NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61508-6

Première édition
First edition
2000-04

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

Functional safety of electrical/electronic/ programmable electronic safety-related systems –

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

Numéro de référence
Reference number
CEI/IEC 61508-6:2000

Numéros des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000.

Publications consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles dans le Catalogue de la CEI.

Les renseignements relatifs à des questions à l'étude et des travaux en cours entrepris par le comité technique qui a établi cette publication, ainsi que la liste des publications établies, se trouvent dans les documents ci-dessous:

- **«Site web» de la CEI***
- **Catalogue des publications de la CEI**
  Publié annuellement et mis à jour régulièrement
  (Catalogue en ligne)*
- **Bulletin de la CEI**
  Disponible à la fois au «site web» de la CEI* et comme périodique imprimé

Terminologie, symboles graphiques et littéraux

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 60050: *Vocabulaire Electrotechnique International* (VEI).

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60027: *Symboles littéraux à utiliser en électrotechnique,* la CEI 60417: S*ymboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles,* et la CEI 60617: *Symboles graphiques pour schémas.*

* Voir adresse «site web» sur la page de titre.

Numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series.

Consolidated publications

Consolidated versions of some IEC publications including amendments are available. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available in the IEC catalogue.

Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is to be found at the following IEC sources:

- **IEC web site***
- **Catalogue of IEC publications**
  Published yearly with regular updates
  (On-line catalogue)*
- **IEC Bulletin**
  Available both at the IEC web site* and as a printed periodical

Terminology, graphical and letter symbols

For general terminology, readers are referred to IEC 60050: *International Electrotechnical Vocabulary* (IEV).

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications IEC 60027: *Letter symbols to be used in electrical technology*, IEC 60417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets* and IEC 60617: *Graphical symbols for diagrams.*

* See web site address on title page.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61508-6

Première édition
First edition
2000-04

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

Functional safety of electrical/electronic/ programmable electronic safety-related systems –

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

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http://www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XB

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

Pages

CONTENTS

Pages

Page

Pages

Page

Pages

Page

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 CEI (Commission Electrotechnique Internationale) est une organisation internationale de normalisation composée de tous les comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour but de promouvoir la coopération internationale en matière de normalisation dans les domaines de l'électricité et de l'électronique. A cette fin et en plus d'autres activités, la CEI publie des Normes internationales. Leur préparation est confiée aux comités d'études; il est permis à tout Comité national intéressé par le sujet traité de participer à ces travaux préparatoires. Les organisations internationales, gouvernementales et non gouvernementales qui assurent la liaison avec la CEI participent également à cette préparation. La CEI travaille en collaboration étroite avec l'Organisation internationale de normalisation (ISO), conformément aux conditions de l'accord passé entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques, représentent, dans la mesure du possible un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure du possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
6) L'attention est attirée sur le fait que certains éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61508-6 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure et commande dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/295/FDIS	65A/304/RVD

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

Les annexes A à E sont données uniquement à titre d'information.

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

– Partie 1: Prescriptions générales
– Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

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

IEC 61508-6 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

FDIS	Report on voting
65A/295/FDIS	65A/304/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annexes A to E are for information only.

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

– Part 1: General requirements
– Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

– Partie 3: Prescriptions concernant les logiciels
– Partie 4: Définitions et abréviations
– Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité
– Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et la CEI 61508-3
– Partie 7: Présentation de techniques et mesures

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2005. A cette date, la publication sera

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

– Part 3: Software requirements
– Part 4: Definitions and abbreviations
– Part 5: Examples of methods for the determination of safety integrity levels
– Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
– Part 7: Overview of techniques and measures

The committee has decided that the contents of this publication will remain unchanged until 2005. At this date, the publication will be

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

INTRODUCTION

Les systèmes électriques/électroniques sont utilisés depuis des années pour exécuter des fonctions liées à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (que l'on nommera de façon générique «systèmes électroniques programmables (PES)» sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non liées à la sécurité, mais aussi de plus en plus souvent liées à la sécurité. Si l'on veut exploiter efficacement, et en toute sécurité, la technologie des systèmes informatiques, il est indispensable de fournir à tous les responsables suffisamment d'éléments liés à la sécurité pour les guider dans leurs prises de décisions.

La présente Norme internationale présente une approche générique de toutes les activités liées au cycle de vie de sécurité de systèmes électriques/électroniques/électroniques programmables (E/E/PES) qui sont utilisés pour réaliser des fonctions de sécurité. Cette approche unifiée a été adoptée afin de développer une politique technique rationnelle et cohérente concernant tous les appareils électriques liés à la sécurité. L'un des principaux objectifs poursuivis consiste à faciliter l'élaboration de normes par secteur d'application.

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes de protection fondés sur diverses technologies (par exemple mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). En conséquence, il est nécessaire que toute stratégie de sécurité prenne non seulement en compte tous les éléments d'un système individuel (par exemple les capteurs, les appareils de commande, les actionneurs), mais aussi qu'elle considère tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. C'est pourquoi la présente Norme internationale, bien que traitant essentiellement des systèmes E/E/PE relatifs à la sécurité, fournit néanmoins un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

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

La présente Norme internationale

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

– a été élaborée dans le souci de l'évolution rapide des technologies – le cadre est suffisamment solide et étendu pour pourvoir aux évolutions futures;

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

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

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

INTRODUCTION

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

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

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

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

This International Standard

– considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs are used to perform safety functions;

– has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;

– enables application sector international standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector international standards, within the framework of this International Standard, should lead to a high level of consistency (for example, of underlying principles, terminology, etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;

– provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;

– uses safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

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

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

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

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

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

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

– adopte une large gamme de principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, mais ne dépend pas du concept de sécurité intrinsèque qui peut être intéressant lorsque les modes de défaillances sont bien définis et que le niveau de complexité est relativement faible. Le concept de sécurité intrinsèque a été considéré comme inadéquat en raison de l'immense gamme de complexité des systèmes E/E/PE relatifs à la sécurité qui entrent dans le domaine d'application de la présente norme.

– adopts a risk-based approach for the determination of the safety integrity level requirements;

– sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in

  - a low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand,
  - a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

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

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 prescriptions de la CEI 61508-2 et 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 avec le paragraphe 7.4.3 et l'annexe C de la CEI 61508-2, et l'annexe D.

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

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

NOTE Aux Etats-Unis d'Amérique et au Canada, les normes nationales de sécurité des processus existantes, basées sur la CEI 61508 (par exemple l'ANSI/ISA S48.01-1996) peuvent être appliquées dans le domaine des processus, à la place de la CEI 61508, et cela jusqu'à ce que les normes internationales concernant la mise en oeuvre de la CEI 61508 (soit la CEI 61511) dans le domaine des processus soient publiées.

1.4 La figure 1 montre la structure générale des parties 1 à 7 et indique le rôle que la présente CEI 61508-6 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

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 3.4.4 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and IEC/ISO Guide 51. IEC 61508 is also intended for use as a stand-alone standard.

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 do not apply unless specifically referred to or included in the publications prepared by those technical committees.

NOTE In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC 61508.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of this standard and indicates the role that IEC 61508-6 plays in the achievement of functional safety for E/E/PE safety-related systems.

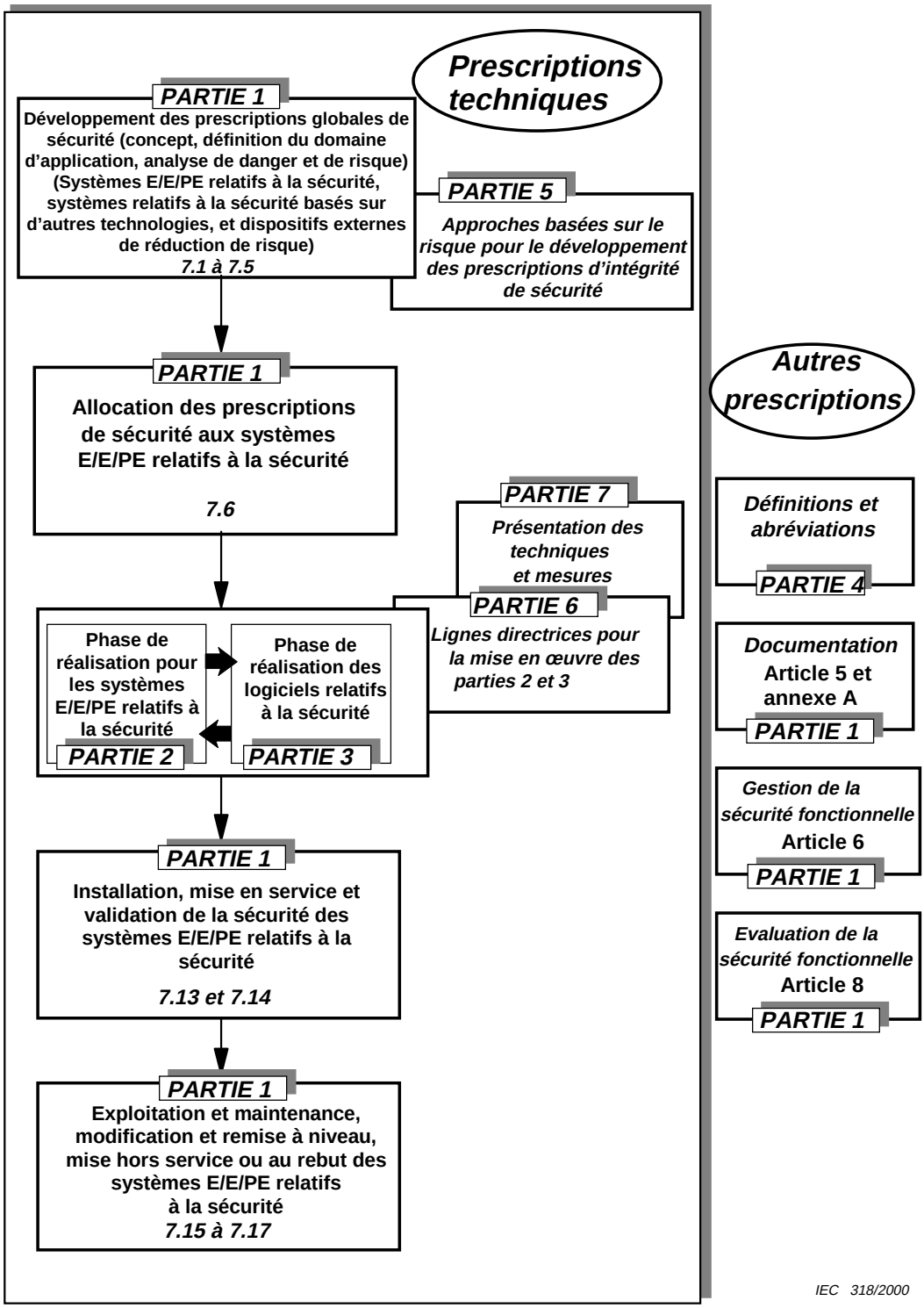


Figure 1 – Structure générale de la CEI 61508

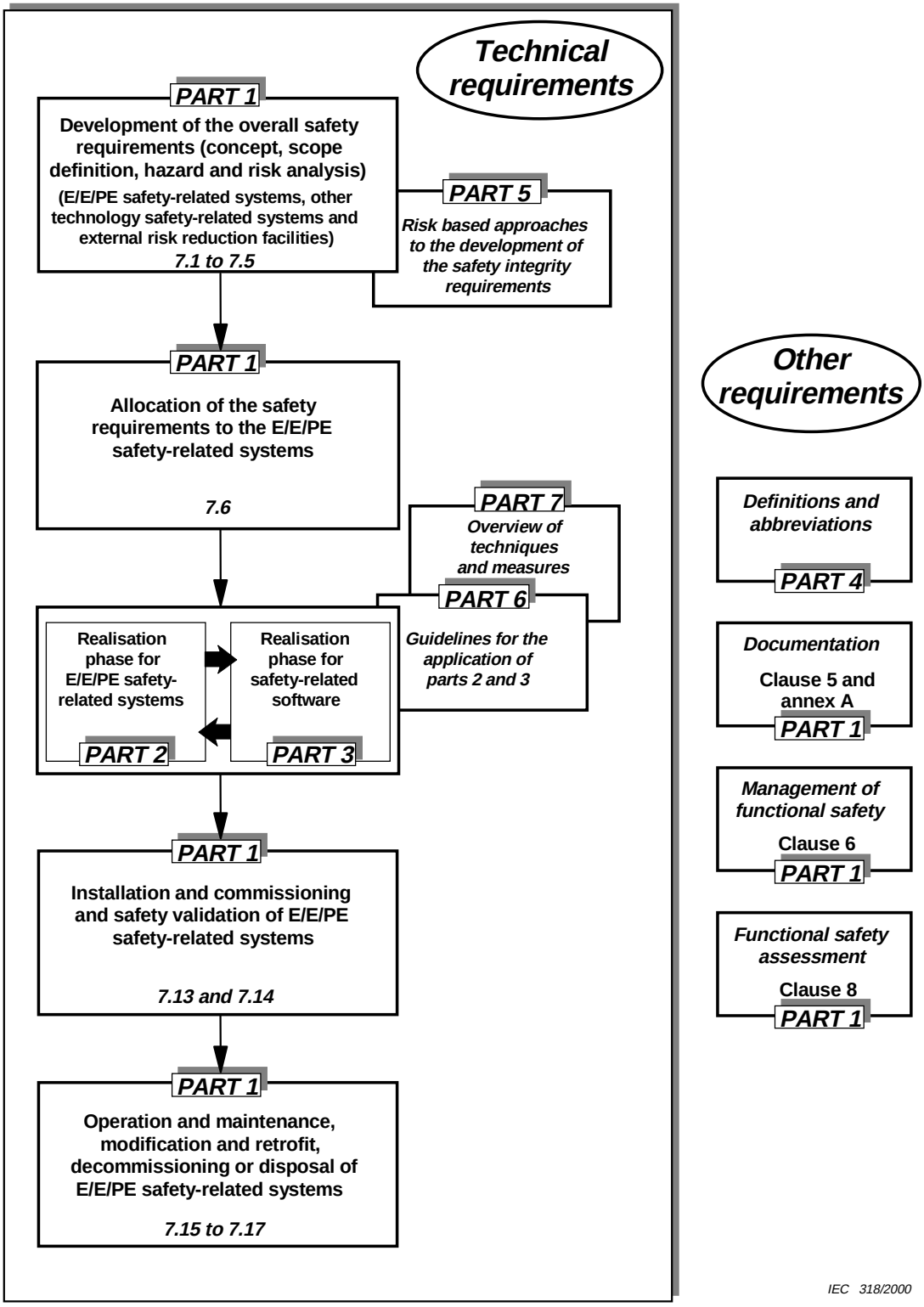


Figure 1 – Overall framework of IEC 61508

2 Références normatives

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

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

Guide CEI 104:1997, *Guide pour la rédaction des normes de sécurité et rôle des comités chargés de fonctions pilotes de sécurité et de fonctions groupées de sécurité*

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

3 Définitions et abréviations

Pour les besoins de la présente norme, les définitions et les abréviations données dans la CEI 61508-4 s'appliquent.

2 Normative references

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

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC Guide 104:1997, *Guide to the drafting of safety standards and the rôle of committees with safety pilot functions and safety group functions*

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

3 Definitions and abbreviations

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

Annexe A
(informative)

Application de la CEI 61508-2 et de la CEI 61508-3

A.1 Généralités

Les machines, les installations de transformation et autres équipements peuvent, en cas de dysfonctionnement (par exemple en raison de défaillances de dispositifs électromécaniques, électroniques et/ou électroniques programmables), présenter des risques pour les individus et l'environnement résultant d'événements dangereux tels que les incendies, explosions, surdoses de radiations, emprisonnement, 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 l'évitement et/ou la maîtrise de défaillances de dispositifs électromécaniques, électroniques ou électroniques programmables.

Le principal objectif est de s'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 pourraient 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 de risque 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 des risques 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 prescriptions relatives à l'intégrité de sécurité affectée à tout système, dit système E/E/P/E relatif à sécurité, par l'application de la CEI 61508-1 et établissent les prescriptions 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
– se concentrent sur les moyens d'évitement et/ou de maîtrise des défaillances aléatoires de matériel et des défaillances systématiques (les cycles de vie de sécurité des E/E/PES et du logiciel [3)]).

———————

1) Les systèmes nécessaires à la sécurité fonctionnelle et contenant un ou plusieurs dispositifs électriques (électromécaniques), électroniques ou électroniques programmables (E/E/PE) dit des systèmes E/E/PE relatifs à la sécurité et comprennent tout le matériel nécessaire pour réaliser la fonction de sécurité requise (voir 3.4.1 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 7.6.2.9 de la CEI 61508-1).

3) Pour permettre une structure claire des prescriptions de la présente norme, il a été décidé d'ordonner les prescriptions 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 6 de la CEI 61508-1).

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 electro-mechanical, 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/PES 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 3.4.1 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 7.6.2.9 of IEC 61508-1).

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 6 of IEC 61508-1).

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 prescriptions de la CEI 61508-2 et de la CEI 61508-3 comprennent

– l'application de mesures et techniques [1)], classées en fonction du niveau d'intégrité de sécurité, afin d'éviter des défaillances systématiques [2)] 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 des 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 prescriptions de tolérance aux anomalies de matériel (voir tableaux 2 et 3 de la CEI 61508-2); et
– la couverture du diagnostic et la fréquence des tests 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;
– l'utilisation de personnel compétent;
– l'application des activités spécifiées du cycle de vie de sécurité, y compris les techniques et mesures spécifiées [3)]; et
– une évaluation indépendante de la sécurité fonctionnelle [4)].

Le principal objectif est de s'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.

La CEI 61508-2 a été élaborée afin de fournir des prescriptions permettant de réaliser une intégrité de sécurité du matériel [5)] des systèmes E/E/PE relatifs à la sécurité, y compris les capteurs et éléments finaux. Des techniques et mesures sont prescrites 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 prescriptions sont fournies pour l'interface opérateur. Des techniques et mesures de test 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.

———————

1) 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 la CEI 61508-3.

2) 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).

3) Des mesures alternatives à celles spécifiées dans la présente norme sont acceptables à condition qu'elles soient justifiées par écrit lors de la planification de la sécurité (voir l'article 6 de la CEI 61508-1).

4) Une évaluation indépendante n'implique pas forcément une évaluation par une tierce partie (voir l'article 8 de la CEI 61508-1).

5) Y compris les logiciels fixes intégrés ou logiciels équivalents (également appelés microprogrammes), tels que les circuits intégrés spécifiques à l'application (ASIC).

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 [1], which are graded against the safety integrity level, for the avoidance of systematic failures [2] 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 [3]; and

– an independent functional safety assessment [4].

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 [5] 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.

———————————

1) 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.

2) 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).

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

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

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

La CEI 61508-3 a été élaborée afin de fournir des prescriptions 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 de conception. La CEI 61508-3 prescrit 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 E/E/PES. 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 prescriptions de sécurité (voir CEI 61508-1). Mettre à jour la planification de la sécurité de manière adéquate pendant le développement de l'E/E/PES.

b) Déterminer les prescriptions de sécurité E/E/PES, y compris les prescriptions relatives à l'intégrité de sécurité, pour chaque fonction de sécurité (voir 7.2 de la CEI 61508-2). Attribuer des prescriptions au logiciel et les transmettre au fournisseur et/ou au développeur du logiciel pour l'application de la CEI 61508-3.

   NOTE Il est nécessaire de prendre en compte à ce stade la possibilité de défaillances coïncidentes du système de commande EUC et du (des) système(s) E/E/PE relatif(s) à la sécurité (voir 7.5.2.4 de la CEI 61508-1). Ces défaillances peuvent résulter des défaillances de composants ayant une cause commune, par exemple des influences environnementales similaires. L'existence de telles défaillances pourrait conduire à un risque résiduel plus élevé que prévu si les précautions appropriées n'étaient pas prises.

c) Entamer la phase de planification pour la validation de sécurité E/E/PES (voir 7.3 de la CEI 61508-2).

d) Spécifier l'architecture (configuration) pour le sous-système logique E/E/PES, capteurs et éléments finaux. Revoir, avec le fournisseur/développeur de logiciel, 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) Etablir 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 tests périodiques pour des défaillances qui ne sont pas automatiquement révélées;

   – le durée moyenne de rétablissement;

   – la couverture du diagnostic (voir annexe C de la CEI 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 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/PES. 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/PES development.

b) Determine the requirements for E/E/PES safety, 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 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 7.5.2.4 of IEC 61508-1). 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/PES safety validation (see 7.3 of IEC 61508-2).

d) Specify the architecture (configuration) for the E/E/PES 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 (components), 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);

- la probabilité de défaillance; et
- la proportion de défaillances en sécurité (voir annexe C de la CEI 61508-2).

g) Déterminer les contraintes architecturales (voir tableaux 2 et 3 de la CEI 61508-2)

h) Créer un modèle de fiabilité pour chacune des fonctions de sécurité exigées pour le système E/E/PE relatif à la sécurité.

NOTE 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.

i) Calculer une prévision de fiabilité pour chaque fonction en utilisant une technique appropriée. Comparer le résultat avec la mesure de défaillance cible déterminé en b) ci-dessus et les prescriptions des tableaux 2 et 3 de la CEI 61508-2 (voir 7.4.3.1 de la CEI 61508-2). Si la fiabilité prévue ne satisfait pas à la mesure de défaillance cible et/ou ne remplit pas les prescriptions des tableaux 2 et 3 de la CEI 61508-2, 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 Plusieurs méthodes de modélisation sont disponibles et il convient que l'analyste choisisse la plus appropriée (voir note 9 du 7.4.3.2.2 de la CEI 61508-2, qui donne une liste de quelques méthodes qui pourraient être utilisées).

j) Mettre en oeuvre la conception d'un 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).

k) 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 suivront lors de l'exploitation du système (voir 7.6 de la partie 2 et l'annexe B de la CEI 61508-2). Inclure des aspects logiciels (voir A.3 f)).

l) En collaboration avec le développeur du logiciel (voir 7.7 de la CEI 61508-3), valider le système E/E/PES (voir 7.7 de la CEI 61508-2 et l'annexe B de la CEI 61508-2).

m) Remettre le matériel et les résultats de la validation de sécurité E/E/PES aux ingénieurs système pour intégration ultérieure dans le système global.

n) Si une maintenance/modification de l'E/E/PES 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/PES. 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 susmentionnées, les techniques et mesures de sécurité de l'E/E/PES exigées 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 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).

