embarqué; et

– le développement logiciel a été évalué par une organisation indépendante.

NOTE Pour la définition d'une organisation indépendante, voir la CEI 61508-4.

Les tableaux suivants montrent comment les tableaux des annexes de la CEI 61508-3 peuvent être interprétés pour cette application.

Tableau E.11 – Spécification des exigences pour la sécurité du logiciel

(voir 7.2 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1a	Méthodes semi-formelles	Tableau B.7	HR	Blocs diagrammes, diagrammes de séquence, diagrammes de transition d'état
1b	Méthodes formelles	B.2.2, C.2.4	R	Seulement exceptionnellement
2	Traçabilité ascendante entre les exigences de sécurité du système et les exigences pour la sécurité du logiciel	C.2.11	HR	Vérifier l'exhaustivité: examen pour assurer que toutes les exigences de sécurité du système sont traitées par les exigences pour la sécurité du logiciel
3	Traçabilité descendante entre les exigences de sécurité et les besoins de sécurité perçus	C.2.11	HR	Réduire au minimum la complexité et la fonctionnalité: examen pour assurer que toutes les exigences pour la sécurité du logiciel sont réellement nécessaires pour traiter les exigences de sécurité du système
4	Outils de spécification assistée par ordinateur pour prise en charge des techniques/mesures appropriées ci-dessus	B.2.4	HR	Outils supportant les méthodes choisies
NOTE Dans les colonnes de références (intitulées Réf.) les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.12 – Conception et développement du logiciel – conception de l'architecture du logiciel

(voir 7.4.3 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1	Détection des anomalies	C.3.1	HR	Utilisé tant que l'on traite les défaillances des capteurs, actionneurs et de la transmission de données et que ces défaillances ne sont pas couvertes par les mesures prises pour le système embarqué selon les exigences de la CEI 61508-2
2	Code de détection d'erreurs	C.3.2	R	Seulement pour les transmissions de données externes
3a	Programmation d'assertion des défaillances	C.3.3	R	La validité des résultats des fonctions d'application est contrôlée
3b	Techniques de surveillance diversifiées (avec indépendance entre l'ordinateur de surveillance et la fonction surveillée du même ordinateur)	C.3.4	R	Application non préférentielle: plus grande complexité du logiciel pour garantir l'indépendance.
3c	Techniques de surveillance diversifiées (avec indépendance entre l'ordinateur de surveillance et l'ordinateur surveillé)	C.3.4	R	Utilisées pour certaines fonctions relatives à la sécurité quand 3a n'est pas utilisé
3d	Redondance diversifiée, mettant en oeuvre la même spécification des exigences pour la sécurité du logiciel	C.3.5	---	Utilisée pour certaines fonctions quand le code source n'est pas disponible
3e	Redondance diversifiée sur le plan fonctionnel, implémentant une spécification différente des exigences pour la sécurité du logiciel	C.3.5	---	Application non préférentielle: pratiquement obtenue par 3c.
3f	Récupération par régression	C.3.7	---	Pas utilisé
3g	Conception de logiciel sans état (ou conception avec état limité)	C.2.12	---	Non utilisée. La commande du processus a besoin des états pour mémoriser l'état de l'installation.
4a	Nouvelle sollicitation des mécanismes de rétablissement après anomalie	C.3.7	---	Pas utilisé
4b	Dégradation progressive	C.3.8	HR	Oui, à cause de la nature du processus technique
5	Intelligence artificielle - correction d'anomalie	C.3.9	NR	Pas utilisé
6	Reconfiguration dynamique	C.3.10	NR	Pas utilisé
7	Approche modulaire	Tableau B.9	HR	Nécessaire à cause de la taille du système
8	Utilisation de composants logiciels sécurisés/vérifiés (s'ils existent)	C.2.10	HR	code pré-existant de projets antérieurs
9	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et l'architecture du logiciel	C.2.11	HR	Examen pour assurer que toutes les exigences pour la sécurité du logiciel sont traitées par l'architecture du logiciel
10	Traçabilité descendante entre la spécification des exigences pour la sécurité du logiciel et l'architecture du logiciel	C.2.11	HR	Réduire au minimum la complexité et la fonctionnalité: examen pour assurer que toutes les exigences de sécurité de l'architecture sont réellement nécessaires pour traiter les exigences pour la sécurité du logiciel
11a	Méthodes diagrammatiques structurées	C.2.1	HR	Nécessaire à cause de la taille du système
11b	Méthodes semi-formelles	Tableau B.7	HR	Blocs diagrammes, diagrammes de séquence, diagrammes de changement d'état