- the probability of failure; and
- the safe failure fraction (see annex C of IEC 61508-2).

g) Determine the architectural constraints (see tables 2 and 3 of IEC 61508-2).

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

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

i) 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 tables 2 and 3 of IEC 61508-2 (see 7.4.3.1 of IEC 61508-2). If the predicted reliability does not meet the target failure measure and/or does not meet the requirements of tables 2 and 3 of IEC 61508-2, 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 A number of modelling methods are available and the analyst should choose which is the most appropriate (see 7.4.3.2.2 note 9 of IEC 61508-2 for a list of some methods that could be used).

j) 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).

k) 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)).

l) Together with the software developer (see 7.7 of IEC 61508-3), validate the E/E/PES (see 7.7 of IEC 61508-2 and annex B of IEC 61508-2).

m) Hand over the hardware and results of the E/E/PES safety validation to the system engineers for further integration into the overall system.

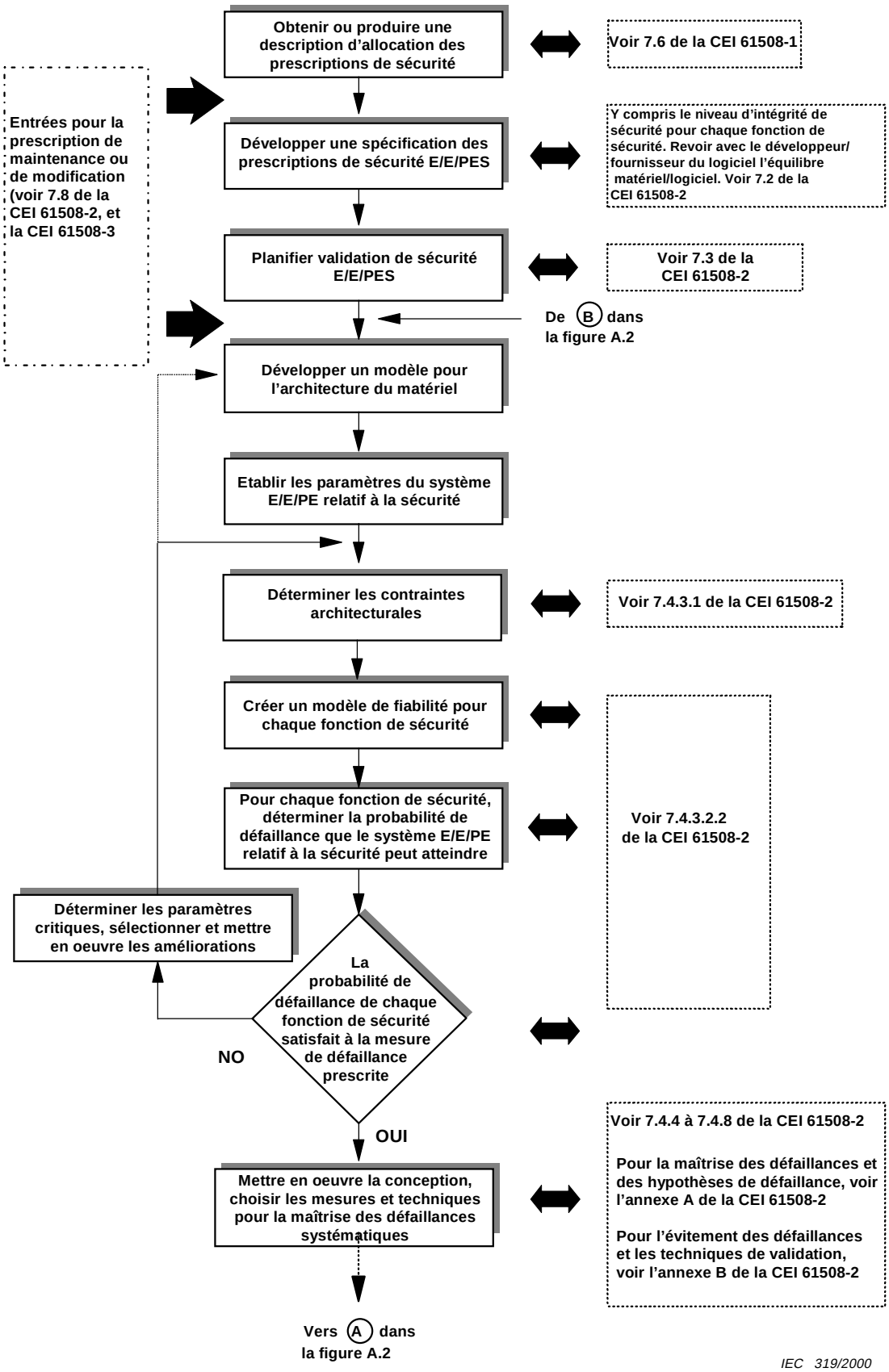
n) If maintenance/modification of the E/E/PES is required during operational life then re-activate IEC 61508-2 as appropriate (see 7.8 of IEC 61508-2).

A number of activities run across the E/E/PES 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/PES 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).

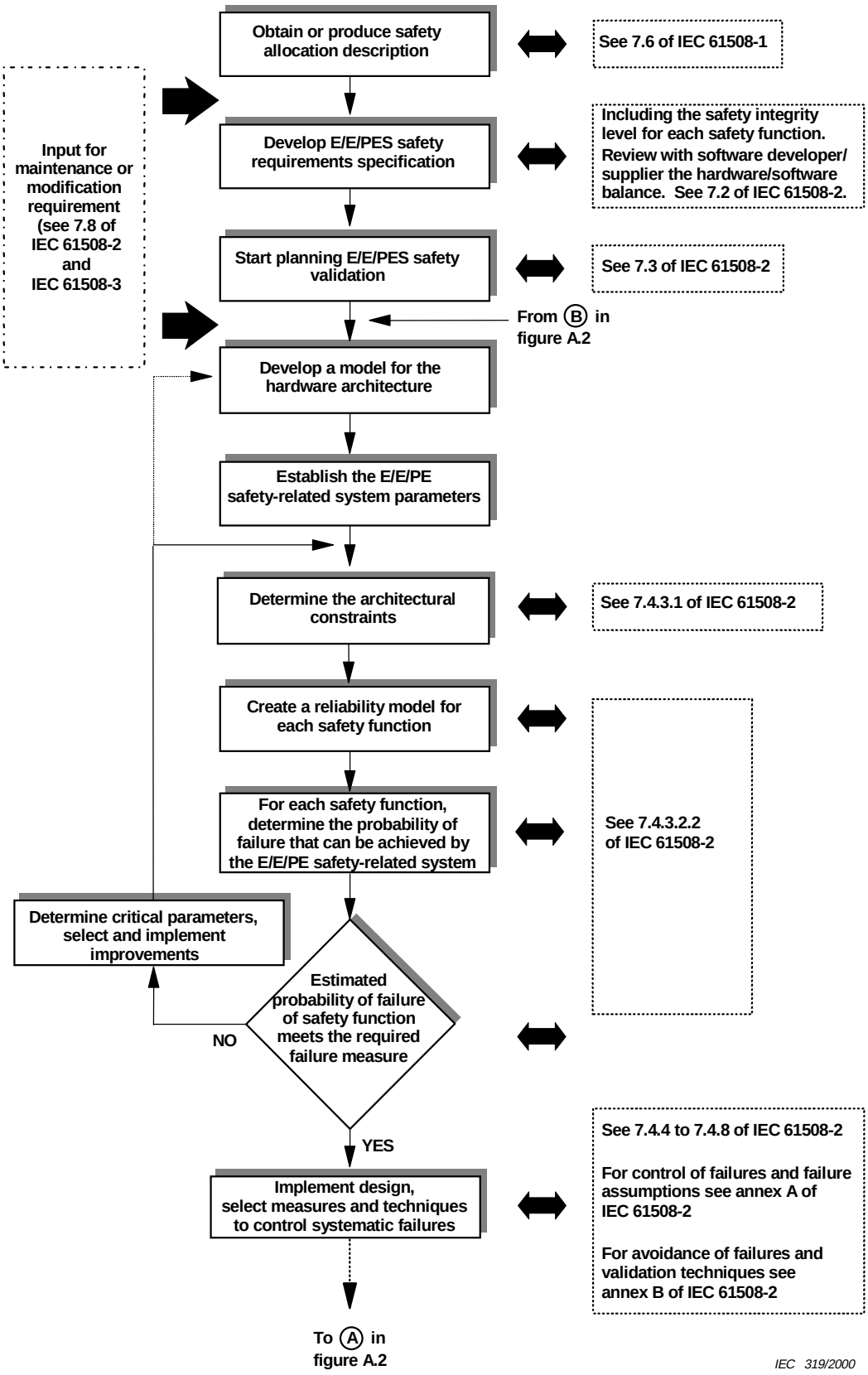
Annex B provides one possible technique for calculating the probabilities of hardware failure for E/E/PE safety-related systems.

NOTE 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).



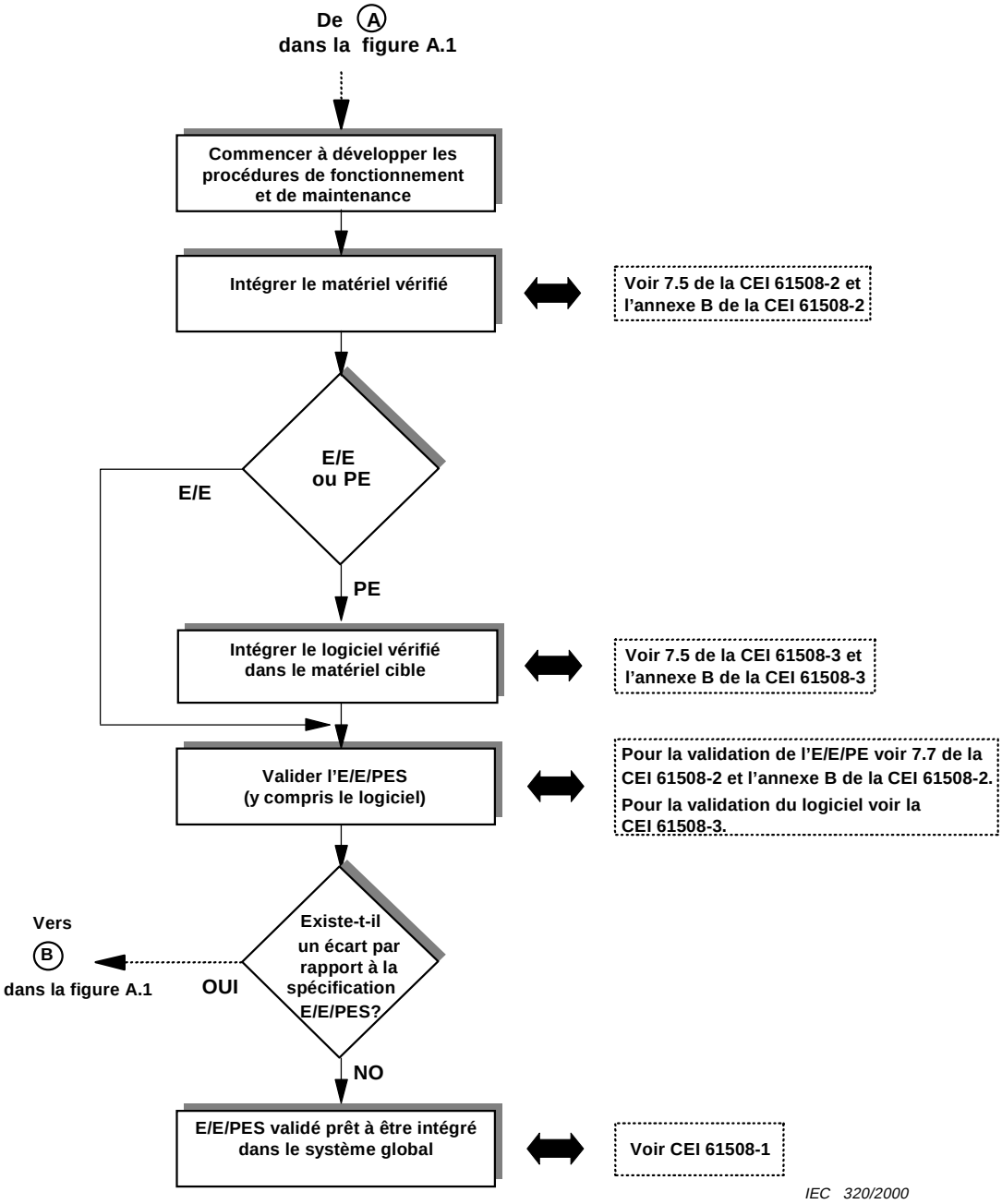
NOTE Pour les systèmes électroniques programmables, les activités du logiciel se produisent en parallèle (voir figure A.3).

Figure A.1 – Application de la CEI 61508-2



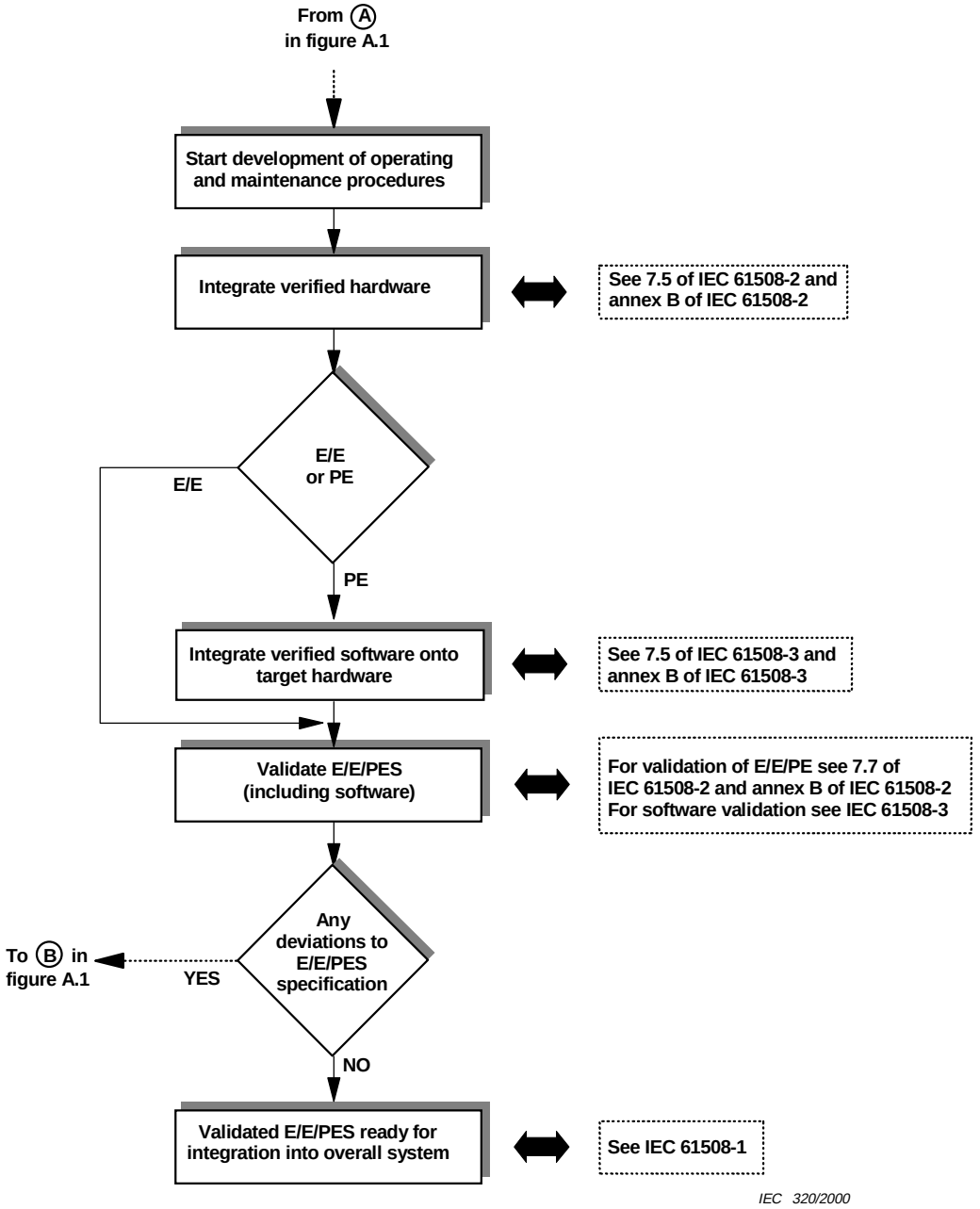
NOTE For PE systems, activities for software occur in parallel (see figure A.3).

Figure A.1 – Application of IEC 61508-2



NOTE Pour les systèmes électroniques programmables, les activités se produisent en parallèle (voir figure A.3).

Figure A.2 – Application de la CEI 61508-2 (suite)



NOTE For PE systems, activities for software occur in parallel (see figure A.3).

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

A.3 Etapes 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 prescriptions 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 Des phases précédentes du cycle de vie ont déjà

- spécifié les fonctions de sécurité présentes 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 de l'E/E/PES, 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/tester 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 suivront 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 E/E/PES 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 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 prédéveloppés (voir l'annexe D de la CEI 61508-7).

NOTE 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).

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 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/PES 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/PES 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 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).

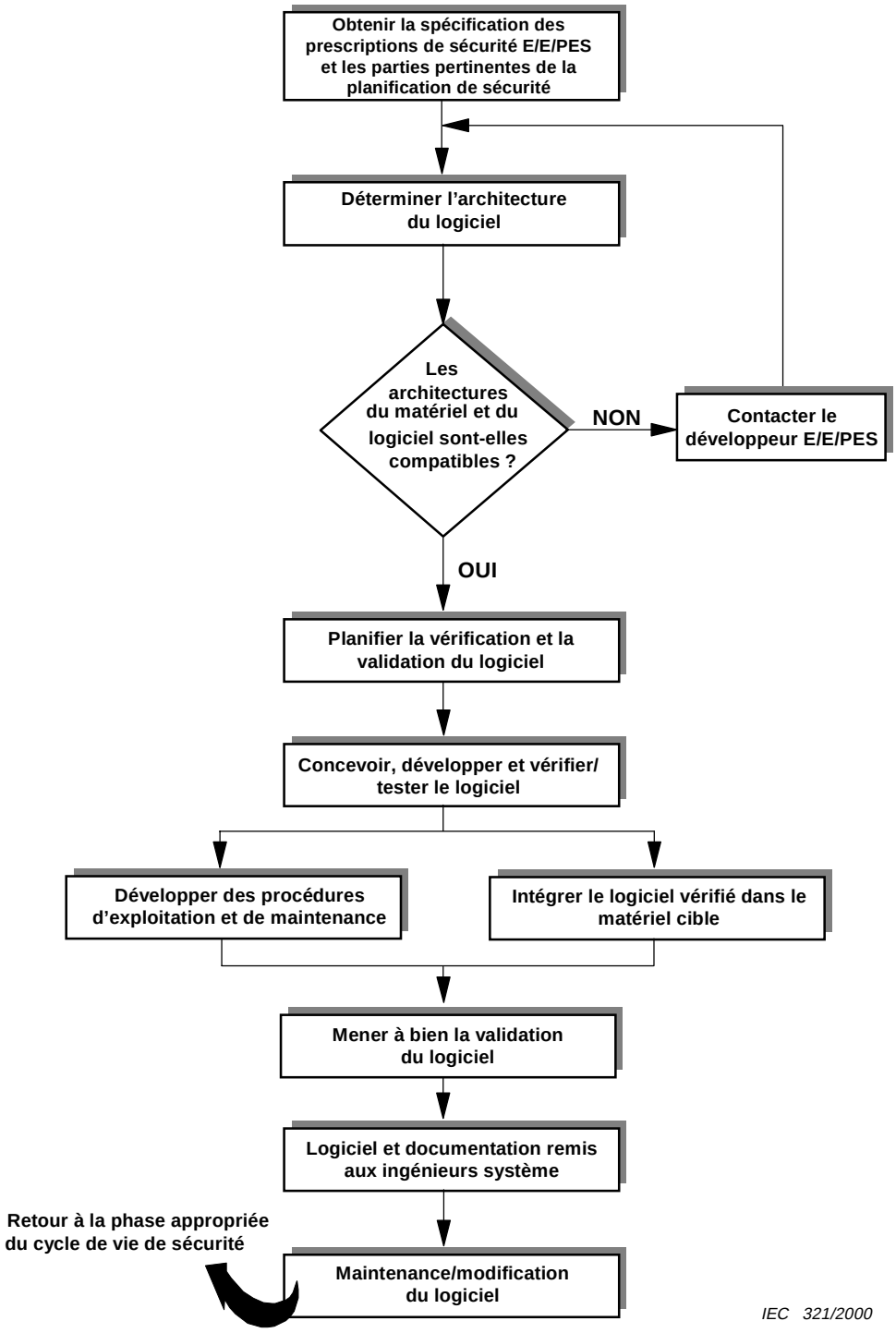


Figure A.3 – Application de la CEI 61508-3

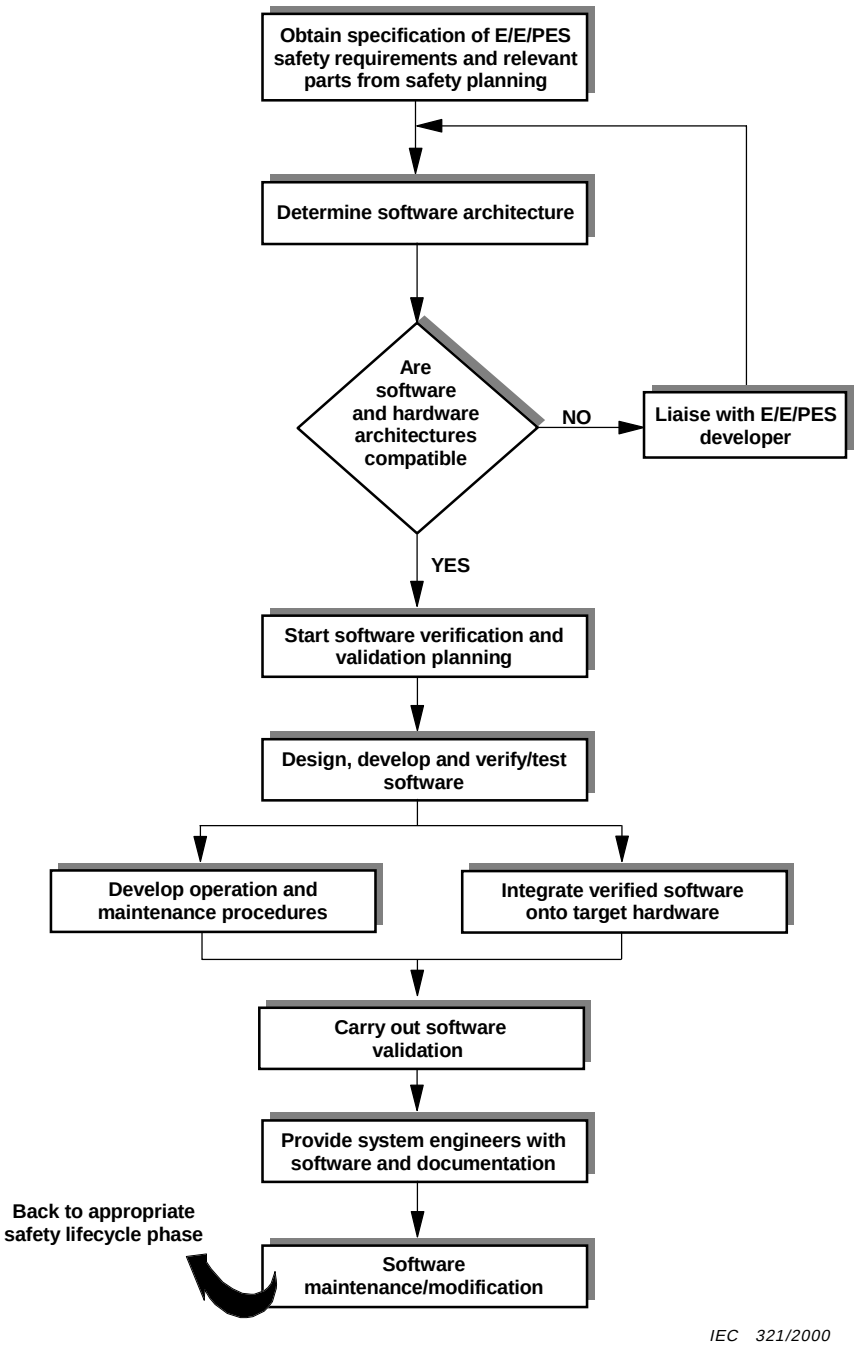


Figure A.3 – Application of IEC 61508-3

Annexe B
(informative)

Exemple de technique permettant d'évaluer les probabilités de défaillance du matériel

B.1 Généralités

La présente annexe propose une technique possible 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 qui pourrait être utilisée. Cette annexe fournit toutefois une approche relativement simple d'évaluation de la capacité des systèmes E/E/PE relatifs à la sécurité.