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
11c	Méthodes formelles de conception et d'affinement	B.2.2, C.2.4	R	Pas utilisé
11d	Génération automatique de logiciels	C.4.6	R	Pas utilisé. Eviter l'incertitude des traducteurs/générateurs.
12	Outils de spécification et de conception assistées par ordinateur	B.2.4	HR	Outils supportant la méthode choisie
13aa	Comportement cyclique, avec temps de cycle maximal garanti	C.3.11	HR	Non utilisé.
13b	Architecture à déclenchement temporel	C.3.11	HR	Non utilisé.
13c	Dirigé par les événements, avec temps de réponse maximal garanti	C.3.11	HR	Non utilisé.
14	Allocation de ressources statiques	C.2.6.3	HR	Non utilisée. Choisir un langage de programmation pour éviter les problèmes liés aux ressources dynamiques
15	Synchronisation statique de l'accès aux ressources partagées	C.2.6.3	R	Non utilisée. Choisir un langage de programmation pour éviter les problèmes liés aux ressources dynamiques
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.13 – Conception et développement du logiciel – outils de support et langage de programmation

(voir 7.4.4 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1	Langage de programmation approprié	C.4.5	HR	Langage à forte variabilité de haut niveau sélectionné
2	Langage de programmation fortement typé	C.4.1	HR	Utilisé
3	Sous-ensemble de langage	C.4.2	HR	Sous-ensemble défini pour le langage utilisé
4a	Outils et traducteurs certifiés	C.4.3	HR	Pas disponibles
4b	Outils et traducteurs dans lesquels on a une confiance accrue résultant de l'utilisation	C.4.4	HR	Disponibles et utilisés
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.14 – Conception et développement du logiciel – conception détaillée

(voir 7.4.5 et 7.4.6 de la CEI 61508-3)
(cela comprend la conception du système logiciel,
la conception des modules logiciels et le codage)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1a	Méthodes structurées	C.2.1	HR	Largement utilisé. En particulier SADT et JSD
1b	Méthodes semi-formelles	Tableau B.7	HR	Machines à états finis/ diagrammes de transition d'état, blocs diagrammes, diagrammes de séquence
1c	Méthodes formelles de conception et d'affinement	B.2.2, C.2.4	R	Seulement exceptionnellement, seulement pour des composants élémentaires
2	Outils de conception assistée par ordinateur	B.3.5	HR	Utilisés pour les méthodes choisies
3	Programmation défensive	C.2.5	HR	Toutes les mesures sauf celles qui sont utilisées automatiquement par le compilateur sont utilisées explicitement pour le logiciel d'application là où elles sont efficaces
4	Approche modulaire	Tableau B.9	HR	Taille limite pour les modules logiciels, masquage/encapsulation des informations, un point d'entrée/un point de sortie dans les sous-programmes et fonctions, interface complètement définie, …
5	Règles de conception et de codage	C.2.6 Tableau B.1	HR	Utilisation de règle de codage, pas d'objet dynamique, pas de variables dynamiques, utilisation limitée des interruptions, utilisation limitée des pointeurs, utilisation limitée de la récursion, pas de sauts inconditionnels, …
6	Programmation structurée	C.2.7	HR	Utilisée
7	Utilisation de composants logiciels sécurisés/ vérifiés (s'ils existent)	C.2.10	HR	Disponible et utilisée
8	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et la conception du logiciel	C.2.11	HR	Examen pour assurer que toutes les exigences pour la sécurité du logiciel sont traitées par la conception du logiciel

NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.

Tableau E.15 – Conception et développement du logiciel – essai et intégration des modules logiciels

(voir 7.4.7 et 7.4.8 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1	Essai probabiliste	C.5.1	R	Utilisé pour les modules logiciels lorsque le code source n'est pas disponible et que la définition des valeurs limites et des classes d'équivalence pour les données d'essai est difficile
2	Analyse dynamique et essai	B.6.5 Tableau B.2	HR	Utilisé pour les modules logiciels lorsque le code source est disponible. Cas d'essai à partir de l'analyse de valeurs limites, modélisation du fonctionnement, classes d'équivalence et partitionnement des entrées, essai structuré
3	Enregistrement et analyse de données	C.5.2	HR	Enregistrement des cas d'essais et des résultats
4	Essais fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Utilisé pour les essais des modules logiciels lorsque le code source n'est pas disponible et pour l'essai d'intégration. Les données d'entrées sont choisies pour simuler tous les cas fonctionnels spécifiés, y compris la gestion des erreurs. Les cas d'essai sont choisis à partir du diagramme cause-conséquence, le prototypage, l'analyse des valeurs limites, les classes d'équivalence et le partitionnement des entrées
5	Essai de fonctionnement	Tableau B.6	HR	Utilisé lors des essais d'intégration sur le matériel cible
6	Essais basés sur le modèle	C.5.27	HR	Pas utilisés
7	Essais d'interface	C.5.3	HR	Inclus dans les essais fonctionnels et boîte noire
8	Outils de gestion et d'automatisation des essais	C.4.7	HR	Utilisés s'ils existent
8	Traçabilité ascendante entre la spécification de conception du logiciel et les spécifications de modules et d'essai d'intégration	C.2.11	HR	Examen pour assurer que les essais d'intégration sont suffisants
9	Vérification formelle	C.5.12	R	Pas utilisée

NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.

Tableau E.16 – Intégration de l'électronique programmable (matériel et logiciel)

(voir 7.5 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1	Essais fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Utilisé en tant qu'essais supplémentaires aux essais d'intégration du logiciel (voir Tableau E.15 ci-dessus) Les données d'entrées sont choisies pour simuler tous les cas fonctionnels spécifiés, y compris la gestion des erreurs. Les cas d'essai sont choisis à partir du diagramme cause-conséquence, le prototypage, l'analyse des valeurs limites, les classes d'équivalence et le partitionnement des entrées
2	Essais de fonctionnement	Tableau B.6	HR	Largement utilisé
3	Traçabilité ascendante entre le système et les exigences de conception du logiciel pour l'intégration du matériel/logiciel et les spécifications d'essai d'intégration du matériel/logiciel	C.2.11	HR	Examen pour assurer que les essais d'intégration sont suffisants
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.17 – Validation de sécurité du logiciel

(voir 7.7 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1	Essai probabiliste	C.5.1	R	Pas utilisé pour la validation
2	Simulation de processus	C.5.18	HR	Machines à états finis, modélisation du fonctionnement, prototypage et animation
3	Modélisation	Tableau B.5	HR	Pas utilisé pour la validation
4	Essais fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Les données d'entrées sont choisies pour simuler tous les cas fonctionnels spécifiés, y compris la gestion des erreurs. Les cas d'essai sont choisis à partir du diagramme cause-conséquence, l'analyse des valeurs limites et le partitionnement des entrées
5	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et le plan de validation de la sécurité du logiciel	C.2.11	HR	Vérifier l'exhaustivité: examen pour assurer que toutes les exigences pour la sécurité du logiciel sont traitées par le plan de validation
6	Traçabilité descendante entre le plan de validation de la sécurité du logiciel et la spécification des exigences pour la sécurité du logiciel	C.2.11	HR	Réduire au minimum la complexité: examen pour assurer que tous les essais de validation sont pertinents
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.18 – Modification du logiciel