NOTE 1 D'autres techniques sont décrites par exemple dans l'ANSI/ISA S84.01-1996, Application of safety instrumented systems for the process industries.

Il existe un certain nombre de techniques pour analyser l'intégrité de sécurité du matériel pour les systèmes E/E/PE relatifs à la sécurité. Deux des techniques les plus utilisées sont les diagrammes de fiabilité (voir C.6.5 de la CEI 61508-7) et les modèles de Markov (voir C.6.4 de la CEI 61508-7). Ces deux méthodes, si elles sont correctement appliquées, donnent des résultats similaires; cependant, pour les sous-systèmes électroniques programmables complexes (par exemple lorsqu'une logique prioritaire à plusieurs canaux et le test automatique sont employés), il peut y avoir une certaine perte de précision si des diagrammes de fiabilité sont utilisés de préférence à des modèles de Markov.

Il est admis que cette perte de précision n'est pas significative dans le cas d'un système E/E/PE complet relatif à la sécurité et lorsque l'on tient compte de la précision des données de fiabilité utilisées pour l'analyse. Par exemple, les données d'exploitation prédominent dans l'analyse de l'intégrité de sécurité du matériel pour les systèmes E/E/PE relatifs à la sécurité. L'importance de la perte de précision ne peut être déterminée que dans des circonstances particulières. Pour les sous-systèmes électroniques programmables complexes, les diagrammes de fiabilité donnent des valeurs d'intégrité de sécurité du matériel plus pessimistes que celles des modèles de Markov (c'est-à-dire que les diagrammes de fiabilité donnent une probabilité de défaillance plus élevée). La présente annexe utilise des diagrammes de fiabilité.

Lorsqu'une défaillance du système de commande EUC émet une demande auprès du système E/E/PE relatif à la sécurité, la probabilité d'occurrence d'un événement dangereux dépend également de la probabilité de défaillance du système de commande EUC. Dans une telle situation, il est nécessaire de prendre en compte la possibilité de défaillance coïncidente des composants du système de commande 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 pourrait conduire à un risque résiduel plus élevé que prévu si les précautions appropriées n'étaient pas prises.

Les calculs se fondent sur les hypothèses suivantes:

– la probabilité de défaillance moyenne qui en résulte lors d'une sollicitation du sous-système est inférieure à 10^{-1}; ou la probabilité de défaillance par heure du sous-système est inférieure à 10^{-5};

– 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'aux (mais non compris ces composants) 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.1);

Annex B
(informative)

Example technique for evaluating probabilities of hardware failure

B.1 General

This annex provides one possible technique 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 technique that might be used. It does, however, provide a relatively simple approach for assessing the capability of E/E/PE safety-related systems.

NOTE 1 Other techniques are described for example in ANSI/ISA S84.01-1996, Application of safety instrumented systems for the process industries.

There are a number of techniques available for the analysis of hardware safety integrity for E/E/PE safety-related systems. Two of the more common techniques are reliability block diagrams (see C.6.5 of IEC 61508-7) and Markov models (see C.6.4 of IEC 61508-7). Both methods, if correctly applied, yield similar results, but in the case of complex programmable electronic subsystems (for example where multiple channel cross-voting and automatic testing are employed) there may be some loss of accuracy when reliability block diagrams are used compared to Markov models.

This loss of accuracy may not be significant in the context of the complete E/E/PE safety-related system and when the accuracy of the reliability data used in the analysis is taken into account. For example, field devices often predominate in the analysis of the hardware safety integrity for E/E/PE safety-related systems. Whether the loss of accuracy is significant can only be determined in the particular circumstances. In the case of complex programmable electronic subsystems, reliability block diagrams give results with more pessimistic hardware safety integrity values than Markov models (i.e. reliability block diagrams give a higher probability of failure). This annex uses reliability block diagrams.

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.

The calculations are based on the following assumptions:

– the resulting average probability of failure on demand for the subsystem is less than 10^{-1}, or the resultant probability of failure per hour for the subsystem is less than 10^{-5};

– 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.1);

– 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 éléments et câblages qui traitent le ou les signaux provenant du sous-système logique, y compris les éléments de commande finaux;

– les probabilités de défaillance du matériel sont calculées pour un seul canal d'un système (redondant) (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 diagnostics de couverture;

– le taux de défaillance global du 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 de test périodique et de réparation (c'est-à-dire que toutes les défaillances non détectées sont détectées par le test périodique); pour les effets d'un test périodique imparfait, voir B.2.5;

– l'intervalle entre tests périodiques est supérieur à celui de l'intervalle entre tests de diagnostic d'un ordre de grandeur au moins;

– pour chaque sous-système, il existe un seul intervalle entre tests périodiques et une seule durée moyenne de rétablissement;

NOTE 3 Le temps moyen de rétablissement est défini en 7.4.3.2.2, note 5 de la CEI 61508-2 comme incluant le temps nécessaire pour détecter une défaillance. Dans la présente annexe, la seule valeur du temps moyen de rétablissement, à la fois pour des défaillances détectées et pour les défaillances non détectées, comprend l'intervalle entre tests de diagnostic mais pas l'intervalle entre tests périodiques. Pour les défaillances non détectées, il convient que le temps moyen de rétablissement utilisé dans les calculs ne comprenne pas l'intervalle entre tests de diagnostic, mais puisque le temps moyen de rétablissement est toujours ajouté à l'intervalle entre tests périodiques, qui est supérieur à celui de l'intervalle entre tests de diagnostic d'un ordre de grandeur au moins, l'erreur n'est pas significative.

– plusieurs équipes de réparation sont disponibles pour intervenir sur toutes les défaillances connues;

– l'intervalle escompté entre les demandes est supérieur au temps moyen de rétablissement d'un ordre de grandeur au moins;

– pour tous sous-systèmes utilisés en mode de fonctionnement demande faible, ainsi que pour les groupes à logique majoritaire 1oo2, 1oo2D et 2oo3 utilisés en mode de fonctionnement demande élevée ou continue, la fraction de défaillances spécifiée par la couverture du diagnostic est à la fois détectée et réparée pendant la durée moyenne de rétablissement utilisée pour déterminer les prescriptions d'intégrité de sécurité du matériel;

EXEMPLE Si l'on considère une durée moyenne de rétablissement de 8 h, cette période comprend l'intervalle entre tests de diagnostic qui est en général inférieur à 1 h, le temps restant constituant le temps de réparation effectif.

NOTE 4 Pour les groupes à logique majoritaire 1oo2, 1oo2D 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 mise en état de sécurité, la probabilité moyenne de défaillance sur demande est améliorée. Le degré d'amélioration dépendra de la couverture du diagnostic.

– pour les groupes à logique majoritaire 1oo1 et 2oo2 fonctionnant en mode demande élevée ou continu, le système E/E/PE relatif à la sécurité se met toujours en arrêt de sécurité après détection d'une anomalie dangereuse; pour parvenir à ce résultat, l'intervalle escompté entre les demandes est au moins d'un ordre de grandeur supérieur à celui de l'intervalle entre tests de diagnostic, ou la somme de l'intervalle entre tests de diagnostic et le temps nécessaire à l'arrêt de sécurité est inférieure au temps de mise en sécurité du processus;

NOTE 5 Le temps de mise en sécurité du processus est défini en 7.4.3.2.5 de la CEI 61508-2 comme l'intervalle de temps entre une défaillance de l'EUC ou du système de commande de l'EUC (susceptible de déclencher un événement dangereux) et l'événement dangereux si la fonction de sécurité n'est pas remplie.

– 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.2.5;

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

– for each subsystem there is a single proof test interval and mean time to restoration;

NOTE 3 The mean time to restoration is defined in 7.4.3.2.2, note 5 of IEC 61508-2 as including the time taken to detect a failure. In this annex, the single assumed value of mean time to restoration for both detected and undetected failures includes the diagnostic test interval but not the proof test interval. For undetected failures, the mean time to restoration used in the calculations should not include the diagnostic test interval, but since the mean time to restoration is always added to the proof test interval, which is at least an order of magnitude greater than the diagnostic test interval, the error is not significant.

– multiple repair teams are available to work on all known failures;

– the expected interval between demands is at least an order of magnitude greater than the mean time to restoration;

– for all subsystems operating in low demand mode of operation, and for 1oo2, 1oo2D 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 mean time to restoration used to determine hardware safety integrity requirements;

EXAMPLE If a mean time to restoration of 8 h is assumed, this includes the diagnostic test interval which is typically less than 1 h, the remainder being the actual repair time.

NOTE 4 For 1oo2, 1oo2D 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 5 The process safety time is defined in 7.4.3.2.5 of IEC 61508-2 as the period of time between a failure occurring in the EUC or the EUC control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed.

– 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 de défaillance sur demande 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 capteur, logique ou élément final du sous-système;

– les abréviations des termes utilisés et les valeurs prises en compte sont indiquées dans le tableau B.1.

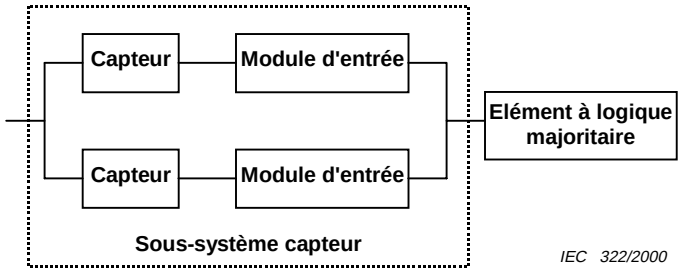


Figure B.1 – Exemple de configuration pour deux canaux de capteurs

– 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.

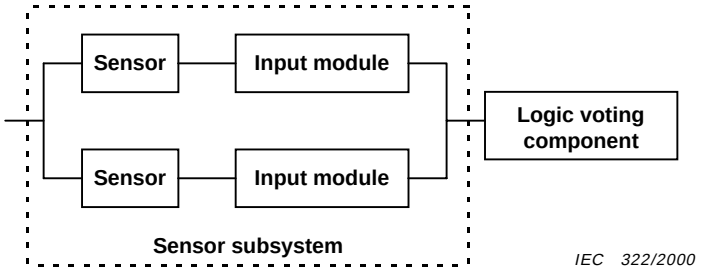


Figure B.1 – Example configuration for two sensor channels

Tableau B.1 – Termes et ordre de grandeur des paramètres correspondants utilisés dans cette annexe (s'applique à 1oo1, 1oo2, 2oo2, 1oo2D 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 du test 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] 10 ans (87 600 h)[2]
MTTR	Durée moyenne de rétablissement (en heures)	8 h
DC	Couverture du diagnostic (exprimée comme une fraction dans les équations et comme 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 tests 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	Taux de défaillance (par heure) du canal d'un sous-système	$0{,}1 \times 10^{-6}$ $0{,}5 \times 10^{-6}$ 1×10^{-6} 5×10^{-6} 10×10^{-6} 50×10^{-6}
PFD_G	Probabilité moyenne de défaillance sur la demande 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 défaillance sur la demande pour le sous-système capteur	
PFD_L	Probabilité moyenne de défaillance sur la demande pour le sous-système logique	
PFD_{FE}	Probabilité moyenne de défaillance sur la demande pour le sous-système élément final	
PFD_{SYS}	Probabilité moyenne de défaillance sur la demande d'une fonction de sécurité pour le système E/E/PE relatif à la sécurité	
PFH_G	Probabilité de défaillance 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	Probabilité de défaillance par heure pour le sous-système capteur	
PFH_L	Probabilité de défaillance par heure pour le sous-système logique	
PFH_{FE}	Probabilité de défaillance par heure pour le sous-système élément final	
PFH_{SYS}	Probabilité de défaillance par heure d'une fonction de sécurité pour le système E/E/PE relatif à la sécurité	
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 demandes (en heures)	

[1] Uniquement pour mode demande élevée ou mode de fonctionnement continu.

[2] Uniquement pour mode faible demande.

Table B.1 – Terms and their ranges used in this annex
(applies to 1oo1, 1oo2, 2oo2, 1oo2D 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 (h)	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] 10 years (87 600 h)[2]
MTTR	Mean time to restoration (hour)	8 h
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	Failure rate (per hour) of a channel in a subsystem	$0{,}1 \times 10^{-6}$ $0{,}5 \times 10^{-6}$ 1×10^{-6} 5×10^{-6} 10×10^{-6} 50×10^{-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	
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	Probability of failure per hour 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	Probability of failure per hour for the sensor subsystem	
PFH_L	Probability of failure per hour for the logic subsystem	
PFH_{FE}	Probability of failure per hour for the final element subsystem	
PFH_{SYS}	Probability of failure per hour of a safety function for the E/E/PE safety-related system	
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)	

[1] High demand or continuous mode only.

[2] Low demand mode only.

B.2 Probabilité moyenne de défaillance sur demande (pour mode de fonctionnement faible demande)

B.2.1 Procédure de calcul

La probabilité moyenne de défaillance sur demande 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 défaillance sur demande 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.2):

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

où

– PFD_{SYS} est la probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système E/E/PE relatif à la sécurité;

– PFD_S est la probabilité moyenne de défaillance sur demande du sous-système capteur;

– PFD_L est la probabilité moyenne de défaillance sur demande du sous-système logique;

– PFD_{FE} est la probabilité moyenne de défaillance sur demande du sous-système élément final.

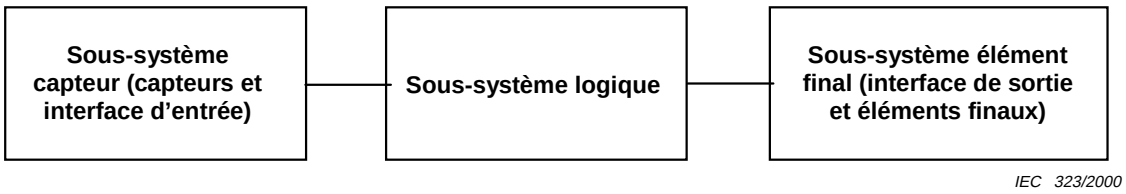


Figure B.2 – Structure du sous-système

Afin de déterminer la probabilité moyenne de défaillance sur demande 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) du système, les composants du sous-système logique ou les composants de sortie du sous-système élément final. Par exemple, les composants d'entrée 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 de sortie 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 ou 2oo3.

b) Pour le tableau correspondant, se reporter aux tableaux B.2 à B.5 donnés pour des intervalles entre tests 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 du diagnostic (par exemple 60 %);

   – le taux de défaillance (par heure), λ, pour l'élément (par exemple 5.0E-06);

B.2 Average probability of failure on demand (for low demand mode of operation)

B.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 provide the safety function. Since in this annex the probabilities are small, this can be expressed by the following (see figure B.2):

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

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.

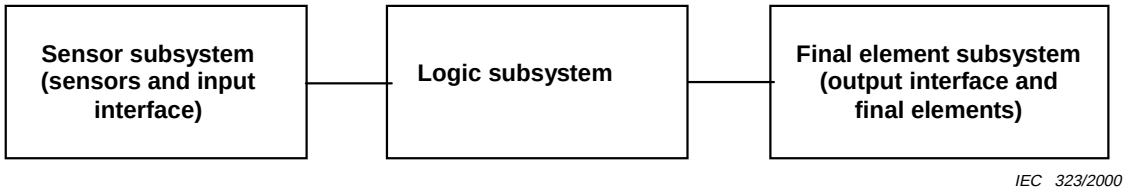


Figure B.2 – Subsystem structure

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 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 failure rate (per hour), λ, of each channel (for example, 5.0E-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 le même diagnostic de couverture 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 de tests de diagnostic (utilisé également pour les défaillances dangereuses non détectées en présence de tests de diagnostic), β, est égal à deux fois le facteur β pour les défaillances détectées par les tests de diagnostic, β_D.

d) Obtenir, à partir du tableau approprié parmi les tableaux B.2 à B.5, la probabilité moyenne de défaillance sur demande 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 défaillance sur demande du capteur ou du sous-système élément final, PFD_S ou PFD_{FE} est donnée dans les équations suivantes, où PFD_{Gi} et PFD_{Gj} est la probabilité moyenne de défaillance sur demande de chaque groupe de capteurs à logique majoritaire sélectionné et d'éléments finaux, respectivement:

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

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

B.2.2 Architectures pour le mode de fonctionnement faible demande

NOTE 1 Il convient de considérer ce paragraphe en tenant compte du fait que les équations valables pour plusieurs architectures ne sont citées que lors de leur première utilisation.

NOTE 2 Les équations sont basées sur les hypothèses énumérées en B.1.

B.2.2.1 1oo1

Cette architecture comprend un seul élément, et toute défaillance dangereuse empêche le traitement correct de tout signal d'alarme valide.

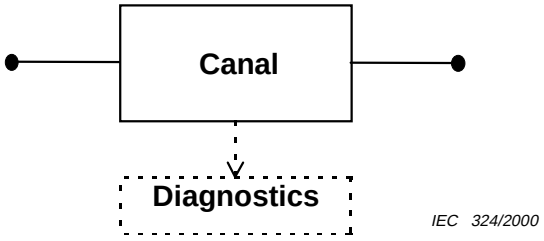


Figure B.3 – Diagramme du bloc physique 1oo1

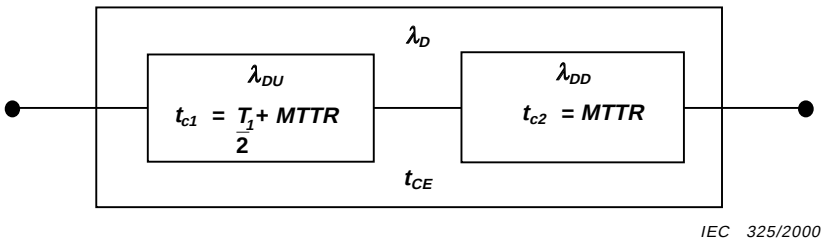


Figure B.4 – Diagramme de fiabilité 1oo1

– 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 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:

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

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

B.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.1.

B.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.

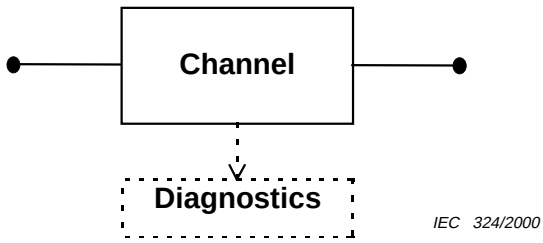


Figure B.3 – 1oo1 physical block diagram

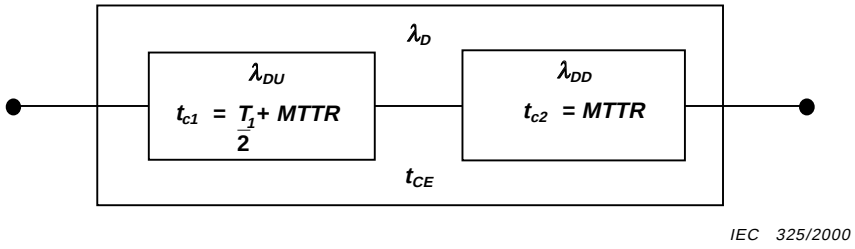


Figure B.4 – 1oo1 reliability block diagram

Les figures B.3 et B.4 comprennent les diagrammes des blocs pertinents. Le taux de défaillances dangereuses est donné par

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

La figure B.4 montre que l'on peut considérer que le canal se compose de deux composants, l'un ayant un taux de défaillances dangereuses λ_{DU} résultant des défaillances non détectées et l'autre un taux de défaillances dangereuses λ_{DD} résultant des défaillances détectées. Il est possible de calculer un temps d'indisponibilité 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:

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

Pour chaque architecture, le taux de défaillances dangereuses détectées et le taux de défaillances dangereuses non détectées sont données par la formule

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC); \quad \lambda_{DD} = \frac{\lambda}{2} DC$$

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 défaillance sur demande est

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

B.2.2.2 1oo2

Cette architecture comprend deux canaux connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Ainsi, il faudrait qu'il y ait une défaillance dangereuse dans les deux canaux pour qu'un signal d'alarme valide ne soit pas traité correctement. On suppose que tout test de diagnostic ne révélerait que les anomalies découvertes et ne modifierait pas les états de sortie ou la logique majoritaire des sorties.