(voir 7.8 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1	Analyse d'impact	C.5.23	HR	Utilisé
2	Revérification du module logiciel modifié	C.5.23	HR	Utilisé
3	Revérification des modules logiciels affectés	C.5.23	HR	Utilisé
4a	Revalidation du système complet	Tableau A.7	HR	Dépend du résultat de l'analyse d'impact
4b	Validation de non régression	C.5.25	HR	Utilisé
5	Gestion de configuration logicielle	C.5.24	HR	Utilisé
6	Enregistrement et analyse de données	C.5.2	HR	Utilisé
7	Traçabilité ascendante entre la spécification des exigences pour la sécurité du logiciel et le plan de modification du logiciel (y compris la revérification et la revalidation)	C.2.11	HR	Vérifier l'exhaustivité: examen pour assurer que les procédures de modification sont appropriées aux exigences pour la sécurité du logiciel
8	Traçabilité descendante entre le plan de modification du logiciel (y compris la revérification et la revalidation) et la spécification des exigences pour la sécurité du logiciel	C.2.11	HR	Réduire au minimum la complexité: examen pour assurer que toutes les procédures de modification sont nécessaires
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.19 – Vérification du logiciel

(voir 7.9 de la CEI 61508-3)

Technique/mesure		Réf.	SIL3	Interprétation pour cette application
1	Preuve formelle	C.5.12	R	Exceptionnellement seulement, pour des classes très élémentaires
2	Animation de la spécification et de la conception	C.5.26	R	Pas utilisée
3	Analyse statique	B.6.4 Tableau B.8 C.5.14	HR	Pour tous les codes nouvellement développés. Analyse des valeurs limites, listes de contrôle, analyse du flux de commandes, analyse du flux de données, inspections selon Fagan, revues de conception
4	Analyse dynamique et essai	B.6.5 Tableau B.2	HR	Pour tous les codes nouvellement développés
5	Traçabilité ascendante entre la spécification de conception du logiciel et le plan de vérification du logiciel (y compris la vérification des données)	C.2.11	HR	Vérifier l'exhaustivité: examen pour assurer que les procédures de modification sont appropriées aux exigences pour la sécurité du logiciel
6	Traçabilité descendante entre le plan de vérification du logiciel (y compris la vérification des données) et la spécification de conception du logiciel	C.2.11	HR	Réduire au minimum la complexité: examen pour assurer que toutes les procédures de modification sont nécessaires
7	Analyse numérique hors ligne	C.2.13	HR	Pas utilisée. La stabilité numérique des calculs n'est pas une préoccupation majeure dans le cas présent
Essai des modules logiciels et intégration		Voir Tableau E.15 de la présente norme		
Essai d'intégration de l'électronique programmable		Voir Tableau E.16 de la présente norme		
Essai du système logiciel (validation)		Voir Tableau E.17 de la présente norme		
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Tableau E.20 – Evaluation de la sécurité fonctionnelle

(voir Article 8 de la CEI 61508-3)

Evaluation/technique		Réf.	SIL3	Interprétation dans cette application
1	Listes de contrôle	B.2.5	R	Utilisé
2	Tables de décision/de vérité	C.6.1	R	Utilisé, dans certaines limites
3	Analyse des défaillances	Tableau B.4	HR	L'analyse par arbre de panne est largement utilisée, et les diagrammes cause-conséquence sont utilisés dans certaines limites
4	Analyse des défaillances de cause commune d'un logiciel diversifié (si un logiciel diversifié est effectivement utilisé)	C.6.3	HR	Utilisé
5	Diagramme de blocs de fiabilité	C.6.4	R	Utilisé
6	Traçabilité ascendante entre les exigences de l'Article 8 et le plan pour l'évaluation de la sécurité fonctionnelle du logiciel	C.2.11	HR	Vérifier l'exhaustivité de la couverture de l'évaluation de la sécurité fonctionnelle
NOTE Dans les colonnes de références (intitulées Réf.), les références informatives "B.x.x.x", "C.x.x.x" réfèrent aux descriptions des techniques des Annexes B et C de la CEI 61508-7, tandis que "Tableau A.x", "Tableau B.x" réfèrent aux tableaux de techniques des Annexes A et B de la CEI 61508-3.				

Bibliographie

[1] CEI 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[2] CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[3] CEI 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional* (disponible en anglais seulement)

Les références suivantes fournissent des détails supplémentaires sur l'évaluation des probabilités de défaillance (voir Annexe B).