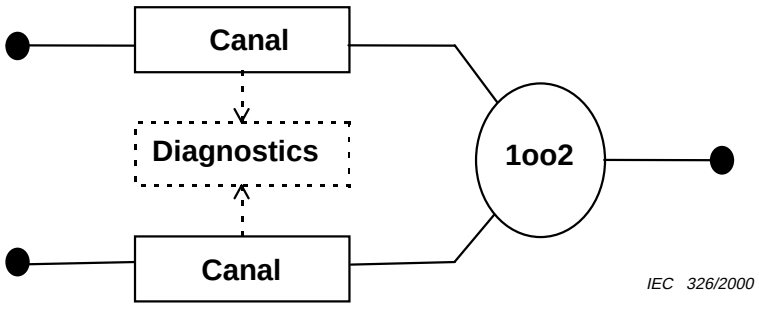


Figure B.5 – Diagramme du bloc physique 1oo2

Figures B.3 and B.4 contain the relevant block diagrams. The dangerous failure rate for the channel is given by

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

Figure B.4 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:

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

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

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC) \;;\; \lambda_{DD} = \frac{\lambda}{2} DC$$

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

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

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

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

B.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.

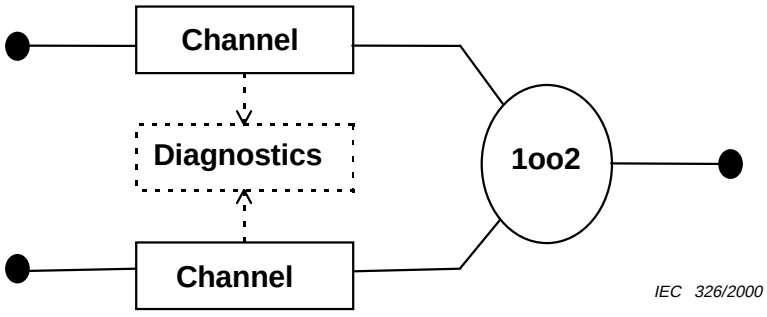


Figure B.5 – 1oo2 physical block diagram

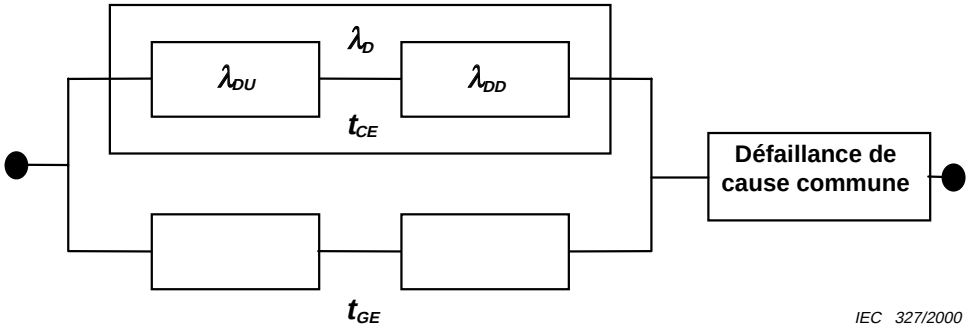


Figure B.6 – Diagramme de fiabilité 1oo2

Les figures B.5 et B.6 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est donnée en B.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

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

La probabilité moyenne de défaillance sur demande de l'architecture est

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

B.2.2.3 2oo2

Cette architecture comporte deux canaux connectés en parallèle de sorte qu'il est nécessaire que les deux canaux demandent la fonction de sécurité avant que celle-ci ne survienne. On suppose que tout test de diagnostic n'indiquerait que les anomalies découvertes et ne modifierait pas les états de sortie ou la logique majoritaire de sortie.

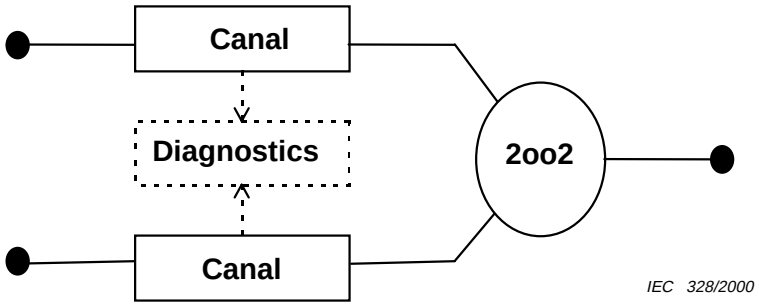


Figure B.7 – Diagramme du bloc physique 2oo2

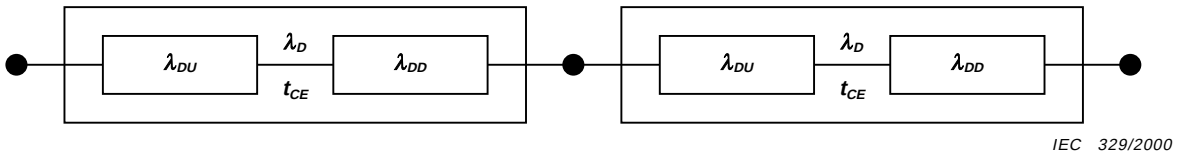


Figure B.8 – Diagramme de fiabilité 2oo2

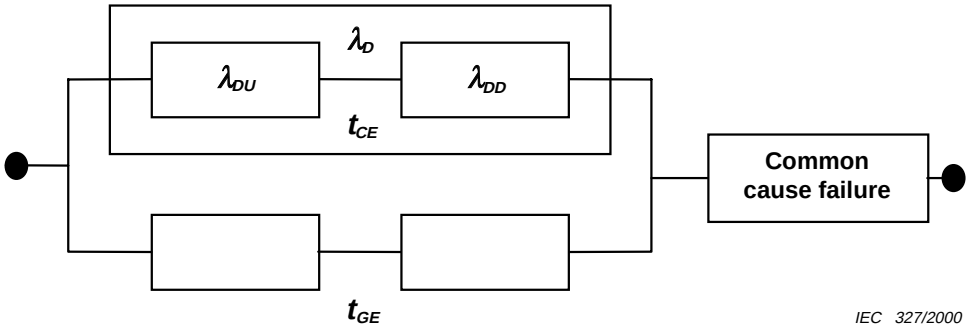


Figure B.6 – 1oo2 reliability block diagram

Figures B.5 and B.6 contain the relevant block diagrams. The value of t_{CE} is as given in B.2.2.1, but now it is necessary to also calculate the system equivalent down time t_{GE}, which is given by

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

The average probability of failure on demand for the architecture is

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

B.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.

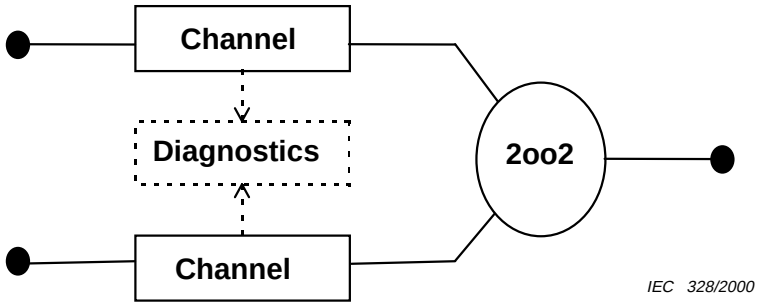


Figure B.7 – 2oo2 physical block diagram

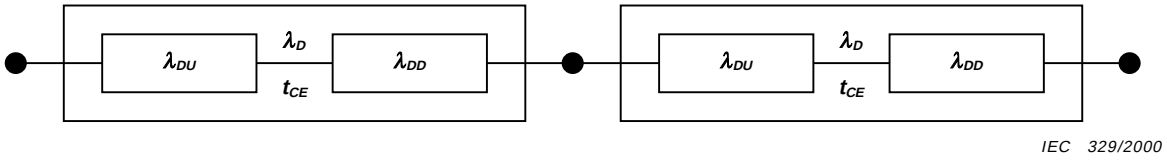


Figure B.8 – 2oo2 reliability block diagram

Les figures B.7 et B.8 montrent les diagrammes correspondants. La valeur de t_{CE} est donnée en B.2.2.1; la probabilité moyenne de défaillance sur demande pour l'architecture est

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

B.2.2.4 1oo2D

Cette architecture comprend deux canaux connectés en parallèle. Dans des conditions normales d'utilisation, les deux canaux doivent demander la fonction de sécurité avant que celle-ci ne survienne. De plus, si les tests de diagnostic détectent une anomalie dans l'un des canaux, 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 tests 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 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.

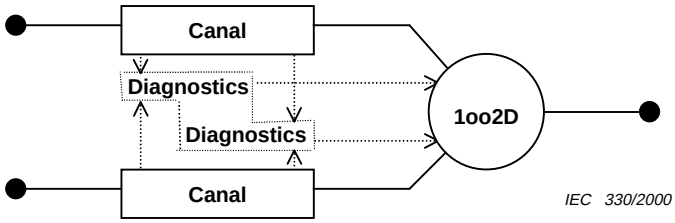


Figure B.9 – Diagramme du bloc physique 1oo2D

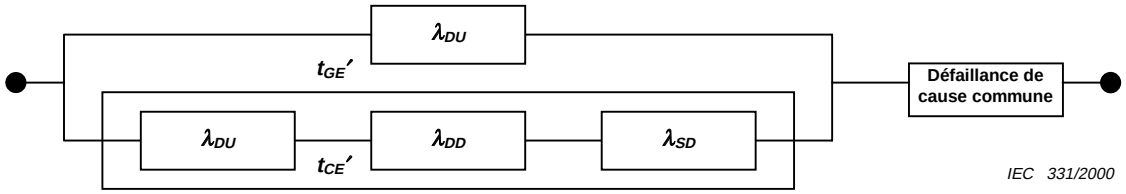


Figure B.10 – Diagramme de fiabilité 1oo2D

Le taux de défaillances en sécurité détectées pour chaque canal est donné par

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

Les figures B.9 et B.10 illustrent les diagrammes de blocs pertinents. Les valeurs des temps moyens d'indisponibilité diffèrent de celles données pour les autres architectures dans le paragraphe B.2.2 et sont pour cela désignées t_{CE}' et t_{GE}'. Leurs valeurs sont données par la formule

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

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

Figures B.7 and B.8 contain the relevant block diagrams. The value of t_{CE} is as given in B.2.2.1, and the average probability of failure on demand for the architecture is

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

B.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.

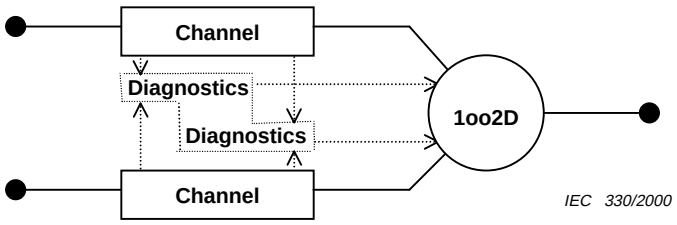


Figure B.9 – 1oo2D physical block diagram

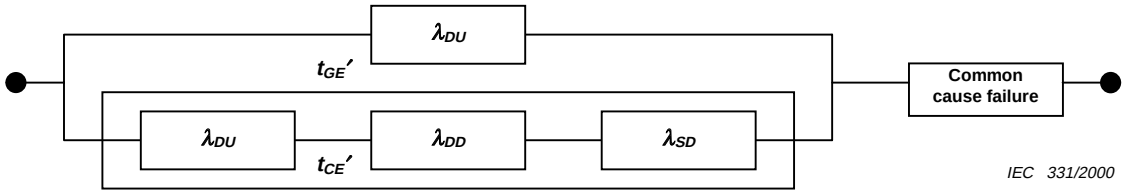


Figure B.10 – 1oo2D reliability block diagram

The detected safe failure rate for every channel is given by

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

Figures B.9 and B.10 contain the relevant block diagrams. The values of the equivalent mean down times differ from those given for the other architectures in B.2.2 and hence are labelled t_{CE}' and t_{GE}'. Their values are given by

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

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

La probabilité moyenne de défaillance sur demande pour l'architecture est donnée par la formule

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

B.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 test de diagnostic n'indiquerait que les anomalies décelées et ne modifierait ni les états de sortie, ni la logique majoritaire.

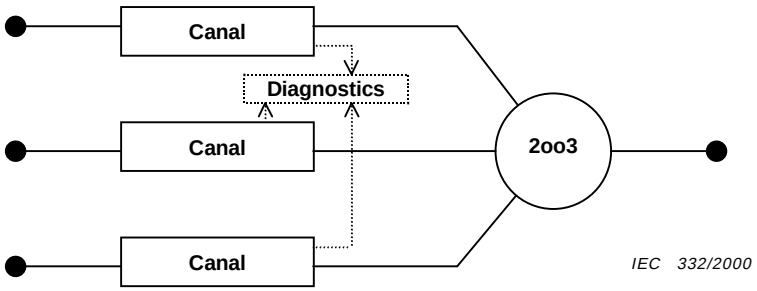


Figure B.11 – Diagramme du bloc physique 2oo3

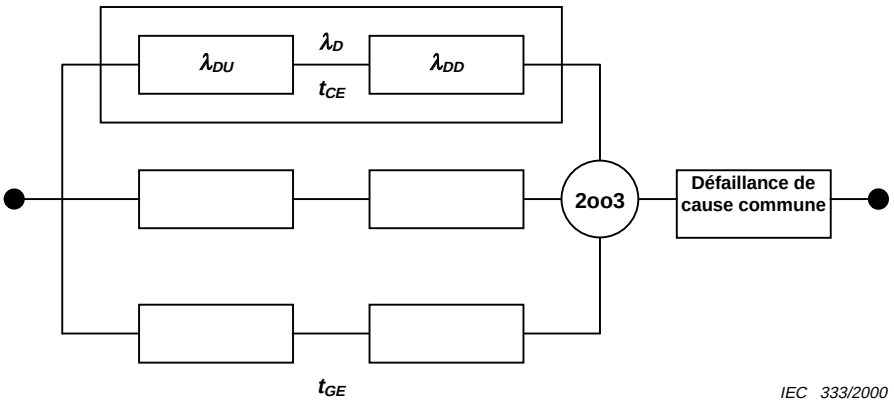


Figure B.12 – Diagramme de fiabilité 2oo3

Les figures B.11 et B.12 montrent les diagrammes correspondants. La valeur de t_{CE} est celle donnée au paragraphe B.2.2.1 et la valeur de t_{GE} est celle donnée au paragraphe B.2.2.2. La probabilité moyenne de défaillance pour l'architecture est

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

The average probability of failure on demand for the architecture is

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

B.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.

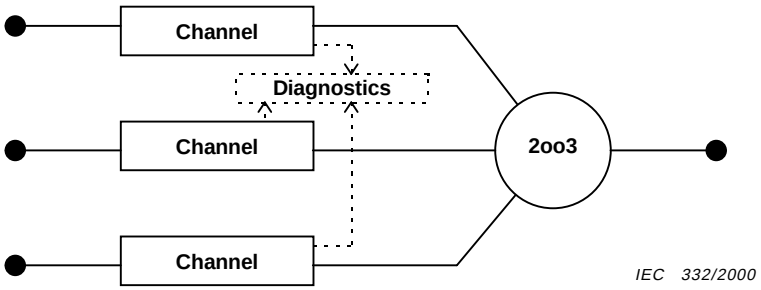


Figure B.11 – 2oo3 physical block diagram

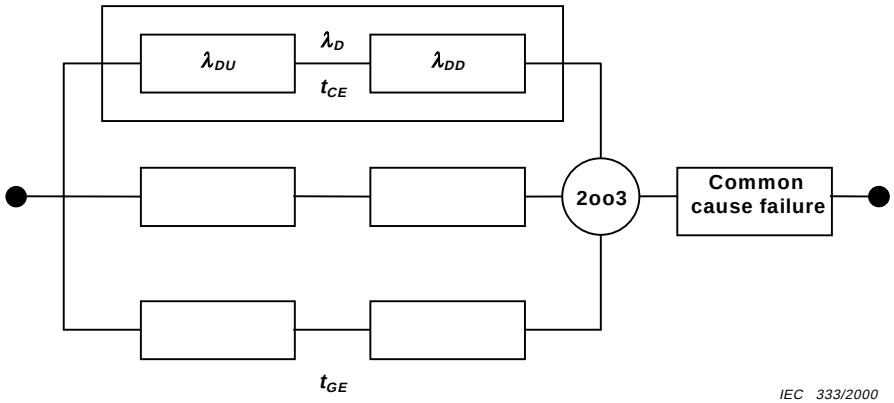


Figure B.12 – 2oo3 reliability block diagram

Figures B.11 and B.12 contain the relevant block diagrams. The value of t_{CE} is as given in B.2.2.1 and the value of t_{GE} is as given in B.2.2.2. The average probability of failure on demand for the architecture is

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

B.2.3 Tableaux détaillés pour le mode de fonctionnement faible demande

Tableau B.2 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de 6 mois et une durée moyenne de rétablissement de 8 h

Architecture	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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	**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	4.4E-06	2.2E-05	4.4E-05	8.9E-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
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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

Tableau B.2 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	4.6E-05	2.2E-04	4.4E-04	9.5E-05	4.5E-04	8.9E-04	6.0E-04	2.3E-03	4.5E-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
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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

B.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 = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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	**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	4.4E-06	2.2E-05	4.4E-05	8.9E-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
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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

Table B.2 *(continued)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	4.6E-05	2.2E-04	4.4E-04	9.5E-05	4.5E-04	8.9E-04	6.0E-04	2.3E-03	4.5E-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
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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

Tableau B.3 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de un an et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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	**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	8.9E-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
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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

Tableau B.3 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	9.4E-05	4.5E-04	8.8E-04	2.0E-04	9.0E-04	1.8E-03	1.5E-03	5.0E-03	9.3E-03
	90 %	2.2E-05	1.1E-04	2.2E-04	4.5E-05	2.2E-04	4.4E-04	2.3E-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
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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

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 = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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	**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	8.9E-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
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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

Table B.3 *(continued)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	9.4E-05	4.5E-04	8.8E-04	2.0E-04	9.0E-04	1.8E-03	1.5E-03	5.0E-03	9.3E-03
	90 %	2.2E-05	1.1E-04	2.2E-04	4.5E-05	2.2E-04	4.4E-04	2.3E-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
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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

Tableau B.4 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de deux ans et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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 %**	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 (voir la 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	**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	1.8E-05	8.8E-05	1.8E-04	3.6E-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
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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

Tableau B.4 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	2.0E-04	9.0E-04	1.8E-03	4.5E-04	1.8E-03	3.6E-03	4.3E-03	1.1E-02	1.9E-02
	90%	4.4E-05	2.2E-04	4.4E-04	8.9E-05	4.4E-04	8.8E-04	4.7E-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
2oo3	**0 %**	2.3E-03	3.7E-03	5.6E-03	8.3E-03	1.1E-02	1.4E-02	>1E-01	>1E-01	>1E-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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

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 = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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	**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	1.8E-05	8.8E-05	1.8E-04	3.6E-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
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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

Table B.4 *(continued)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	2.0E-04	9.0E-04	1.8E-03	4.5E-04	1.8E-03	3.6E-03	4.3E-03	1.1E-02	1.9E-02
	90 %	4.4E-05	2.2E-04	4.4E-04	8.9E-05	4.4E-04	8.8E-04	4.7E-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
2oo3	**0 %**	2.3E-03	3.7E-03	5.6E-03	8.3E-03	1.1E-02	1.4E-02	>1E-01	>1E-01	>1E-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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

Tableau B.5 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de dix ans et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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	**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 %	1.8E-05	8.8E-05	1.8E-04	9.4E-05	4.4E-04	8.8E-04	2.0E-04	9.0E-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
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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

Tableau B.5 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	1.5E-03	4.9E-03	9.2E-03	4.2E-03	1.1E-02	1.9E-02	7.1E-02	9.9E-02	>1E-01
	90 %	2.3E-04	1.1E-03	2.2E-03	4.7E-04	2.2E-03	4.4E-03	3.0E-03	1.2E-02	2.3E-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
2oo3	**0 %**	4.8E-02	5.0E-02	5.3E-02	>1E-01	>1E-01	>1E-01	>1E-01	>1E-01	>1E-01
	60 %	8.3E-03	1.1E-02	1.4E-02	3.2E-02	3.5E-02	4.0E-02	>1E-01	>1E-01	>1E-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

NOTE 1 Ce tableau donne des exemples de valeurs de PFD_G calculées en appliquant les équations données en B.2.2 et en fonction des hypothèses énoncées en B.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.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.

Table B.5 – Average probability of failure on demand for a proof-test interval of 10 years and a mean time to restoration of 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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	**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 %	1.8E-05	8.8E-05	1.8E-04	9.4E-05	4.4E-04	8.8E-04	2.0E-04	9.0E-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
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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

Table B.5 *(continued)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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	**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 %	1.5E-03	4.9E-03	9.2E-03	4.2E-03	1.1E-02	1.9E-02	7.1E-02	9.9E-02	>1E-01
	90 %	2.3E-04	1.1E-03	2.2E-03	4.7E-04	2.2E-03	4.4E-03	3.0E-03	1.2E-02	2.3E-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
2oo3	**0 %**	4.8E-02	5.0E-02	5.3E-02	>1E-01	>1E-01	>1E-01	>1E-01	>1E-01	>1E-01
	60 %	8.3E-03	1.1E-02	1.4E-02	3.2E-02	3.5E-02	4.0E-02	>1E-01	>1E-01	>1E-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

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.2.2 and depending on the assumptions listed in B.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.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.

B.2.4 Exemple pour un mode de fonctionnement faible demande

Soit une fonction de sécurité nécessitant un système de niveau SIL2. 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. Il convient que la soupape d'arrêt et la soupape de mise à l'air libre fonctionnent de telle sorte que la fonction de sécurité s'accomplisse. L'architecture est illustrée à la figure B.13. Pour l'évaluation initiale, on suppose une période de test périodique d'un an.

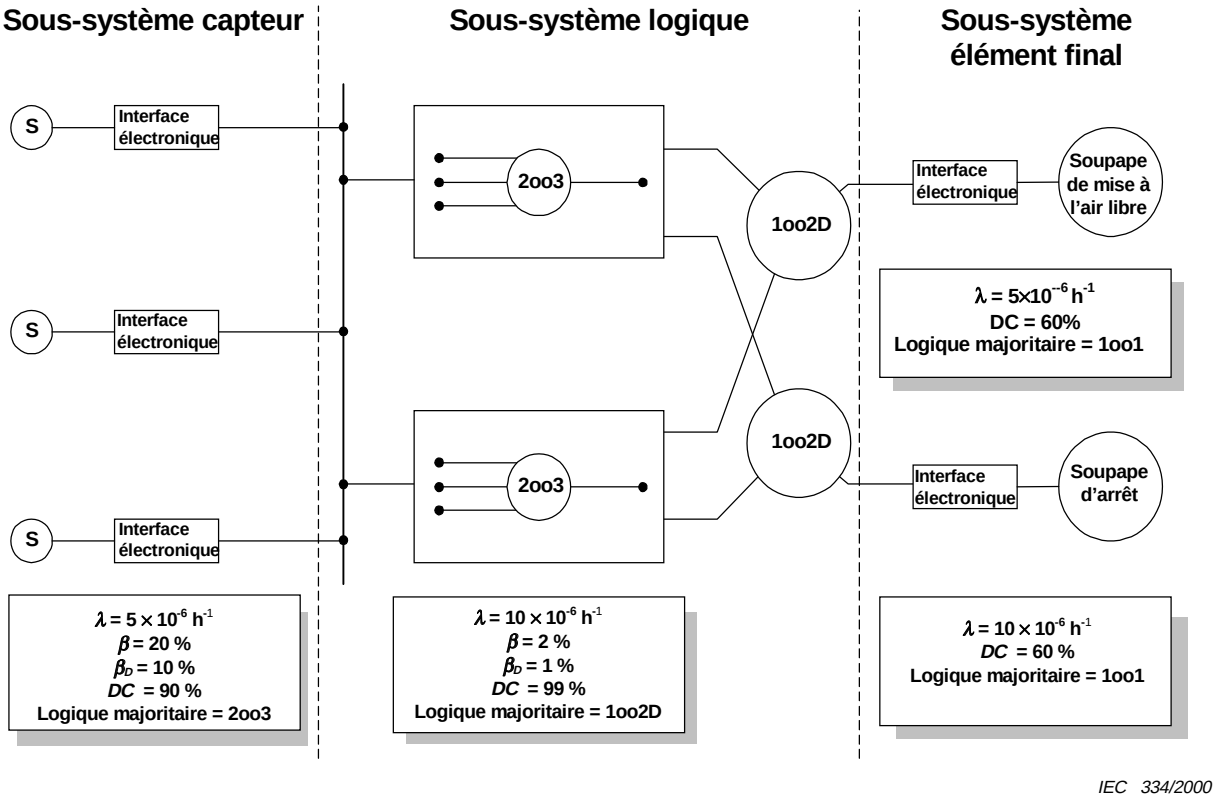


Figure B.13 – Architecture d'un exemple de fonctionnement en mode demande faible

Tableau B.6 – Probabilité moyenne de défaillance sur demande pour le sous-système capteur dans l'exemple de fonctionnement en mode demande faible (intervalle entre tests périodiques d'un an et MTTR de 8 h)

Architecture	*DC*	λ = 5.0E-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.				

B.2.4 Example for low demand mode of operation

Consider a safety function requiring a SIL2 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 PES 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.13. For the initial assessment, a proof-test period of one year is assumed.

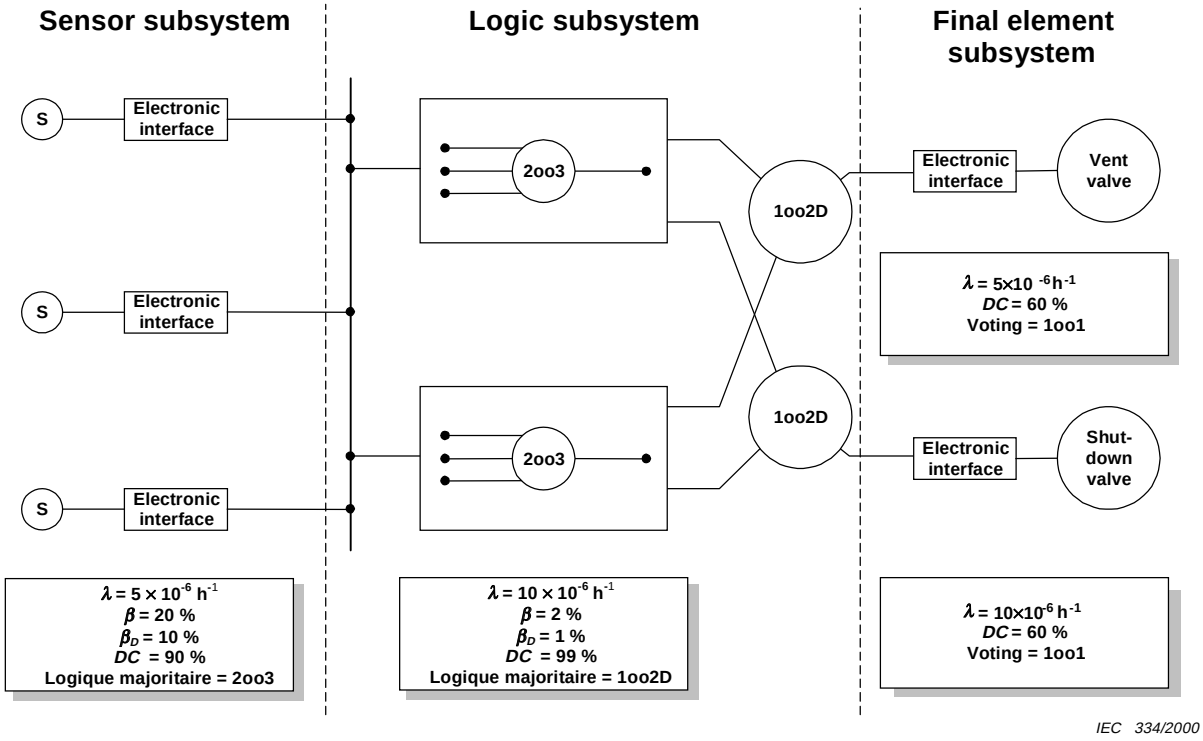


Figure B.13 – Architecture of an example for low demand mode of operation

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 = 5.0E-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.				

Tableau B.7 – Probabilité moyenne de défaillance sur demande pour le sous-système logique de l'exemple de fonctionnement en mode demande faible (intervalle entre tests périodiques d'un an et MTTR de 8 h)

Architecture	*DC*	λ = 1.0E-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 défaillance sur demande pour le sous-système élément final de l'exemple de fonctionnement en mode demande faible (intervalle entre tests périodiques d'un an et durée MTTR de 8 h)

Architecture	*DC*	λ = 5.0E-06	λ = 1.0E-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,

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

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

$$\equiv \textbf{niveau 1 d'intégrité de sécurité}$$

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 = 1.0E-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 = 5.0E-06	λ = 1.0E-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**

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 tests périodiques à six mois

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

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

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

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

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

$\equiv$ **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 %)

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

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

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

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

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

$\equiv$ **niveau 2 d'intégrité de sécurité**

B.2.5 Effets d'un test périodique imparfait

Les anomalies dans le système de sécurité qui ne sont détectées ni par des tests de diagnostic ni par des tests périodiques ne sont détectées que par une demande incidente nécessitant la fonction de sécurité affectée par l'anomalie. Ainsi, pour ces anomalies entièrement non détectées, le temps d'indisponibilité effectif dépend du taux de demande attendu sur le système de sécurité.

Un exemple est donné ci-dessous pour une architecture 1oo2. T_2 est le délai entre les demandes sur le système:

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

$$t_{GE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \frac{\lambda_{DU}}{2}\left(\frac{T_1}{2} + MTTR\right) + \beta \frac{\lambda_{DU}}{2}\left(\frac{T_2}{2} + MTTR\right)$$

Le tableau B.9 ci-dessous donne les résultats numériques d'un système 1oo2 avec un test périodique de 100 % sur un an comparé à un test périodique de 50 % où la période de demande T_2 est supposée être de 10 ans. Cet exemple a été calculé en prenant pour hypothèse un taux de défaillance de 1×10^{-5} par heure, une valeur β de 10 % et une valeur β_D de 5 %.

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

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

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

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

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

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

$\equiv$ **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 %)

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

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

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

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

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

$\equiv$ **safety integrity level 2**

B.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 are found only by an incidence of demand that requires the safety function affected by the fault. Thus, for these totally undetected faults, the expected demand rate on the safety system governs 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:

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

$$t_{GE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \frac{\lambda_{DU}}{2}\left(\frac{T_1}{2} + MTTR\right) + \beta \frac{\lambda_{DU}}{2}\left(\frac{T_2}{2} + MTTR\right)$$

Table B.9 below gives the numeric results of a 1oo2 system with a 100 % one-year proof test compared against a 50 % proof test where the demand period T_2 is assumed to be 10 years. This example has been calculated assuming a failure rate of 1×10^{-5} per hour, a β value of 10 % and a β_D value of 5 %.

Tableau B.9 – Exemple d'un test périodique imparfait

Architecture	*DC*	λ = 1.0E-05	
		Test périodique 100 %	Test périodique 50 % (T_2 = dix ans)
		β = 10 % β_D = 5 %	β = 10 % β_D = 5 %
1oo2	0 %	2.7E-03	6.6E-02
	60 %	9.7E-04	2.6E-02
	90 %	2.3E-04	6.6E-03
	99 %	2.4E-05	7.0E-04

B.3 Probabilité de défaillance par heure (pour un mode de fonctionnement demande élevée ou continu)

B.3.1 Procédure de calcul

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 demande élevée ou continu est identique à celle utilisée pour le calcul d'un mode de fonctionnement faible demande (voir B.2.1); la probabilité moyenne de défaillance sur demande (PFD_{SYS}) est cependant remplacée par la probabilité d'une 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 probabilité de défaillance par heure d'une fonction de sécurité du système E/E/PE relatif à la sécurité;

– PFH_S est la probabilité de défaillance par heure du sous-système capteur;

– PFH_L est la probabilité de défaillance par heure du sous-système logique; et

– PFH_{FE} est la probabilité de défaillance par heure du sous-système élément final.

B.3.2 Architectures pour un mode de fonctionnement demande 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.2.2.

NOTE 2 Les calculs sont basés sur les hypothèses données en B.1.

B.3.2.1 1oo1

Les figures B.3 et B.4 montrent les diagrammes de blocs pertinents.

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

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

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC)\,;\ \lambda_{DD} = \frac{\lambda}{2} DC$$

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

Architecture	*DC*	λ = 1.0E-05	
		100 % proof test	50 % proof test (T_2 = 10 years)
		β = 10 % β_D = 5 %	β = 10 % β_D = 5 %
1oo2	0 %	2.7E-03	6.6E-02
	60 %	9.7E-04	2.6E-02
	90 %	2.3E-04	6.6E-03
	99 %	2.4E-05	7.0E-04

B.3 Probability of failure per hour (for high demand or continuous mode of operation)

B.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 probability of a dangerous failure per hour (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 probability of failure per hour of a safety function for the E/E/PE safety-related system;

– PFH_S is the probability of failure per hour for the sensor subsystem;

– PFH_L is the probability of failure per hour for the logic subsystem; and

– PFH_{FE} is the probability of failure per hour for the final element subsystem.

B.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.2.2.

NOTE 2 The calculations are based on the assumptions listed in B.1.

B.3.2.1 1oo1

Figures B.3 and B.4 show the relevant block diagrams.

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

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

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC)\,;\ \lambda_{DD} = \frac{\lambda}{2} DC$$

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.3.2.2 1oo2

Les figures B.5 et B.6 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est donnée en B.3.2.1.

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

B.3.2.3 2oo2

Les figures B.7 et B.8 illustrent les diagrammes de blocs pertinents. Si l'on suppose que chacun des canaux sera 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.3.2.4 1oo2D

Les figures B.9 et B.10 illustrent les diagrammes de blocs pertinents.

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

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

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

B.3.2.5 2oo3

Les figures B.11 et B.12 montrent les diagrammes de blocs pertinents. La valeur de t_{CE} est donnée en B.3.2.1.

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

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.3.2.2 1oo2

Figures B.5 and B.6 show the relevant block diagrams. The value of t_{CE} is as given in B.3.2.1.

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

B.3.2.3 2oo2

Figures B.7 and B.8 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.3.2.4 1oo2D

Figures B.9 and B.10 show the relevant block diagrams.

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

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

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

B.3.2.5 2oo3

Figures B.11 and B.12 show the relevant block diagrams. The value of t_{CE} is as given in B.3.2.1.

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

B.3.3 Tableaux détaillés pour mode de fonctionnement forte demande ou mode de fonctionnement continu

Tableau B.10 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques d'un mois et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 1 %	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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.1E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.0E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

Tableau B.10 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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 %**	2.5E-06			5.0E-06			>1E-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 %	3.7E-08	1.8E-07	3.5E-07	7.7E-08	3.6E-07	7.1E-07	5.4E-07	1.9E-06	3.6E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.7E-07	1.3E-06	2.5E-06
2oo2 (voir la note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	3.6E-08	1.8E-07	3.5E-07	7.3E-08	3.5E-07	7.0E-07	4.3E-07	1.8E-06	3.6E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.5E-08	2.8E-07	5.5E-07	2.8E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-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 %	4.1E-08	1.8E-07	3.5E-07	9.2E-08	3.7E-07	7.2E-07	9.1E-07	2.2E-06	3.9E-06
	90 %	2.9E-08	1.4E-07	2.8E-07	6.2E-08	2.8E-07	5.6E-07	4.4E-07	1.5E-06	2.9E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	3.0E-07	1.3E-06	2.6E-06

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

B.3.3 Detailed tables for high demand or continuous mode of operation

Table B.10 – Probability of failure per hour (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 = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.1E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.0E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

Table B.10 *(continued)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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			>1E-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 %	3.7E-08	1.8E-07	3.5E-07	7.7E-08	3.6E-07	7.1E-07	5.4E-07	1.9E-06	3.6E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.7E-07	1.3E-06	2.5E-06
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	3.6E-08	1.8E-07	3.5E-07	7.3E-08	3.5E-07	7.0E-07	4.3E-07	1.8E-06	3.6E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.5E-08	2.8E-07	5.5E-07	2.8E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-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 %	4.1E-08	1.8E-07	3.5E-07	9.2E-08	3.7E-07	7.2E-07	9.1E-07	2.2E-06	3.9E-06
	90 %	2.9E-08	1.4E-07	2.8E-07	6.2E-08	2.8E-07	5.6E-07	4.4E-07	1.5E-06	2.9E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	3.0E-07	1.3E-06	2.6E-06

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

Tableau B.11 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques de trois mois et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %
		β_D = 1 %	β_D = 5 %	β_D = 10 %	β_D = 1 %	β_D = 5 %	β_D = 10 %	β_D = 1 %	β_D = 5 %	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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.1E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.7E-09	3.6E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

Tableau B.11 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %	β = 2 %	β = 10 %	β = 20 %
		β_D = 1 %	β_D = 5 %	β_D = 10 %	β_D = 1 %	β_D = 5 %	β_D = 10 %	β_D = 1 %	β_D = 5 %	β_D = 10 %
1oo1 (voir la note 2)	**0 %**	2.5E-06			5.0E-06			>1E-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 %	4.0E-08	1.8E-07	3.5E-07	9.2E-08	3.7E-07	7.2E-07	8.9E-07	2.2E-06	3.9E-06
	90 %	2.9E-08	1.4E-07	2.8E-07	6.1E-08	2.8E-07	5.5E-07	4.2E-07	1.5E-06	2.9E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.8E-07	1.3E-06	2.5E-06
2oo2 (voir la note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	3.7E-08	1.8E-07	3.5E-07	7.9E-08	3.6E-07	7.1E-07	5.7E-07	1.9E-06	3.7E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	2.9E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-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 %	5.1E-08	1.9E-07	3.6E-07	1.4E-07	4.1E-07	7.5E-07	2.0E-06	3.2E-06	4.7E-06
	90 %	3.2E-08	1.4E-07	2.8E-07	7.2E-08	2.9E-07	5.6E-07	7.1E-07	1.8E-06	3.1E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.6E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

Table B.11 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of three months and a mean time to restoration of 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.1E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.7E-09	3.6E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

Table B.11 *(continued)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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			>1E-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 %	4.0E-08	1.8E-07	3.5E-07	9.2E-08	3.7E-07	7.2E-07	8.9E-07	2.2E-06	3.9E-06
	90 %	2.9E-08	1.4E-07	2.8E-07	6.1E-08	2.8E-07	5.5E-07	4.2E-07	1.5E-06	2.9E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.8E-07	1.3E-06	2.5E-06
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	3.7E-08	1.8E-07	3.5E-07	7.9E-08	3.6E-07	7.1E-07	5.7E-07	1.9E-06	3.7E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	2.9E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-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 %	5.1E-08	1.9E-07	3.6E-07	1.4E-07	4.1E-07	7.5E-07	2.0E-06	3.2E-06	4.7E-06
	90 %	3.2E-08	1.4E-07	2.8E-07	7.2E-08	2.9E-07	5.6E-07	7.1E-07	1.8E-06	3.1E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.6E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

Tableau B.12 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques de six mois et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.4E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.1E-10	3.5E-09	7.0E-09	3.8E-09	1.8E-08	3.5E-08	8.3E-09	3.6E-08	7.1E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.8E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

Tableau B.12 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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 %**	2.5E-06			5.0E-06			>1E-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 %	4.6E-08	1.8E-07	3.6E-07	1.1E-07	3.9E-07	7.3E-07	1.4E-06	2.7E-06	4.3E-06
	90 %	3.0E-08	1.4E-07	2.8E-07	6.6E-08	2.9E-07	5.6E-07	5.5E-07	1.6E-06	3.0E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	2.9E-07	1.3E-06	2.6E-06
2oo2 (voir la note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	3.9E-08	1.8E-07	3.5E-07	8.7E-08	3.7E-07	7.1E-07	7.8E-07	2.1E-06	3.8E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	3.0E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-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 %	6.7E-08	2.0E-07	3.7E-07	2.0E-07	4.6E-07	8.0E-07	3.6E-06	4.6E-06	6.0E-06
	90 %	3.6E-08	1.5E-07	2.8E-07	8.8E-08	3.1E-07	5.8E-07	1.1E-06	2.1E-06	3.4E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.5E-08	2.6E-07	5.1E-07	3.6E-07	1.4E-06	2.6E-06

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

Table B.12 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of six months and a mean time to restoration of 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.4E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.1E-10	3.5E-09	7.0E-09	3.8E-09	1.8E-08	3.5E-08	8.3E-09	3.6E-08	7.1E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.8E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

Table B.12 *(continued)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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			>1E-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 %	4.6E-08	1.8E-07	3.6E-07	1.1E-07	3.9E-07	7.3E-07	1.4E-06	2.7E-06	4.3E-06
	90 %	3.0E-08	1.4E-07	2.8E-07	6.6E-08	2.9E-07	5.6E-07	5.5E-07	1.6E-06	3.0E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	2.9E-07	1.3E-06	2.6E-06
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	3.9E-08	1.8E-07	3.5E-07	8.7E-08	3.7E-07	7.1E-07	7.8E-07	2.1E-06	3.8E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	3.0E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-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 %	6.7E-08	2.0E-07	3.7E-07	2.0E-07	4.6E-07	8.0E-07	3.6E-06	4.6E-06	6.0E-06
	90 %	3.6E-08	1.5E-07	2.8E-07	8.8E-08	3.1E-07	5.8E-07	1.1E-06	2.1E-06	3.4E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.5E-08	2.6E-07	5.1E-07	3.6E-07	1.4E-06	2.6E-06

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

Tableau B.13 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques d'un an et une durée moyenne de rétablissement de 8 h

Architecture	*DC*	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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 1)	**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 %	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.9E-09	3.6E-08	7.1E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.3E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.3E-10	3.5E-09	7.0E-09	4.1E-09	1.8E-08	3.5E-08	9.6E-09	3.7E-08	7.2E-08
	90 %	5.6E-10	2.8E-09	5.5E-09	2.9E-09	1.4E-08	2.8E-08	6.2E-09	2.8E-08	5.6E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

Tableau B.13 *(suite)*

Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-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 %**	2.5E-06			5.0E-06			>1E-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 %	5.6E-08	1.9E-07	3.7E-07	1.6E-07	4.3E-07	7.7E-07	2.5E-06	3.7E-06	5.1E-06
	90 %	3.3E-08	1.4E-07	2.8E-07	7.7E-08	2.9E-07	5.7E-07	8.2E-07	1.9E-06	3.2E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.5E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06
2oo2 (voir la note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	4.4E-08	1.8E-07	3.6E-07	1.0E-07	3.8E-07	7.3E-07	1.2E-06	2.5E-06	4.1E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	**0 %**	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-06	1.4E-06	>1E-05	>1E-05	>1E-05
	60 %	9.9E-08	2.3E-07	4.0E-07	3.3E-07	5.8E-07	9.0E-07	6.8E-06	7.5E-06	8.4E-06
	90 %	4.4E-08	1.5E-07	2.9E-07	1.2E-07	3.3E-07	6.0E-07	1.9E-06	2.9E-06	4.1E-06
	99 %	2.7E-08	1.3E-07	2.5E-07	5.8E-08	2.6E-07	5.1E-07	4.4E-07	1.4E-06	2.7E-06

NOTE 1 Ce tableau donne des exemples de valeurs de PFH_G calculées en appliquant les équations données en B.3.2 et en fonction des hypothèses énoncées en B.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.3.1 et B.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.