[4] CEI 61078:2006, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

[5] CEI 61165:2006, *Application des techniques de Markov*

[6] BS 5760, *Reliability of system equipment and components – Part 2: Guide to assessment of reliability* (disponible en anglais seulement)

[7] D. J. SMITH, *Reliability, maintainability and risk – Practical methods for engineers*, Butterworth-Heinemann, 5th edition, 1997, ISBN 0-7506-3752-8 (disponible en anglais seulement)

[8] R. BILLINGTON AND R. N. ALLAN, *Reliability evaluation of engineering systems*, Plenum, 1992, ISBN 0-306-44063-6 (disponible en anglais seulement)

[9] W. M. GOBLE, *Evaluating control system reliability – Techniques and applications*, Instrument Society of America, 1992, ISBN 1-55617-128-5 (disponible en anglais seulement)

Les références suivantes sont utiles pour le calcul de la couverture de diagnostic (voir Annexe C).

[10] Reliability Analysis Center (RAC), *Failure Mode/Mechanism Distributions,* 1991, Department of Defense, United States of America, PO Box 4700, 201 Mill Street, Rome, NY 13440-8200, Organization report number: FMD-91, NSN 7540-01-280-5500 (disponible en anglais seulement)

[11] ALLESSANDRO BIROLINI, *Qualität und Zuverlassigkeit technischer Systeme, Theorie, Praxis, Management,* Dritte Auflage,1991, Springer-Verlag, Berlin Heidelberg New York, ISBN 3-540-54067-9, 3 Aufl., ISBN 0-387-54067-9 3 ed. (disponible en allemand seulement)

[12] MIL-HDBK-217F, *Military Handbook Reliability prediction of electronic equipment,* 2 December 1991, Department of Defense, United States of America (disponible en anglais seulement)

Les références suivantes donnent des informations utiles en ce qui concerne les défaillances de cause commune (voir Annexe D).

[13] *Health and Safety Executive Books*, email hsebooks@prolog.uk.com (disponible en anglais seulement)

[14] R. HUMPHREYS, A., PROC., *Assigning a numerical value to the beta factor common-cause evaluation,* Reliability 1987 (disponible en anglais seulement)

[15] UPM3.1, *A pragmatic approach to dependent failures assessment for standard systems*, AEA Technology, Report SRDA-R-13, ISBN 085 356 4337, 1996 (disponible en anglais seulement)

Il est fait référence à la norme suivante dans le Tableau E.3.

[16] CEI 61131-3:2003, *Programmable controllers – Part 3: Programming languages* (disponible en anglais seulement)

[17] ISA-TR84.00.02-2002 – Parts 1-5, *Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques Package* (disponible en anglais seulement)

[18] CEI 61025:2006, *Analyse par arbre de panne (AAP)*

[19] CEI 62551, *Techniques d'analyse pour la sûreté de fonctionnement – Technique des réseaux de Pétri*[10]

[20] ANIELLO AMENDOLA, kluwer academic publisher, ISPRA 16-19 November 1987, *Advanced seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment,* ISBN 0-7923-0268-0 (disponible en anglais seulement)

[21] CORWIN L. ATWOOD, *The Binomial Failure Rate Common Cause Model,* Technometrics May 1986 Vol 28 n°2 (disponible en anglais seulement)

[22] A. ARNOLD, A. GRIFFAULT, G. POINT, AND A. RAUZY. *The altarica language and its semantics*. *Fundamenta Informaticae*, 34,pp.109–124, 2000 (disponible en anglais seulement)

[23] M. BOITEAU, Y. DUTUIT, A. RAUZY AND J.-P. SIGNORET, The AltaRica *Data-Flow Language in Use: Assessment of Production Availability of a MultiStates System*, *Reliability Engineering and System Safety*, Elsevier, Vol. 91, pp 747-755 (disponible en anglais seulement)

[24] A. RAUZY. *Mode automata and their compilation into fault trees. Reliability Engineering and System Safety*, Elsevier 2002, Volume 78, Issue 1, pp 1-12 (disponible en anglais seulement)

[25] For PDS method; see <www.sintef.no/pds>; and further background material in:Hokstad, Per; Corneliussen, Kjell Source: Reliability Engineering and System Safety, v 83, n 1, p 111-120, January 2004 (disponible en anglais seulement)

[26] CEI 60601 (toutes les parties), *Appareils électromédicaux*

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

10 A l'étude.

[28] CEI 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques /électroniques /électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

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

_____

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