Table B.13 – Probability of failure per hour (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 = 1.0E-07			λ = 5.0E-07			λ = 1.0E-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 %	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.9E-09	3.6E-08	7.1E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
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	**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 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.3E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-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 %	7.3E-10	3.5E-09	7.0E-09	4.1E-09	1.8E-08	3.5E-08	9.6E-09	3.7E-08	7.2E-08
	90 %	5.6E-10	2.8E-09	5.5E-09	2.9E-09	1.4E-08	2.8E-08	6.2E-09	2.8E-08	5.6E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

Table B.13 *(continued)*

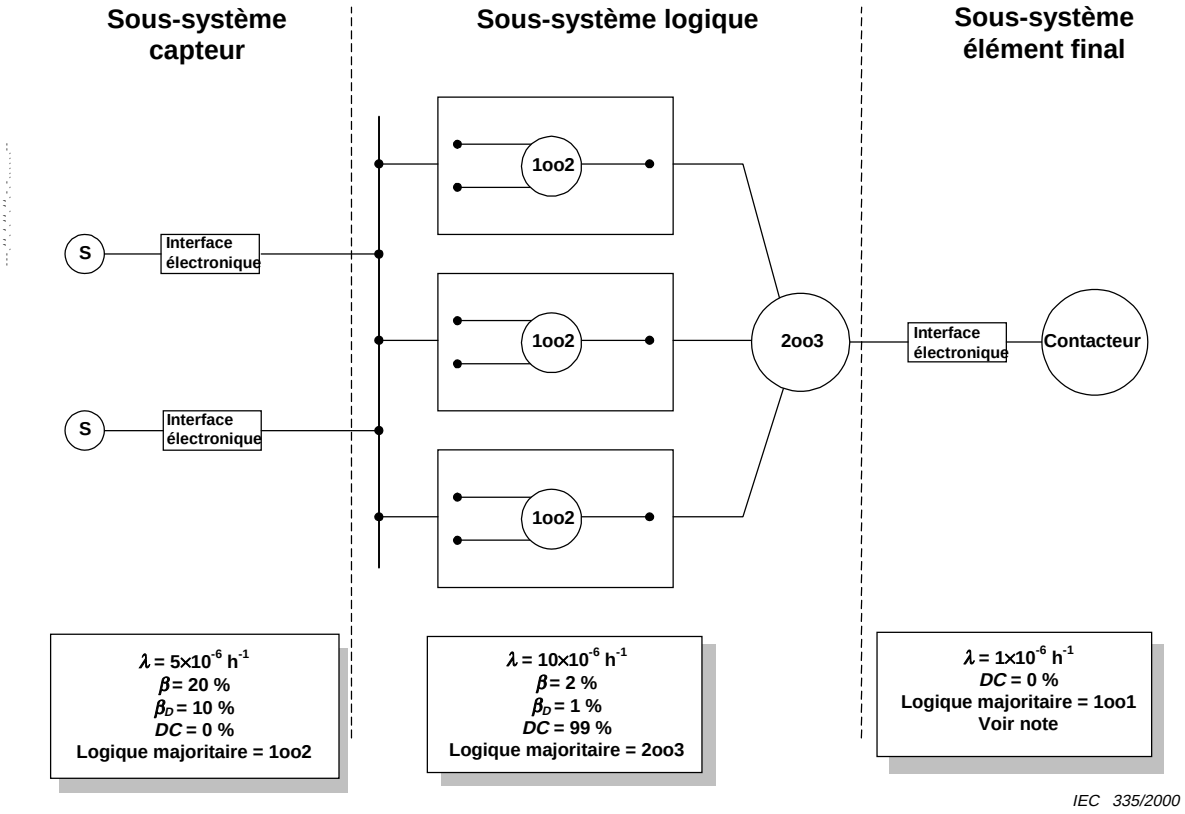
Architecture	*DC*	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	**0 %**	2.5E-06			5.0E-06			>1E-05		
	60 %	1.0E-06			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 %	5.6E-08	1.9E-07	3.7E-07	1.6E-07	4.3E-07	7.7E-07	2.5E-06	3.7E-06	5.1E-06
	90 %	3.3E-08	1.4E-07	2.8E-07	7.7E-08	2.9E-07	5.7E-07	8.2E-07	1.9E-06	3.2E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.5E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06
2oo2 (see note 2)	**0 %**	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	**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 %	4.4E-08	1.8E-07	3.6E-07	1.0E-07	3.8E-07	7.3E-07	1.2E-06	2.5E-06	4.1E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	**0 %**	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-06	1.4E-06	>1E-05	>1E-05	>1E-05
	60 %	9.9E-08	2.3E-07	4.0E-07	3.3E-07	5.8E-07	9.0E-07	6.8E-06	7.5E-06	8.4E-06
	90 %	4.4E-08	1.5E-07	2.9E-07	1.2E-07	3.3E-07	6.0E-07	1.9E-06	2.9E-06	4.1E-06
	99 %	2.7E-08	1.3E-07	2.5E-07	5.8E-08	2.6E-07	5.1E-07	4.4E-07	1.4E-06	2.7E-06

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.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.3.1 and B.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.

B.3.4 Exemple pour mode de fonctionnement demande élevée ou mode continu

Soit une fonction de sécurité exigeant un système de niveau SIL2. Supposons que l'évaluation initiale pour cette architecture, 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.14. On suppose un test 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 %.

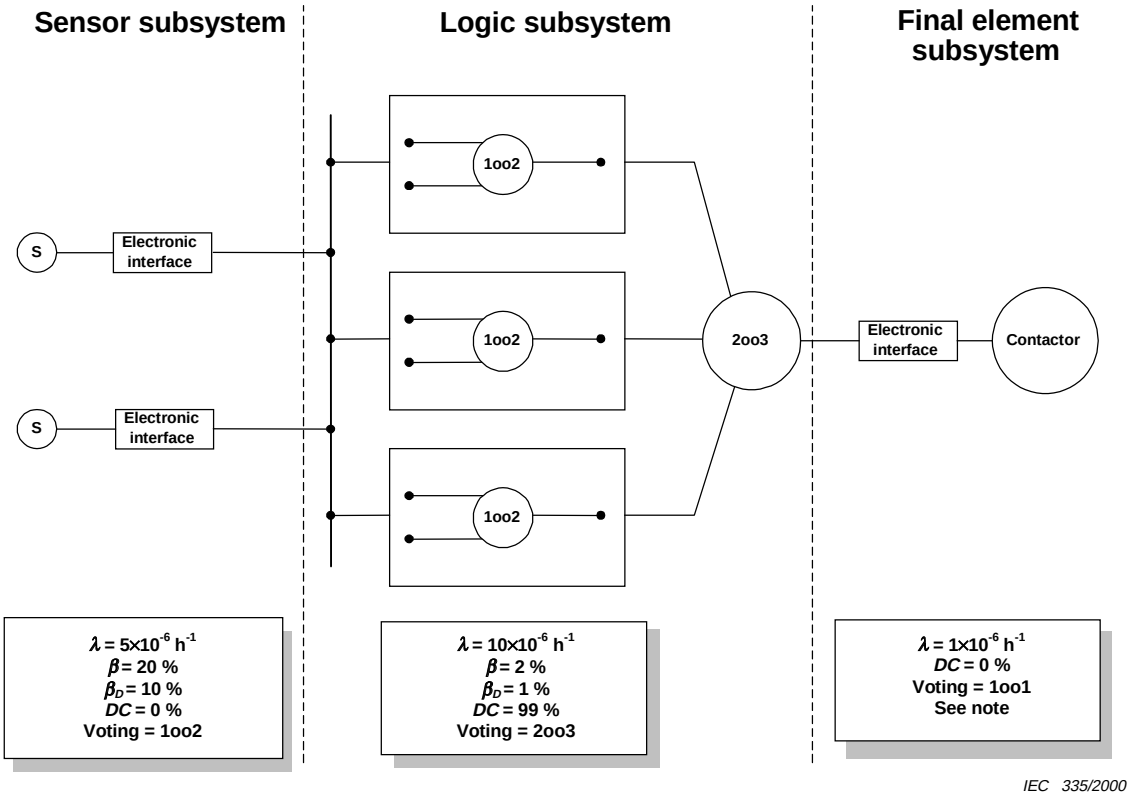
Figure B.14 – Architecture d'un exemple de fonctionnement en mode demande élevée ou continu

Tableau B.14 – Probabilité de défaillance par heure du sous-système capteur dans l'exemple de mode de fonctionnement demande élevée ou continu (intervalle entre tests périodiques de six mois et MTTR de 8 h)

Architecture	*DC*	λ = 5.0E-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 %	4.6E-08	1.8E-07	3.6E-07
	90 %	3.0E-08	1.4E-07	2.8E-07
	99 %	2.6E-08	1.3E-07	2.5E-07
NOTE Ce tableau est extrait du tableau B.12.				

B.3.4 Example for high demand or continuous mode of operation

Consider a safety function requiring a SIL2 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 PES driving a single shutdown contactor. This is shown in figure B.14. 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.14 – Architecture of an example for high demand or continuous mode of operation

Table B.14 – Probability of failure per hour 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 = 5.0E-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 %	4.6E-08	1.8E-07	3.6E-07
	90 %	3.0E-08	1.4E-07	2.8E-07
	99 %	2.6E-08	1.3E-07	2.5E-07
NOTE This table is abstracted from table B.12.				

Tableau B.15 – Probabilité de défaillance par heure du sous-système logique dans l'exemple de mode de fonctionnement demande élevée ou continu (intervalle entre tests périodiques de six mois et MTTR de 8 h)

Architecture	*DC*	λ = 1.0E-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 %	2.0E-07	4.6E-07	8.0E-07
	90 %	8.8E-08	3.1E-07	5.8E-07
	99 %	5.5E-08	2.6E-07	5.1E-07
NOTE Ce tableau est extrait du tableau B.12.				

Tableau B.16 – Probabilité de défaillance par heure du sous-système élément final dans l'exemple de mode de fonctionnement demande élevée ou continu (intervalle entre tests périodiques de six mois et MTTR de 8 h)

Architecture	*DC*	λ = 1.0E-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,

$PFH_L = 5{,}5 \times 10^{-8}$ / h

Pour le sous-système élément final,

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

Ainsi, pour la fonction de sécurité,

$PFH_{SYS} = 5{,}2 \times 10^{-7} + 5{,}5 \times 10^{-8} + 5{,}0 \times 10^{-7}$

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

$\equiv$ **niveau 1 d'intégrité de sécurité**

Table B.15 – Probability of failure per hour 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 = 1.0E-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 %	2.0E-07	4.6E-07	8.0E-07
	90 %	8.8E-08	3.1E-07	5.8E-07
	99 %	5.5E-08	2.6E-07	5.1E-07
NOTE This table is abstracted from table B.12.				

Table B.16 – Probability of failure per hour 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 = 1.0E-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,

$PFH_L = 5{,}5 \times 10^{-8}$/ h

For the final element subsystem,

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

Therefore, for the safety function,

$PFH_{SYS} = 5{,}2 \times 10^{-7} + 5{,}5 \times 10^{-8} + 5{,}0 \times 10^{-7}$

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

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

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

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

PFH_{SYS} = $8{,}3 \times 10^{-7}$ / 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 = $5{,}5 \times 10^{-8}$ / h

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

PFH_{SYS} = $6{,}3 \times 10^{-7}$ / h

≡ **niveau 2 d'intégrité de sécurité**

B.4 Références

Voir les références [1] à [6] dans la bibliographie pour des détails complémentaires sur l'évaluation des probabilité de défaillance.

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

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

PFH_{SYS} = $8{,}3 \times 10^{-7}$ / 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 = $5{,}5 \times 10^{-8}$ / h

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

PFH_{SYS} = $6{,}3 \times 10^{-7}$ / h

≡ **safety integrity level 2**

B.4 References

References [1] to [6] in the bibliography give further details on evaluating probabilities of failure.

Annexe C
(informative)

Calcul de la couverture du diagnostic et de la proportion de défaillance en sécurité: exemple élaboré

Une méthode de calcul de la couverture du 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 du diagnostic d'un système E/E/PE relatif à la sécurité. 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 du diagnostic qui peuvent être revendiquées pour certains composants ou sous-systèmes 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, qui permettrait de déterminer tous les modes de défaillance devrait être déterminé. Ces valeurs ne sont données qu'à titre d'exemple, et certains composants du tableaux C.1 ne supportent pas de couverture du 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 tests 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 du diagnostic pour chaque test 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 du 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 de tests de diagnostic, pour chaque composant (respectivement λ_S and 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 (soit 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 du 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 du diagnostic spécifique pour défaillances dangereuses de un et en multipliant le résultat obtenu par le taux de défaillances dangereuses (voir colonne (4)).

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 of an E/E/PE safety-related system. 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 system components or subsystems. 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) 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 du diagnostic respectivement par le taux de défaillance 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 du diagnostic pour des défaillances en sécurité

$$\frac{\sum \lambda_{SD}}{\sum \lambda_S} = \frac{3{,}38}{3{,}65} = 93\ \%$$

couverture du diagnostic des défaillances dangereuses

$$\frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{6{,}21}{6{,}72} = 92\ \%$$

(en général simplement désignée par l'expression «couverture du diagnostic»)

proportion de défaillances en sécurité

$$\frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{986}{365 + 672} = 95\ \%$$

g) La répartition du taux de défaillance sans tests de diagnostic est de 35 % de défaillances non dangereuses et de 65 % de défaillances dangereuses.

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 $\dfrac{\sum \lambda_{SD}}{\sum \lambda_S} = \dfrac{3{,}38}{3{,}65} = 93\ \%$

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 $\dfrac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} = \dfrac{986}{365 + 672} = 95\ \%$

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

Tableau C.1 – Exemples de calcul de la couverture du 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 du 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 du 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 n'importe lequel des composants.

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.

Tableau C.2 – Couverture du diagnostic et efficacité pour différents sous-systèmes

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 %	-
calcul d'adresse (voir note 3)	50 % - 70 %	85 % - 98 %	-
registre d'adresse d'instruction, pointeur de pile	50 % - 60 %	60 % - 90 %	85 % - 98 %
	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 terminaux	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 du 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 de test qui appliquent une contrainte dynamique élevée sur la fonction à tester.

NOTE 3 Pour les techniques n'ayant pas de valeur élevée de couverture du 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 temporaire et logique est d'efficacité moyenne.

Voir les références [7]* à [9].

———————

* Les chiffres entre crochets se réfèrent à la bibliographie.

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

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.

Useful references include those listed as [7]* to [9].

———————

* Figures in square brackets refer to the bibliography.

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

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 y a 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, le potentiel de défaillance pouvant affecter plus d'un canal sur des systèmes à plusieurs canaux, c'est-à-dire des défaillances de cause commune, se traduit en erreurs substantielles lorsque des calculs de fiabilité seront appliqués à des systèmes à plusieurs canaux.

Cette annexe informative décrit une méthodologie qui permet de prendre en compte les défaillances de cause commune dans l'évaluation de sécurité des systèmes E/E/PE à plusieurs canaux. L'utilisation de cette méthodologie permet d'estimer l'intégrité d'un tel système de manière plus précise que si les défaillances de cause commune potentielles sont ignorées.

Cette méthodologie est utilisée pour calculer une valeur de β, facteur fréquemment utilisé dans la modélisation des défaillances de cause communes. 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). D'autres méthodologies sont dans certains cas préférables, notamment lorsqu'un facteur β plus précis peut être obtenu grâce à la disponibilité de données relatives aux défaillances de cause commune.

D.2 Présentation concise

On considère que les défaillances d'un système ont deux causes:

– 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. Il existe une probabilité restreinte que des défaillances aléatoires du matériel puissent avoir lieu sur tous les canaux d'un système à plusieurs canaux de sorte que tous les canaux présentent 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.

Toutefois, certaines défaillances, c'est-à-dire les défaillances de cause commune résultant d'une cause unique, peuvent affecter plusieurs canaux. Celles-ci peuvent avoir pour origine une défaillance systématique (par exemple, une erreur de conception ou de spécification) ou d'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 sera 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.

Annex D
(informative)

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

D.1 General

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, i.e. common cause failures, results in substantial errors when reliability calculations are applied to multi-channel systems.

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

The methodology is used to calculate a value for β, the 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). 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.

D.2 Brief overview

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

– 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. 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.

However, some failures, i.e. common cause failures which result from a single cause, may affect more than one channel. 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.

Bien que les défaillances de cause commune résultent d'une cause unique, elles ne se manifestent pas simultanément dans tous les canaux. Par exemple, si un ventilateur est défectueux, tous les canaux d'un système E/E/PE à plusieurs voies pourraient 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 de test de l'ordre de 99 % est réalisable [10]. 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 tests 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 le test 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 test 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 au test 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 tests 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 voies d'approche peuvent être empruntées pour réduire la probabilité des défaillances de cause commune potentiellement dangereuses.

Although common cause failures result from a single cause, they do not all manifest themselves 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 PES 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 [10]. 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 PES can monitor the outputs of other channels in a multi-channel PES (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) 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. (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 lorsqu'un seul canal est affecté et avant qu'un deuxième ne le soit, c'est-à-dire utiliser les tests de diagnostic.

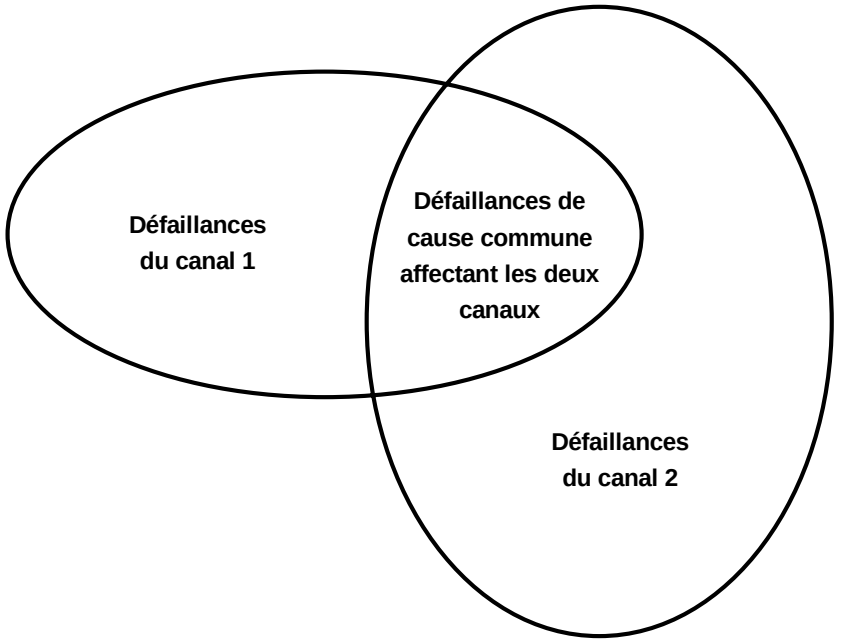


Figure D.1 – Relation entre défaillances de cause commune et défaillances de canaux individuels

La présente norme se fonde sur ces trois orientations et nécessite donc une triple approche.

a) Appliquer les techniques spécifiées dans la CEI 61508 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 cette 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 sera 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,

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. (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.

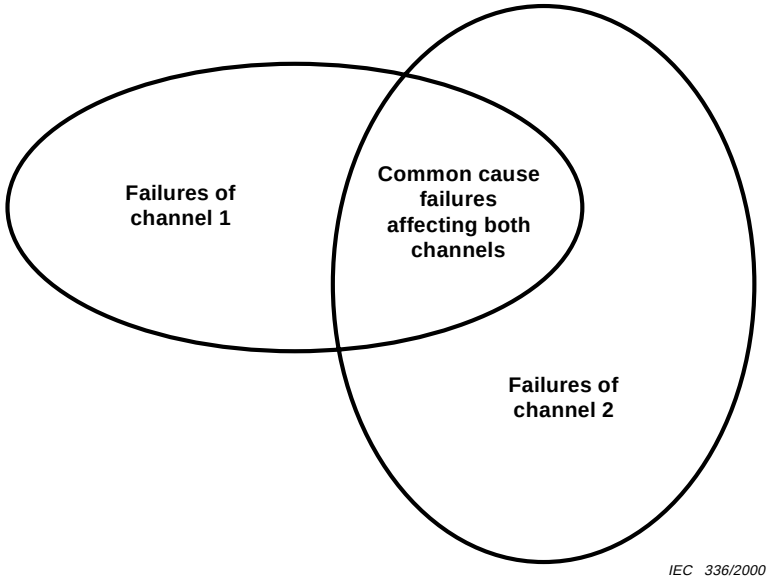


Figure D.1 – Relationship of common cause failures to the failures of individual channels

This standard is based on these three avenues and requires a threefold approach.

a) Apply the techniques specified in IEC 61508 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

- une réparation, suivie de tests 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 tests 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 tests, 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.

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 d'un système à plusieurs canaux. La méthodologie décrite dans cette annexe se fonde sur une approche similaire au modèle communément admis du facteur β, utilisée comme troisième partie de la triple approche décrite ci-dessus.

On se heurte aux deux difficultés suivantes lorsque l'on utilise le facteur β sur un système E/E/PE.

– Quelle valeur convient-il de choisir pour le facteur β ? 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 de la présente annexe se fonde sur le système décrit en premier lieu dans la référence [11] et récemment redéfinie dans la référence [12].

– Le modèle du facteur β ne tient pas compte des capacités de test de diagnostic sophistiquées des systèmes électroniques programmables modernes, qui peuvent être utilisées pour la détection de défaillances de cause commune non simultanées avant qu'elle 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 tests de diagnostic sur l'estimation de la valeur probable de β.

Les fonctions de test 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 sous cette optique, les fonctions de test 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 nombreuse 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 tests 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.

  - 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.

Despite the limitations of the current models, it is believed that they represent the best way forward at the present time for providing an estimate of the probability of common cause failure of a multi-channel system. The methodology described in this annex uses an approach similar to the well-established β-factor model as the third part of the threefold approach already described.

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

- What value should be chosen for the β-factor? Many sources (for example reference [10]) 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 methodology in this annex is based on the system originally described in reference [11] and recently redefined in reference [12].
- The β-factor model does not take into account the sophisticated diagnostic testing capabilities of modern PESs, 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 [11] and [12] 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 PES are continuously comparing the operation of the PES 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 PES.

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 PES technology, cross-monitoring may be carried out with a high repetition frequency.

D.3 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 relie la probabilité de défaillance de cause commune à la probabilité de défaillances aléatoires du matériel. La probabilité de défaillance 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 déduire un taux de défaillance global prenant en compte la probabilité de défaillance relative au logiciel.

D.4 Eléments à prendre en compte dans la méthodologie

Puisque les capteurs, les sous-systèmes logiques et éléments finaux sont sujets, par exemple, à des conditions environnementales différentes et des tests 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 de test 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 terminaux.

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 tests 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.

Toutes les caractéristiques d'un système à plusieurs canaux, qui ont une incidence sur son immunité aux défaillances de cause commune, ne peuvent pas être évaluée par les tests de diagnostic. Cependant, les caractéristiques ayant trait à la diversité ou à l'indépendance sont réalisées avec plus d'efficacité. 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 des tests de diagnostic et de mise en sécurité de l'usine. 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 de tests 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.

D.3 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 model relates 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.4 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 have 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.

Toutefois, pour un système à trois canaux, la probabilité que des défaillances de cause commune affectent les trois canaux sera légèrement inférieure à la probabilité de défaillance affectant deux canaux; on suppose, pour simplifier la méthodologie, 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.

Il n'existe pas de données disponibles connues sur les défaillances de cause commune relatives au matériel permettant l'étalonnage de cette méthodologie. Les tableaux de la présente annexe ont donc été élaborés à partir d'un raisonnement théorique.

Les programmes de test 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 tests de diagnostic possèdent une intégrité qui correspond au niveau d'intégrité de sécurité cible. Il convient donc de développer tout programme de test de diagnostic lié au logiciel en utilisant des techniques adaptées au niveau d'intégrité de sécurité cible.

D.5 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 de tests de diagnostic dans chacun de ses canaux.

Si l'on utilise le modèle du facteur β, la probabilité de défaillance de cause commune est

$$\lambda_D \beta$$

où λ_D est la probabilité de défaillance dangereuse aléatoire du matériel pour chaque canal individuel et β est le facteur β en l'absence de tests 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 à l'intervalle de temps entre des défaillances de cause commune successives.

Supposons qu'il existe des tests 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 tests de diagnostic (et qui ne seront donc jamais détectées) et celles qui s'inscrivent dans cette couverture (qui seront en fin de compte détectées par les tests de diagnostic).

La probabilité globale de défaillance provoquée par des défaillances de cause commune est donc donnée par

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

où

– λ_{DU} est la probabilité d'une défaillance non détectée d'un canal unique, c'est-à-dire la probabilité de défaillances qui ne s'inscrivent pas dans la couverture des tests de diagnostic; toute réduction dans le facteur β induite par la fréquence de répétition des tests de diagnostic n'affectera manifestement pas cette fraction 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 de test de diagnostic.

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 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.

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.5 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 probability of dangerous common cause failures is

$$\lambda_D \beta$$

where λ_D is the probability of dangerous random hardware failures 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 probability of failure due to dangerous common cause failures is then given by

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

where

- λ_{DU} is the probability of an undetected failure of a single channel, i.e. the probability of 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} est la probabilité d'une défaillance détectée d'un canal unique, c'est-à-dire la probabilité de défaillances d'un seul canal qui s'inscrivent dans la couverture des tests de diagnostic; ici, lorsque la fréquence de répétition est élevée, une fraction des défaillances est découverte, entraînant ainsi une réduction de la valeur de β, c'est-à-dire β_D;

– β_D est le facteur de défaillance de cause commune pour les anomalies dangereuses détectées. Plus le taux de répétition du test de diagnostic est augmenté, plus la valeur de β_D descend en dessous de celle de β.

– β est obtenu à partir du tableau D.4, en utilisant un résultat tel que, $S = X + Y$ (voir D.6);

– β_D est obtenu à partir du tableau D.4, en utilisant un résultat tel que, $S_D = X(Z+1) + Y$.

D.6 Utilisation des tables pour l'estimation de β

Il convient de calculer séparément le facteur β pour les capteurs, le sous-système logique et les éléments terminaux.

Afin de réduire au minimum la probabilité d'occurrence de défaillances de cause commune, il faut 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 estimation d'ingénierie, qui représente la contribution de chacune des mesures à la réduction des défaillances de cause commune. Les capteurs et éléments terminaux sont traités différemment des composants électroniques programmables, et des colonnes distinctes sont donc utilisées dans le tableau D.1 pour énumérer ces composants ainsi que les capteurs ou éléments terminaux.

Des tests de diagnostic peuvent être inclus dans des systèmes électroniques programmables pour détecter des défaillances de cause commune non simultanées. Pour pouvoir prendre en compte les tests de diagnostic dans l'estimation du facteur β, la contribution globale de chaque mesure du tableau D.1 est répartie, en utilisant une estimation d'ingénierie, 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 défaillance de cause commune par les tests 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_{SA} et Y_{SA} pour les capteurs ou éléments terminaux, 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 tests 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, comme indiqué (voir l'article précédent):

– $S = X + Y$ pour obtenir la valeur de β (facteur β pour les défaillances non détectées); et

– $S_D = X(Z+1) + Y$ pour obtenir la valeur de β_D (facteur β pour défaillances détectées).

Ici, S ou S_D est le résultat utilisé dans le tableau D.4 pour déterminer le facteur β approprié.

– λ_{DD} is the probability of a detected failure of a single channel, i.e. the probability of failures of a single channel that lie within the coverage of the diagnostic tests; here, 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.4, using a score, $S = X + Y$ (see D.6);

– β_D is obtained from table D.4, using a score, $S_D = X(Z+1) + Y$.

D.6 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 (the β-factor for undetected failures); and

– $S_D = X(Z+1) + Y$ to obtain the value of β_D (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-factor.

Tableau D.1 – Calcul des résultats électroniques programmables ou des capteurs/éléments terminaux

Article	Sous-système logique		Capteurs et éléments terminaux	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
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 dans des armoires séparées ?	2,5	0,5		
Si les capteurs/éléments terminaux 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 terminaux 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 ?	7,0			
Les canaux emploient-ils des technologies électroniques différentes, par exemple, un canal électronique et l'autre un canal électronique programmable ?	5,0			
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. ?			7,5	
Les dispositifs utilisent-ils des principes électriques/conceptions différents par exemple numérique et analogique, fabricant différent (pas simplement de marque différente) ou technologie différente ?			5,5	
Les canaux emploient-ils une redondance améliorée avec architecture MooN, où $N > M + 2$?	2,0	0,5	2,0	0,5
Les canaux emploient-ils une redondance améliorée avec architecture MooN, où $N = M + 2$?	1,0	0,5	1,0	0,5
Une faible diversité est-elle utilisée par exemple des tests de diagnostic du matériel utilisant la même technologie ?	2,0	1,0		
Une diversité moyenne est-elle utilisée, par exemple des tests de diagnostic utilisant une technologie différente	3,0	1,5		
Les canaux ont-ils été conçus par des concepteurs différents sans communiquer entre eux pendant les activités de conception ?	1,0	1,0		
Des méthodes de test et des individus différents sont-ils utilisés pour chaque canal pendant la mise en service ?	1,0	0,5	1,0	1,0
La maintenance de chaque canal est-elle réalisée par des personnes différentes à des moments différents ?	2,5		2,5	
Complexité/conception/application/maturité/expérience				
L'interconnexion entre des canaux prévient-elle l'échange d'informations autres que celles utilisées pour les besoins des tests 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

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 subsystem channels 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?	7,0			
Do the channels employ different electronic technologies for example, one electronic, the other programmable electronic?	5,0			
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc?			7,5	
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?			5,5	
Do the channels employ enhanced redundancy with MooN architecture, where $N > M + 2$?	2,0	0,5	2,0	0,5
Do the channels employ enhanced redundancy with MooN architecture, where $N = M + 2$?	1,0	0,5	1,0	0,5
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	1,5		
Were the channels designed by different designers with no communication between them during the design activities?	1,0	1,0		
Are separate test methods and people used for each channel during commissioning?	1,0	0,5	1,0	1,0
Is maintenance on each channel carried out by different people at different times?	2,5		2,5	
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

Tableau D.1 *(suite)*

Article	Sous-système logique		Capteurs et éléments terminaux	
	X_{LS}	Y_{LS}	X_{SA}	Y_{SA}
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 tests 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 exemples des câbles, etc.), conçus pour être indépendants les uns des autres, ne seront pas allouées de façons différentes ?	0,5	0,5	0,5	0,50
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 tests 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 tests de diagnostic du système rapportent-ils les défaillances au niveau d'un module remplaçable en exploitation ?			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 testé, 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 pourrait 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 estimation d'ingénierie et prennent en compte les effets directs et indirects des articles énumérés dans la première colonne. Par exemple, l'utilisation de modules de remplacement sur le terrain 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*.

Table D.1 *(continued)*

Item	Logic subsystem		Sensors and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
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		
Does the system diagnostic tests report failures to the level of a field-replaceable module?			1,0	1,0
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.

Tableau D.2 – Valeur de *Z*: électronique programmable

Couverture du diagnostic	Intervalle entre les tests 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 terminaux

Couverture du diagnostic	Intervalle entre les tests de diagnostic			
	Moins de 2 heures	Entre 2 heures 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 terminaux 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 terminaux dans le cas contraire.

NOTE 4 Pour une valeur non nulle de *Z*, il convient de s'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 tests 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 [1)], mais les tests de diagnostic

  - déterminent l'emplacement de l'anomalie et sont capables de localiser l'anomalie, et
  - sont toujours aptes à placer l'EUC en sécurité après la détection d'anomalies postérieures; ou

– une procédure de travail formelle est en mise place pour s'assurer que la cause de toute anomalie détectée est examinée de manière exhaustive pendant l'intervalle entre tests 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 tests de diagnostic signalé.

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 tests de diagnostic tel que décrit dans le tableau D.2. Il est recommandé de ne pas interpréter cette méthodologie comme une prescription exigeant 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 réduction du facteur β ne peut être obtenue par l'utilisation de tests 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 tests 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 de tests de diagnostic. La couverture du diagnostic est la couverture totale assurée par tous les modules.

———————————

1) Il faut prendre en compte le fonctionnement du système pour l'identification d'une anomalie. Par exemple, il faut 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 indentification d'une défaillance simple. Si cela n'est pas le cas, une défaillance sur un second canal pourrait 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 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.

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 2 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 [1)], 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.

---

1) 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.

Tableau D.4 – Calcul de β ou de β_D

Résultat (S ou S_D)	Valeur correspondante de β ou de β_D pour:	
	Sous-système logique	Capteurs ou éléments terminaux
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 β_D 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 β_D inférieures à 0,5 % pour le sous-système logique et à 1 % pour les capteurs seraient difficiles à justifier.

D.7 Exemples de l'utilisation de la méthodologie

Afin de démontrer les effets de cette méthodologie, quelques exemples simples ont été extraits du tableau D.5 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 tests 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; 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 divers 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.

Table D.4 – Calculation of β or β_D

Score (S or S_D)	Corresponding value of β or β_D 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 β_D 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 β_D lower than 0,5 % for the logic subsystem and 1 % for the sensors would be difficult to justify.		

D.7 Examples of the use of the methodology

In order to demonstrate the effect of using the methodology, some simple examples have been worked through in table D.5 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.

Tableau D.5 – Exemples de valeurs pour l'électronique programmable

Catégorie		Diversité du système avec test de diagnostic satisfaisant	Diversité du système avec test de diagnostic médiocre	Redondance du système avec test de diagnostic satisfaisant	Redondance du système avec test 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'environnent	*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 du 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 %

D.8 Références

Les références [10] à [12] donnent des informations utiles en ce qui concerne les défaillances de cause commune.

Table D.5 – Example values for programmable electronics

Category		Diverse system with good diagnostic testing	Diverse system with poor diagnostic testing	Redundancy system with good diagnostic testing	Redundancy 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 %

D.8 References

References [10] to [12] provide useful information relating to common cause failures.

Annexe E
(informative)

Exemples d'application des tableaux d'intégrité de sécurité logicielle contenus dans la CEI 61508-3

E.1 Généralités

Cette 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.

Le premier 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. Le système électronique programmable relatif à la sécurité utilise le langage à contact pour le programme d'application, comme illustration de programmation d'application dans un langage de variabilité limitée.

Le second exemple est un programme d'arrêt réalisé avec un langage de haut niveau, de niveau 3 d'intégrité de sécurité.

Ces deux exemples fictifs donnent des conseils pour l'application des tableaux d'intégrité de sécurité du logiciel dans différentes circonstances. 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.

E.2 Exemple pour le niveau 2 d'intégrité de sécurité

L'application est composée de plusieurs cuves de réacteur liées par des cuves de stockage intermédiaire qui sont remplies de gaz inerte à certain points du cycle de réaction afin de supprimer ignition 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 était exigé, et que le niveau 2 d'intégrité de sécurité était 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;
– le langage utilisé pour la programmation de l'application est un langage à contact, 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 tests de validation;

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.

The first 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 second example is a shut-down application based on a high-level language, of safety integrity level 3.

Both worked examples provide guidance on how the software safety integrity tables might be applied in different circumstances. 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.

E.2 Example for safety integrity level 2

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 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;

– 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 3.8.10 de la CEI 61508-4.

Les tableaux suivants montrent comment l'annexe A de la CEI 61508-3 peut être interprétée pour cette application.

NOTE 2 Dans les colonnes de références (intitulées Réf.) des tableaux suivants, les paragraphes techniques/mesures (par exemple, B.2.4, C.3.1) se réfèrent à la CEI 61508-7 et les tableaux (par exemple, tableau B.7) se réfèrent à la CEI 61508-3.

NOTE 3 Les notes de 7.4.3, 7.4.4 et 7.4.5 de la CEI 61508-3 donnent des information sur la répartition des responsabilités entre le fournisseur et l'utilisateur lorsqu'une programmation à variabilité limitée est utilisée.

Tableau E.1 – Spécification des prescriptions de sécurité (voir 7.2 de la CEI 61508-3)

Technique/mesure	Réf.	SIL2	Interprétation pour cette application
1 Outils de spécification assistée par ordinateur	B.2.4	R	Outils de développement fournis par le fabricant de PLC
2a Méthodes semi-formelles	Tableau B.7	R	Diagrammes cause-conséquence, diagrammes de séquence, blocs fonctionnels. Typiquement utilisés pour la spécification de prescriptions d'application logicielles sur PLC
2b Méthodes formelles comprenant, par exemple, CCS, CSP, HOL, LOTOS, OBJ, logique temporelle, VDM et Z	C.2.4	R	Pas utilisées pour la programmation en langage de variabilité limitée
NOTE Les prescriptions de sécurité du logiciel ont été spécifiées en langage naturel.			

– modifications (if needed) require authorization by a person independent of the software team.

NOTE 1 For the definition of an independent person, see 3.8.10 of IEC 61508-4.

The following tables show how annex A of IEC 61508-3 may be interpreted for this application.

NOTE 2 In the reference columns (entitled Ref) of the following tables, the technique/measure subclauses (e.g. B.2.4, C.3.1) refer to IEC 61508-7 and the tables (e.g. table B.7) refer to IEC 61508-3.

NOTE 3 See the notes to 7.4.3, 7.4.4 and 7.4.5 of IEC 61508-3 for information on the division of responsibility between supplier and user when limited variability programming is used.

Table E.1 – Software safety requirements specification (see 7.2 of IEC 61508-3)

Technique/measure	Ref	SIL2	Interpretation in this application
1 Computer-aided specification tools	B.2.4	R	Development tools supplied by the PLC manufacturer
2a Semi-formal methods	Table B.7	R	Cause-effect diagrams, sequence diagrams, function blocks. Typically used for PLC application software requirements specification
2b Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	R	Not used for limited variability programming
NOTE The software safety requirements were specified in natural language.			

Tableau E.2 – Conception et réalisation 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 d'anomalie et diagnostic	C.3.1	R	Vérification domaine de valeur, chien de garde, entrées/sorties, communication. Emettre une alarme en cas d'erreur (voir 3a)
2 Code de détection et correction d'erreurs	C.3.2	R	Inclus dans les options utilisateur - sélection faite avec le soin nécessaire
3a Programmation par assertion des défaillances	C.3.3	R	Dédiée à certain programmes PLC à langage à contact pour tester certaines conditions essentielles de sécurité (voir 1)
3b Techniques à base de dispositif externe de sécurité	C.3.4	R	Contrôler les combinaisons d'entrées/sorties autorisées dans un superviseur de sécurité matériel indépendant
3c Programmation diversifiée	C.3.5	R	Requis par l'application (voir 3b)
3d Bloc de récupération	C.3.6	R	Inclus dans les options utilisateur - sélection faite avec soin nécessaire
3e Récupération arrière	C.3.7	R	Inclus dans les options utilisateur - sélection faite avec soin nécessaire
3f Récupération avant	C.3.8	R	Inclus dans les options utilisateur - sélection faite avec soin nécessaire
3g Mécanismes de récupération d'anomalie par relance	C.3.9	R	Utilisés comme requis par l'application (voir 2 et 3b)
3h Mémorisation de cas d'exécution	C.3.10	R	Pas utilisée pour la programmation en langage de variabilité limitée
4 Dégradation «élégante»	C.3.11	R	Pas utilisée pour la programmation en langage de variabilité limitée
5 Intelligence artificielle - correction d'anomalie	C.3.12	NR	Pas utilisée pour la programmation en langage de variabilité limitée
6 Reconfiguration dynamique	C.3.13	NR	Pas utilisée pour la programmation en langage de variabilité limitée
7a Méthodes structurées comprenant, par exemple, JSD, MASCOT, SADT et Yourdon.	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
7b Méthodes semi-formelles	Tableau B.7	R	Peuvent être utilisées pour l'interface DCS
7c Méthodes formelles comprenant, par exemple, CCS, CSP, HOL, LOTOS, OBJ, logique temporelle, VDM et Z	C.2.4	R	Rarement utilisées pour la programmation en langage de variabilité limitée
8 Outils de spécification assistée par ordinateur	B.2.4	R	Outils de développement fournis par le fabricant de PLC
NOTE Il n'est pas pratique d'implémenter certaines des techniques ci-dessus lorsqu'on programme dans un langage de variabilité limitée.			

Tableau E.3 – Conception et réalisation du logiciel: outils supports 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 adéquat	C.4.6	HR	En général langage graphique, et souvent propriétaire, dépendant du fournisseur
2 Langage de programmation fortement typé	C.4.1	HR	Texte structuré selon la CEI 61131-3
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 certifiés	C.4.3	HR	Disponibles chez les fabricants de PLC
4b Outils 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
5a Traducteur certifié	C.4.3	HR	Disponibles chez les fabricants de PLC
5b Traducteur: confiance accrue résultant de l'utilisation	C.4.4	HR	Pas utilisée pour la programmation en langage de variabilité limitée
6 Bibliothèque de modules logiciels et composants éprouvés/vérifiés	C.4.5	HR	Blocs fonctionnels, programmes composants

Table E.2 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3)

Technique/measure	Ref	SIL2	Interpretation in this application
1 Fault detection and diagnosis	C.3.1	R	Checking of data range, watch-dog timer, I/O, communication. Raise an alarm if errors (see 3a)
2 Error detecting and correcting 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 Safety bag techniques	C.3.4	R	Check legal I/O combinations in an independent hardware safety monitor
3c Diverse programming	C.3.5	R	Required by the application (see 3b)
3d Recovery block	C.3.6	R	Embedded with user options – careful selection required
3e Backward recovery	C.3.7	R	Embedded with user options - careful selection required
3f Forward recovery	C.3.8	R	Embedded with user options - careful selection required
3g Re-try fault recovery mechanisms	C.3.9	R	Used as required by the application (see 2 and 3b)
3h Memorizing executed cases	C.3.10	R	Not used for limited variability programming
4 Graceful degradation	C.3.11	R	Not used for limited variability programming
5 Artificial intelligence fault correction	C.3.12	NR	Not used for limited variability programming
6 Dynamic reconfiguration	C.3.13	NR	Not used for limited variability programming
7a Structured methods including for example, JSD, MASCOT, SADT and Yourdon.	C.2.1	HR	Data flow methods and data logic tables may be used for representing at least the design architecture
7b Semi-formal methods	Table B.7	R	May be used for DCS interface
7c Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	R	Rarely used for limited variability programming
8 Computer-aided specification tools	B.2.4	R	Development tools supplied by the PLC manufacturer
NOTE 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	SIL2	Interpretation in this application
1 Suitable programming language	C.4.6	HR	Usually ladder, and often the proprietary variety of the PLC supplier
2 Strongly typed programming language	C.4.1	HR	IEC 61131-3 structured text
3 Language subset	C.4.2	---	Beware of complex "macro" instructions, interrupts which alter PLC scan cycle, etc.
4a Certified tools	C.4.3	HR	Available from some PLC manufacturers
4b Tools: increased confidence from use	C.4.4	HR	PLC supplier's development kit; in-house tools developed over several projects
5a Certified translator	C.4.3	HR	Available from some PLC manufacturers
5b Translator: increased confidence from use	C.4.4	HR	Not used for limited variability programming
6 Library of trusted/verified software modules and components	C.4.5	HR	Function blocks, part programs

Tableau E.4 – Conception et réalisation 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 comprenant, par exemple, JSD, MASCOT, SADT et Yourdon	C.2.1	HR	Non utilisées pour la programmation à variabilité limitée
1b Méthodes semi-formelles	Tableau B.7	HR	Diagrammes cause-conséquence, diagrammes de séquence, blocs fonctionnels. Typique des langages de variabilité limités
1c Méthodes formelles comprenant, par exemple, CCS, CSP, HOL, LOTOS, OBJ, logique temporelle, VDM et Z	C.2.4	R	Pas utilisées pour la programmation en langage de 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 langage à contact pour augmenter sa modularité par rapport aux fonctions requises
5 Règles de conception et de codage	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 modules logiciels et composants éprouvés/ vérifiés (si disponibles)	C.4.5	HR	Utilisée

Tableau E.5 – Conception et réalisation du logiciel: test des modules logiciels et intégration (voir 7.4.7 et 7.4.8 de la CEI 61508-3)

Technique/mesure	Réf.	SIL2	Interprétation pour cette application
1 Test probabiliste	C.5.1	R	Pas utilisé pour la programmation en langage de variabilité limitée
2 Analyse dynamique et test	B.6.5 Tableau B.2	HR	Utilisé
3 Enregistrement et analyse de données	C.5.2	HR	Enregistrement des cas de test et des résultats
4 Tests fonctionnel 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 de test issus de diagrammes cause-conséquence, d'analyse des valeurs limites, et du partitionnement des entrées
5 Modélisation du fonctionnement	C.5.20 Tableau B.6	R	Pas utilisé pour la programmation en langage de variabilité limitée
6 Test d'interface	C.5.3	R	Inclus dans le test fonctionnel et boîte noire

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 Tests fonctionnel 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 de test issus de diagrammes cause-conséquence, d'analyse des valeurs limites, et du partitionnement des entrées
2 Modélisation du fonctionnement	C.5.20 Tableau B.6	R	Au moment de l'assemblage du système PLC pour le test d'acceptation en usine

Table E.4 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3)
(this includes software system design, software module design and coding)

Technique/measure	Ref	SIL2	Interpretation in this application
1a Structured methods including for example, JSD, MASCOT, SADT and Yourdon	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 methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	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	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 modules and components (if available)	C.4.5	HR	Used

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	SIL2	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 modelling	C.5.20 Table B.6	R	Not used for limited variability programming
6 Interface testing	C.5.3	R	Included in functional and black-box testing

Table E.6 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3)

Technique/measure	Ref	SIL2	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	C.5.20 Table B.6	R	When the PLC system is assembled for factory acceptance test

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 Test probabiliste	C.5.1	R	Pas utilisé pour la programmation en langage de variabilité limitée
2 Simulation/modélisation	Tableau B.5	R	Pas utilisée pour la programmation en langage de variabilité limitée, mais de plus en plus communément utilisé dans le développement des systèmes PLC
3 Tests fonctionnel 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 de test issus de diagrammes cause-conséquence, d'analyse des valeurs limites, et du partitionnement des entrées

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 d'un module logiciel modifié	C.5.23	HR	Répéter les tests déjà faits
3 Revérification des modules logiciels affectés	C.5.23	HR	Répéter les tests déjà faits
4 Revalidation du système complet	C.5.23	R	L'analyse d'impact a montré que la modification est nécessaire. La revalidation est donc effectuée selon les prescriptions
5 Gestion de configuration logicielle	C.5.24	HR	Référentiels, enregistrement des changements, impact sur d'autres prescriptions système
6 Enregistrement et analyse de données	C.5.2	HR	Enregistrement des cas de test et résultats

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.5.13	R	Pas utilisée pour la programmation en langage de variabilité limitée
2 Test probabiliste	C.5.1	R	Remplacé par l'expérience en exploitation des composants existants
3 Analyse statique	B.6.4 Tableau B.8	HR	Références croisées écrites de l'utilisation des variables, conditions, etc
4 Analyse dynamique et test	B.6.5 Tableau B.2	HR	Banc de test automatique pour faciliter les tests de non-régression
5 Métriques de complexité du logiciel	C.5.14	R	Pas utilisées pour la programmation en langage de variabilité limitée
Test des modules logiciels et intégration	Voir tableau E.5		
Test d'intégration de l'électronique programmable	Voir tableau E.6		
Test du système logiciel (validation)	Voir tableau E.7		

Table E.7 – Software safety validation (see 7.7 of IEC 61508-3)

Technique/measure	Ref	SIL2	Interpretation in this application
1 Probabilistic testing	C.5.1	R	Not used for limited variability programming
2 Simulation/modelling	Table B.5	R	Not used for limited variability programming, but becoming more commonly used in PLC systems development
3 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

Table E.8 – Software modification (see 7.8 of IEC 61508-3)

Technique/measure	Ref	SIL2	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
4 Revalidate complete system	C.5.23	R	Impact analysis showed that the modification is necessary, so revalidation is done as required
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

Table E.9 – Software verification (see 7.9 of part 3)

Technique/measure	Ref	SIL2	Interpretation in this application
1 Formal proof	C.5.13	R	Not used for limited variability programming
2 Probabilistic testing	C.5.1	R	Replaced by operating experience of existing parts
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 Software complexity metrics	C.5.14	R	Not used for limited variability programming
Software module testing and integration	See table E.5		
Programmable electronics integration testing	See table E.6		
Software system testing (validation)	See table E.7		

Tableau E.10 – Evaluation de la sécurité fonctionnelle (voir article 8 de la CEI 61508-3)

	Technique/mesure	Réf.	SIL2	Interprétation pour cette application
1	Liste de contrôle	B.2.5	R	Utilisé
2	Tables de décision/de vérité	C.6.1	R	Utilisé à un degré limité
3	Métriques de complexité du logiciel	C.5.14	R	Pas utilisées pour la programmation en langage de variabilité limitée
4	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 en langage de variabilité limitée
5	Analyse des défaillances de cause commune d'un logiciel diversifié (si du logiciel diversifié est effectivement utilisé)	C.6.3	R	Pas utilisée pour la programmation en langage de variabilité limitée
6	Diagramme de blocs de fiabilité	C.6.5	R	Pas utilisé pour la programmation en langage de variabilité limitée

E.3 Exemple pour le niveau 3 d'intégrité de sécurité

Le système logiciel est relativement gros pour un système de sécurité: plus de 30 000 lignes de code source ont été développées spécifiquement pour le système; des fonctions intrinsèques usuelles sont également utilisées: au moins deux systèmes d'exploitation différents et du code préexistant de projets antérieurs (validé en utilisation). Au total, le système ainsi conçu correspond à plus de 100 000 lignes de code source.

L'ensemble du matériel (y compris les capteurs et actionneurs) correspond à un système double canal avec ses sorties vers les éléments finals 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, leur code objet est généré par des traducteurs différents;
– le logiciel s'exécute sur plusieurs processeurs disponibles dans le commerce qui remplissent les prescriptions de la CEI 61508-2;
– toutes les prescriptions pour maîtriser et éviter les pannes matérielles conformément à la CEI 61508-2 sont respectées par le système embarqué; et
– le développement logiciel a été évalué par une organisation indépendante.

NOTE 1 Pour la définition d'une organisation indépendante, voir 3.8.12 de la CEI 61508-4.

Les tableaux suivants montrent comment les tableaux des annexes de la CEI 61508-3 peuvent être interprétés pour cette application.

NOTE 2 Dans les colonnes de références (intitulées Réf.) des tableaux suivants, les paragraphes techniques/mesures (par exemple, B.2.4, C.3.1) se réfèrent à la CEI 61508-7 et les tableaux (par exemple tableau B.7) se réfèrent à la CEI 61508-3.

Table E.10 – Functional safety assessment (see clause 8 of IEC 61508-3)

Technique/measure		Ref	SIL2	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	Software complexity metrics	C.5.14	R	Not used for limited variability programming
4	Failure analysis	Table B.4	R	Cause-consequence diagrams at system level, but otherwise, failure analysis is not used for limited variability programming
5	Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3	R	Not used for limited variability programming
6	Reliability block diagram	C.6.5	R	Not used for limited variability programming

E.3 Example for 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 1 For the definition of an independent organization, see 3.8.12 of IEC 61508-4.

The following tables show how the annex tables of IEC 61508-3 may be interpreted for this application.

NOTE 2 In the reference columns (entitled Ref) of the following tables, the technique/measure subclauses (e.g. B.2.4, C.3.1) refer to IEC 61508-7 and the tables (e.g. table B.7) refer to IEC 61508-3.

Tableau E.11 – Spécification des prescriptions de sécurité du logiciel (voir 7.2 de la CEI 61508-3)

Technique/mesure	Réf.	SIL3	Interprétation pour cette application
1 Outils de spécification assistée par ordinateur	B.2.4	HR	Outils supportant les méthodes choisies
2a Méthodes semi-formelles	Tableau B.7	HR	Blocs diagrammes, diagrammes de séquence, diagrammes de changement d'état
2b Méthodes formelles comprenant, par exemple, CCS, CSP, HOL, LOTOS, OBJ, logique temporelle, VDM et Z	C.2.4	R	Seulement exceptionnellement

Tableau E.12 – Conception et réalisation 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 d'anomalie et diagnostic	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 prescriptions de la CEI 61508-2
2 Code de détection et correction d'erreurs	C.3.2	R	Seulement pour les transmissions de données externes
3a Programmation par assertion des défaillances	C.3.3	R	La validité des résultats des fonctions d'application sont contrôlés
3b Techniques à base de dispositif externe de sécurité	C.3.4	R	Utilisées pour certaines fonctions relatives à la sécurité quand 3a et 3c ne sont pas utilisés
3c Programmation diversifiée	C.3.5	R	Utilisée pour certaines fonctions quand le code source n'est pas disponible
3d Bloc de récupération	C.3.6	R	Pas utilisé
3e Récupération arrière	C.3.7	R	Pas utilisé
3f Récupération avant	C.3.8	R	Pas utilisé
3g Mécanismes de récupération d'anomalie par relance	C.3.9	R	Pas utilisé
3h Mémorisation de cas d'exécution	C.3.10	R	Pas utilisé (les mesures 3a, 3b et 3c sont suffisantes)
4 Dégradation «élégante»	C.3.11	HR	Oui, à cause de la nature du processus technique
5 Intelligence artificielle - correction d'anomalie	C.3.12	NR	Pas utilisé
6 Reconfiguration dynamique	C.3.13	NR	Pas utilisé
7a Méthodes structurées comprenant, par exemple, JSD, MASCOT, SADT et Yourdon.	C.2.1	HR	Nécessaire à cause de la taille du système
7b Méthodes semi-formelles	Tableau B.7	HR	Blocs diagrammes, diagrammes de séquence, diagrammes de changement d'état
7c Méthodes formelles comprenant, par exemple, CCS, CSP, HOL, LOTOS, OBJ, logique temporelle, VDM et Z	C.2.4	R	Pas utilisé
8 Outils de spécification assistée par ordinateur	B.2.4	HR	Outils supportant la méthode choisie

Table E.11 – Software safety requirements specification (see 7.2 of IEC 61508-3)

	Technique/measure	Ref	SIL3	Interpretation in this application
1	Computer-aided specification tools	B.2.4	HR	Tools supporting the chosen methods
2a	Semi-formal methods	Table B.7	HR	Block diagrams, sequence diagrams, state transition diagrams
2b	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	R	Only exceptionally

Table E.12 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3)

	Technique/measure	Ref	SIL3	Interpretation in this application
1	Fault detection and diagnosis	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 and correcting 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	Safety bag techniques	C.3.4	R	Used for some safety related functions where 3a and 3c are not used
3c	Diverse programming	C.3.5	R	Used for some functions where source code is not available
3d	Recovery block	C.3.6	R	Not used
3e	Backward recovery	C.3.7	R	Not used
3f	Forward recovery	C.3.8	R	Not used
3g	Re-try fault recovery mechanisms	C.3.9	R	Not used
3h	Memorizing executed cases	C.3.10	R	Not used (measures 3a, 3b and 3c are sufficient)
4	Graceful degradation	C.3.11	HR	Yes, because of the nature of the technical process
5	Artificial intelligence - fault correction	C.3.12	NR	Not used
6	Dynamic reconfiguration	C.3.13	NR	Not used
7a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon.	C.2.1	HR	Needed because of the size of the system
7b	Semi-formal methods	Table B.7	HR	Block diagrams, sequence diagrams, state transition diagrams
7c	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	R	Not used
8	Computer-aided specification tools	B.2.4	HR	Tools supporting the chosen method

Tableau E.13 – Conception et réalisation du logiciel: outils supports et langages de programmation (voir 7.4.4 de la CEI 61508-3)

Technique/mesure	Réf.	SIL3	Interprétation pour cette application
1 Langage de programmation adéquat	C.4.6	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 certifiés	C.4.3	HR	Pas disponibles
4b Outils dans lesquels on a une confiance accrue résultant de l'utilisation	C.4.4	HR	Disponibles et utilisés
5a Traducteur certifié	C.4.3	HR	Pas disponible
5b Traducteur: confiance accrue résultant de l'utilisation	C.4.4	HR	Disponible et utilisé
6 Bibliothèque de modules logiciels et composants éprouvés/vérifiés	C.4.5	HR	Disponibles et utilisés

Tableau E.14 – Conception et réalisation 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 comprenant, par exemple, JSD, MASCOT, SADT et Yourdon	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 changement d'état, blocs diagrammes, diagrammes de séquence
1c Méthodes formelles comprenant, par exemple, CCS, CSP, HOL, LOTOS, OBJ, logique temporelle, VDM et Z	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 celle 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	Tableau B.1	HR	Utilisation de standard 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 modules logiciels et composants éprouvés/ vérifiés (si disponibles)	C.4.5	HR	Disponible et utilisée

Table E.13 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3)

	Technique/measure	Ref	SIL3	Interpretation in this application
1	Suitable programming language	C.4.6	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	C.4.3	HR	Not available
4b	Tools: increased confidence from use	C.4.4	HR	Available, and used
5a	Certified translator	C.4.3	HR	Not available
5b	Translator: increased confidence from use	C.4.4	HR	Available, and used
6	Library of trusted/verified software modules and components	C.4.5	HR	Available, and used

Table E.14 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3)
(this includes software system design, software module design and coding)

	Technique/measure	Ref	SIL3	Interpretation in this application
1a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon	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 methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	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	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 modules and components (if available)	C.4.5	HR	Available, and used

Tableau E.15 – Conception et réalisation du logiciel: test des modules logiciels et intégration (voir 7.4.7 et 7.4.8 de la CEI 61508-3)

Technique/mesure	Réf.	SIL3	Interprétation pour cette application
1 Test 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 de test est difficile
2 Analyse dynamique et test	B.6.5 Tableau B.2	HR	Utilisé pour les modules logiciels lorsque le code source est disponible Cas de tests à partir de l'analyse de valeurs limites, modélisation du fonctionnement, classes d'équivalence et partitionnement des entrées, test structuré
3 Enregistrement et analyse de données	C.5.2	HR	Enregistrement des cas des tests et des résultats
4 Tests fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Utilisé pour les modules logiciels lorsque le code source n'est pas disponible et pour le test 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 causes-conséquences, le prototypage, l'analyse des valeurs limites, les classes d'équivalence et le partitionnement des entrées
5 Modélisation du fonctionnement	C.5.20 Tableau B.6	HR	Utilisé lors des tests d'intégration sur le matériel cible
6 Test d'interface	C.5.3	HR	Pas utilisé

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 Tests fonctionnels et boîte noire	B.5.1 B.5.2 Tableau B.3	HR	Utilisé en tant que tests supplémentaires aux tests d'intégration du logiciel (voir tableau E.15). 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 causes-conséquences, le prototypage, l'analyse des valeurs limites, les classes d'équivalence et le partitionnement des entrées
2 Modélisation du fonctionnement	C.5.20 Tableau B.6	HR	Largement utilisé

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 Test probabiliste	C.5.1	R	Pas utilisé pour la validation
2 Simulation/modélisation	Tableau B.5	HR	Machines à états finis, modélisation du fonctionnement, prototypage et animation
3 Tests 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 causes-conséquences, l'analyse des valeurs limites et le partitionnement des entrées

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	SIL3	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
5 Performance modelling	C.5.20 Table B.6	HR	Used during integration testing on the target hardware
6 Interface testing	C.5.3	HR	Not used

Table E.16 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3)

Technique/measure	Ref	SIL3	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) 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 modelling	C.5.20 Table B.6	HR	Extensively used

Table E.17 – Software safety validation (see 7.7 of IEC 61508-3)

Technique/measure	Ref	SIL3	Interpretation in this application
1 Probabilistic testing	C.5.1	R	Not used for validation
2 Simulation/modelling	Table B.5	HR	Finite state machines, performance modelling, prototyping and animation
3 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

Tableau E.18 – Modification (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 d'un module logiciel modifié	C.5.23	HR	Utilisé
3 Revérification des modules logiciels affectés	C.5.23	HR	Utilisé
4 Revalidation du système complet	C.5.23	HR	Dépend des résultats de l'analyse d'impact.
5 Gestion de configuration logicielle	C.5.24	HR	Utilisé
6 Enregistrement et analyse de données	C.5.2	HR	Utilisé

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.5.13	R	Exceptionnellement seulement, pour des cas très élémentaires
2 Test probabiliste	C.5.1	R	Inclus dans le tableau E.15
3 Analyse statique	B.6.4 Tableau B.8	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 test	B.6.5 Tableau B.2	HR	Inclus dans le tableau E.15
5 Métriques de complexité du logiciel	C.5.14	R	Utilisé seulement de façon marginale
Test des modules logiciels et intégration	Voir tableau E.15		
Test d'intégration de l'électronique programmable	Voir tableau E.16		
Test du système logiciel (validation)	Voir tableau E.17		

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 Liste de contrôle	B.2.5	R	Utilisé
2 Tables de décision/de vérité	C.6.1	R	Utilisé, dans certaines limites
3 Métriques de complexité du logiciel	C.5.14	R	Utilisé seulement de façon marginale
4 Analyse des défaillances	Tableau B.4	HR	L'analyse par arbre de pannes est largement utilisée, et les diagrammes causes-conséquences sont utilisés dans certaines limites
5 Analyse des défaillances de cause commune d'un logiciel diversifié (si du logiciel diversifié est effectivement utilisé)	C.6.3	HR	Utilisé
6 Diagramme de blocs de fiabilité	C.6.5	R	Utilisé

Table E.18 – Modification (see 7.8 of IEC 61508-3)

Technique/measure	Ref	SIL3	Interpretation in this application
1 Impact analysis	C.5.23	HR	Used
2 Re-verify changed software module	C.5.23	HR	Used
3 Re-verify affected software modules	C.5.23	HR	Used
4 Revalidate complete system	C.5.23	HR	Depends on the result of the impact analysis
5 Software configuration management	C.5.24	HR	Used
6 Data recording and analysis	C.5.2	HR	Used

Table E.19 – Software verification (see 7.9 of IEC 61508-3)

Technique/measure	Ref	SIL3	Interpretation in this application
1 Formal proof	C.5.13	R	Only exceptionally, for some very basic classes only
2 Probabilistic testing	C.5.1	R	Included in table E.15
3 Static analysis	B.6.4 Table B.8	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	Included in table E.15
5 Software complexity metrics	C.5.14	R	Used only marginally
Software module testing and integration	See table E.15		
Programmable electronics integration testing	See table E.16		
Software system testing (validation)	See table E.17		

Table E.20 – Functional safety assessment (see clause 8 of IEC 61508-3)

Assessment/technique	Ref	SIL3	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 Software complexity metrics	C.5.14	R	Used only marginally
4 Failure analysis	Table B.4	HR	Fault-tree analysis is extensively used, and cause consequence diagrams are used to a limited degree
5 Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3	HR	Used
6 Reliability block diagram	C.6.5	R	Used

Bibliographie

Les références suivantes fournissent des détails supplémentaires sur l'évaluation des probabilités de défaillance (voir annexe B).

[1] CEI 61078:1991, *Techniques d'analyse de la sûreté de fonctionnement – Méthode du diagramme de fiabilité*

[2] CEI 61165:1995, *Application des techniques de Markov*

[3] BS 5760, *Reliability of system equipment and components – Part 2: Guide to assessment of reliability*

[4] D. J. Smith, *Reliability, maintainability and risk – Practical methods for engineers,* Butterworth-Heinemann, 5th edition, 1997, ISBN 0-7506-3752-8

[5] R. Billington and R. N. Allan, *Reliability evaluation of engineering systems,* Plenum, 1992, ISBN 0-306-44063-6

[6] W. M. Goble, *Evaluating control system reliability – Techniques and applications,* Instrument Society of America, 1992, ISBN 1-55617-128-5

Les références suivantes sont utiles pour le calcul de la couverture de diagnostic (voir annexe C).

[7] *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

[8] *Qualität und Zuverlassigkeit technischer Systeme, Theorie, Praxis, Management,* Dritte Auflage,1991, Allessandro Birolini, Springer-Verlag, Berlin Heidelberg New York, ISBN 3-540-54067-9, 3 Aufl., ISBN 0-387-54067-9 3 ed.

[9] MIL-HDBK-217F, *Military Handbook Reliability prediction of electronic equipment,* 2 December 1991, Department of Defense, United States of America, Washington DC 20301.

Les références suivantes donnent des informations utiles en ce qui concerne les défaillances de cause commune (voir annexe D).

[10] *Programmable electronic systems in safety-related applications, Part 2: General technical guidelines, Health and Safety Executive,* HMSO, ISBN 0 11 883906 3, 1987.

[11] *Assigning a numerical value to the beta factor common-cause evaluation,* Humphreys, R. A., Proc. Reliability '87.

[12] UPM3.1: *A pragmatic approach to dependent failures assessment for standard systems,* AEA Technology, Report SRDA-R-13, ISBN 085 356 4337, 1996.

Il est fait référence à la norme suivante dans le tableau E.3.

[13] CEI 61131-3:1993, *Automates programmables – Partie 3: Langages de programmation*

Il est fait référence à la norme suivante en 1.3, note.

[14] ANSI/ISA S84.01:1996, *Application of safety instrumented systems for the process industries*.

Bibliography

The following references give further details on evaluating probabilities of failure (see annex B).

[1] IEC 61078:1991, *Analysis techniques for dependability – Reliability block diagram method*

[2] IEC 61165:1995, *Application of Markov techniques*

[3] BS 5760, *Reliability of system equipment and components – Part 2: Guide to assessment of reliability*

[4] D. J. Smith, *Reliability, maintainability and risk – Practical methods for engineers*, Butterworth-Heinemann, 5th edition, 1997, ISBN 0-7506-3752-8

[5] R. Billington and R. N. Allan, *Reliability evaluation of engineering systems*, Plenum, 1992, ISBN 0-306-44063-6

[6] 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.

[7] *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

[8] *Qualität und Zuverlassigkeit technischer Systeme, Theorie, Praxis, Management*, Dritte Auflage,1991, Allessandro Birolini, Springer-Verlag, Berlin Heidelberg New York, ISBN 3-540-54067-9, 3 Aufl., ISBN 0-387-54067-9 3 ed.

[9] MIL-HDBK-217F, *Military Handbook Reliability prediction of electronic equipment*, 2 December 1991, Department of Defense, United States of America, Washington DC 20301.

The following references provide useful information relating to common cause failures (see annex D).

[10] *Programmable electronic systems in safety-related applications, Part 2: General technical guidelines, Health and Safety Executive*, HMSO, ISBN 0 11 883906 3, 1987.

[11] *Assigning a numerical value to the beta factor common-cause evaluation*, Humphreys, R. A., Proc. Reliability '87.

[12] 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.

[13] IEC 61131-3:1993, *Programmable controllers – Part 3: Programming languages*

The following standard is referred to in 1.3, note.

[14] ANSI/ISA S84.01:1996, *Application of safety instrumented systems for the process industries.*

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-5211-0

ICS 25.040.40

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND