# IEC 61800-5-2

Edition 1.0 2007-07

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

## Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional

## Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle



IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

## About the IEC

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

## About IEC publications

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

**Useful links:**

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

## A propos de la CEI

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

## A propos des publications CEI

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

**Liens utiles:**

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

# IEC 61800-5-2

Edition 1.0 2007-07

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside



## Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional

## Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 13.110; 29.200

ISBN 978-2-83220-595-2

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

## Part 5-2: Safety requirements – Functional

## FOREWORD

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

International Standard IEC 61800-5-2 has been prepared by subcommittee 22G: Adjustable speed electric drive systems incorporating semiconductor power converters, of IEC technical committee 22: Power electronic systems and equipment.

This bilingual version (2013-01) corresponds to the monolingual English version, published in 2007-07.

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

| FDIS | Report on voting |
|---|---|
| 22G/179/FDIS | 22G/182/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.

The French version of this standard has not been voted upon.

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

A list of all parts of the IEC 61800 series, published under the general title *Adjustable speed electric drive systems*, can be found on the IEC website.

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

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

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

# INTRODUCTION

As a result of automation, demand for increased production and reduced operator physical effort, control systems of machinery and plant items play an increasing role in the achievement of overall safety. These control systems increasingly employ complex electrical/ electronic/programmable electronic devices and systems.

Prominent amongst these devices and systems are adjustable speed electrical power drive systems (PDS) that are suitable for use in safety-related applications (PDS(SR)).

Examples of industrial applications are:

- machine tools, robots, production test equipment, test benches;
- papermaking machines, textile production machines, calendars in the rubber industry;
- process lines in plastics, chemicals or metal production, rolling-mills;
- cement crushing machines, cement kilns, mixers, centrifuges, extrusion machines;
- drilling machines;
- conveyors, materials handling machines, hoisting equipment (cranes, gantries, etc);
- pumps, fans, etc.

This standard can also be used as a reference for developers using PDS(SR) for other applications.

Users of this standard should be aware that some type C standards for machinery currently refer to ISO 13849-1 for safety-related control systems. In this case, PDS(SR) manufacturers may be requested to provide further information (e.g. category and/or performance level) to facilitate the integration of a PDS(SR) into the safety-related control systems of such machinery.

NOTE "Type C standards" are defined in ISO 12100-1 as machine safety standards dealing with detailed safety requirements for a particular machine or group of machines.

Previously, in the absence of standards, there has been a reluctance to accept electronic, and in particular programmable electronic, devices and systems in safety-related functions because of uncertainty regarding the safety performance of such technology.

There are many situations where control systems that incorporate a PDS(SR) are employed, for example as part of safety measures that have been provided to achieve risk reduction. A typical case is guard interlocking in order to exclude personnel from hazards where access to the danger zone is only possible when rotating parts have attained a safe condition. This part of IEC 61800 gives a methodology to identify the contribution made by a PDS(SR) to identified safety functions and to enable the appropriate design of the PDS(SR) and verification that it meets the required performance.

Measures are given to co-ordinate the safety performance of the PDS(SR) with the intended risk reduction taking into account the probabilities and consequences of its random and systematic faults.

# ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

## Part 5-2: Safety requirements – Functional

## 1 Scope and object

This part of IEC 61800 specifies requirements and makes recommendations for the design and development, integration and validation of PDS(SR)s in terms of their functional safety considerations. It applies to adjustable speed electric drive systems covered by the other parts of the IEC 61800 series of standards.

NOTE 1 The term "integration" refers to the PDS(SR) itself, not to its incorporation into the safety-related application.

This International Standard is only applicable where functional safety of a PDS(SR) is claimed and the PDS(SR) is operating in the high demand or continuous mode (see 3.10). For low demand applications, see IEC 61508.

This part of IEC 61800, which is a product standard, sets out safety-related considerations of PDS(SR)s in terms of the framework of IEC 61508, and introduces requirements for PDS(SR)s as subsystems of a safety-related system. It is intended to facilitate the realisation of the electrical/electronic/ programmable electronic (E/E/PE) elements of a PDS(SR) in relation to the safety performance of safety function(s) of a PDS.

Manufacturers and suppliers of PDS(SR)s by using the normative requirements of this part of IEC 61800 will indicate to users (control system integrators, machinery and plant designers, etc.) the safety performance for their equipment. This will facilitate the incorporation of a PDS(SR) into a safety-related control system using the principles of IEC 61508, and possibly its specific sector implementations (for example IEC 61511, IEC 61513, IEC 62061) or ISO 13849.

Conformity with this part of IEC 61800 fulfils all the requirements of IEC 61508 that are necessary for a PDS(SR).

This part of IEC 61800 does not specify requirements for:

- the hazard and risk analysis of a particular application;
- the identification of safety functions for that application;
- the initial allocation of SILs to those safety functions;
- the driven equipment except for interface arrangements;
- secondary hazards (for example from failure in a production or manufacturing process);
- the electrical, thermal and energy safety considerations, which are covered in IEC 61800-5-1;
- the PDS(SR) manufacturing process;
- the validity of signals and commands to the PDS(SR).

NOTE 2 The functional safety requirements of a PDS(SR) are dependent on the application, and must be considered as a part of the overall risk assessment of the installation. Where the supplier of the PDS(SR) is not also responsible for the driven equipment, the installation designer is responsible for the risk assessment, and for specifying the functional and safety integrity requirements of the PDS(SR).

NOTE 3 Even though malevolent actions can influence the functional safety of PDS(SR), security aspects are not considered in this standard.

This part of IEC 61800 only applies to PDS(SR)s implementing safety functions with a SIL not greater than SIL 3.

Figure 1 shows the functional elements of a PDS(SR) that are considered in this part of IEC 61800.

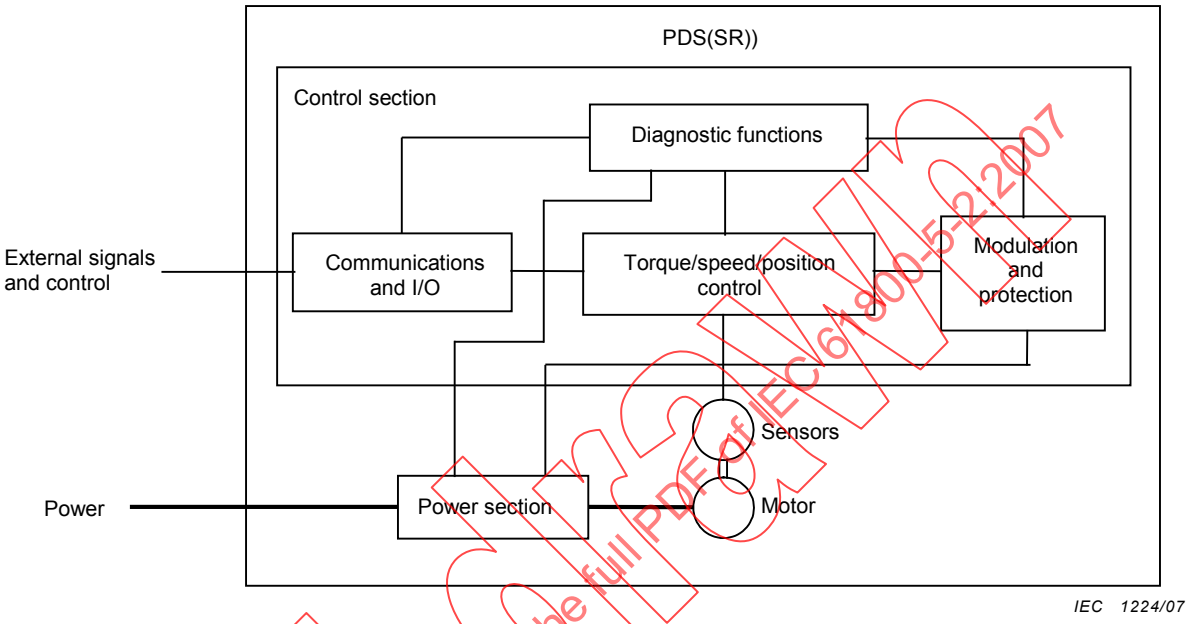



**Figure 1 – Functional elements of a PDS(SR)**

NOTE Figure 1 shows a logical representation of a PDS(SR) rather than its physical description.

## 2 Normative references

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

NOTE 1 This does not mean that compliance is required with all clauses of the referenced documents, but rather that this document makes a reference that cannot be understood in the absence of the referenced documents.

NOTE 2 References to various parts of IEC 61508 are undated, except where specific clauses are indicated.

IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

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

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

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

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

IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

IEC 61800-1, *Adjustable speed electrical power drive systems – Part 1: General requirements – Rating specifications for low voltage adjustable speed d.c. power drive systems*

IEC 61800-2, *Adjustable speed electrical power drive systems – Part 2: General requirements – Rating specifications for low voltage adjustable frequency a.c. power drive systems*

IEC 61800-3, *Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods*

IEC 61800-4, *Adjustable speed electrical power drive systems – Part 4: General requirements – Rating specifications for a.c. power drive systems above 1 000 V a.c. and not exceeding 35 kV*

IEC 61800-5-1:2003, *Adjustable speed electrical power drive systems – Part 5-1: Safety requirements – Electrical, thermal and energy*

IEC 62280 (all parts), *Railway applications – Communication, signalling and processing systems*

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE 1 For an alphabetical list of definitions, see Table 1.

**Table 1 – Alphabetical list of definitions**

| Term | Definition number | Term | Definition number |
|---|---|---|---|
| common cause failure | 3.1 | safe failure | 3.14 |
| dangerous failure | 3.2 | safe failure fraction (SFF) | 3.15 |
| diagnostic coverage (DC) | 3.3 | safety function(s) (of a PDS(SR)) | 3.16 |
| diagnostic test(s) | 3.4 | safety integrity | 3.17 |
| fault reaction function | 3.5 | safety integrity level (SIL) | 3.18 |
| functional safety | 3.6 | safety-related system | 3.19 |
| hazard | 3.7 | safety requirements specification (SRS) | 3.20 |
| installation | 3.8 | SIL capability | 3.21 |
| mission time | 3.9 | subsystem | 3.22 |
| mode of operation | 3.10 | systematic failure | 3.23 |
| PDS(SR) | 3.11 | systematic safety integrity | 3.24 |
| PFH | 3.12 | validation | 3.25 |
| proof test | 3.13 | verification | 3.26 |

NOTE 2 Throughout this international standard, references to the following definitions are identified by writing them in *italic* script.

**3.1**
**common cause failure**
failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to failure of the *safety function*

[IEC 61508-4:1998; definition 3.6.10]

**3.2**
**dangerous failure**
failure which has the potential to put the *safety-related system* in a hazardous or fail-to-function state

[IEC 61508-4:1998; definition 3.6.7]

**3.3**
**diagnostic coverage**
**DC**
fractional decrease in the probability of dangerous hardware failures resulting from the operation of the automatic *diagnostic tests*

[IEC 61508-4:1998; definition 3.8.6]

NOTE 1 This can also be expressed as the ratio of the sum of the detected *dangerous failure* rates $\lambda_{DD}$ to the sum of the total *dangerous failure* rates $\lambda_D$: $DC = \Sigma\lambda_{DD}/\Sigma\lambda_D$.

NOTE 2 *Diagnostic coverage* may exist for the whole or parts of a *safety-related system*. For example, *diagnostic coverage* may exist for sensors and/or logic system and/or final elements.

**3.4**
**diagnostic test(s)**
test(s) intended to detect faults or failures and produce a specified output information or activity when a fault or failure is detected

**3.5**
**fault reaction function**
function that is initiated when a fault or failure within the PDS(SR), which could cause a loss of the safety function, is detected, and which is intended to maintain the safe condition of the installation or prevent hazardous conditions arising at the installation

**3.6**
**functional safety**
part of the overall safety relating to the EUC (equipment under control) and the EUC control system which depends on the correct functioning of the E/E/PE (electrical/electronic/ programmable electronic) safety-related systems, other technology safety-related systems and external risk reduction facilities

[IEC 61508-4:1998; definition 3.1.9]

NOTE This standard only considers those aspects in the definition of functional safety that depend on the correct functioning of the PDS(SR).

**3.7**
**hazard**
potential source of harm

[ISO/IEC Guide 51:1999, definition 3.5]

NOTE 1 The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

NOTE 2 IEC 61508-4:1998 (modified) defines **hazardous situation** as: circumstance in which people, property or the environment are exposed to one or more hazards or hazardous events.

**3.8**
**installation**
equipment or equipments including at least the PDS(SR) and the driven equipment

NOTE The word "installation" is also used in this international standard to denote the process of installing a PDS(SR). In these cases, the word does not appear in italics.

**3.9**
**mission time**
specified cumulative operating time of the PDS(SR) during its overall lifetime

**3.10**
**mode of operation**
way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it

[IEC 61508-4:1998; definition 3.5.12, modified]

NOTE 1 Two modes of operation are considered in IEC 61508:

- **low demand mode:** where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency;

- **high demand or continuous mode:** where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-test frequency.

The low demand mode of operation is not generally considered to be relevant for PDS(SR) applications. Therefore, in this standard, PDS(SR)s are only considered to operate in the high demand or continuous mode.

NOTE 2 Demand mode means that a safety function is only performed on request (demand) in order to transfer the installation into a specified state.

NOTE 3 Continuous mode means that a safety function is performed continuously, i.e. the PDS(SR) is continuously controlling the installation and a (dangerous) failure of its function can result in a hazard.

**3.11**
**PDS(SR)**
adjustable speed electrical power drive system suitable for use in safety-related applications

**3.12**
**PFH**
probability of a dangerous random hardware failure per hour

NOTE in IEC 62061:2005, the abbreviation $PFH_D$ is used.

**3.13**
**proof test**
periodic test performed to detect faults in a safety-related system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition

NOTE Proof tests are normally undertaken to reveal dangerous faults which are undetected by *diagnostic tests*. The effectiveness of the proof test will be dependent upon how close to the "as new" condition the system is restored. For the proof test to be fully effective, it will be necessary to detect 100 % of all dangerous faults. Although, in practice, 100 % is not easily achieved for other than low-complexity systems, this should be the target.

[IEC 61508-4:1998; definition 3.8.5, modified]

**3.14**
**safe failure**
failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state

(IEC 61508-4:1998; definition 3.6.8)

**3.15**
**safe failure fraction**
**SFF**
ratio of the average rate of safe failures plus detected *dangerous failures* of a PDS(SR) subsystem to the total average failure rate of that subsystem

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

NOTE See Annex C of IEC 61508-2:2000.

**3.16**
**safety function(s) (of a PDS(SR))**
function(s) with a specified safety performance, to be implemented in whole or in part by a PDS(SR), which is(are) intended to maintain the safe condition of the installation or prevent hazardous conditions arising at the installation

**3.17**
**safety integrity**
probability of a PDS(SR) satisfactorily performing a required safety function under all stated conditions

NOTE 1 The higher the level of safety integrity of the PDS(SR)(s), the lower the probability that the PDS(SR)(s) will fail to carry out the required safety function.

NOTE 2 The safety integrity may not be the same for each safety function performed by the PDS(SR).

(IEC 61508-4:1998; definition 3.5.2, modified)

**3.18**
**safety integrity level**
**SIL**
discrete level (one out of a possible four) for specifying the safety integrity requirements of a safety function allocated (in whole or in part) to a PDS(SR)

NOTE 1 SIL 4 has the highest level of safety integrity and SIL 1 has the lowest.

NOTE 2 SIL 4 is not considered in this standard as it is not relevant to the risk reduction requirements normally associated with PDS(SR)s. For requirements applicable to SIL 4, see IEC 61508.

(IEC 61508-4:1998; definition 3.5.6, modified)

**3.19**
**safety-related system**
designated system that both

– implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and

– is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

**3.20**
**safety requirements specification**
**SRS**
specification containing all the requirements of the safety functions that have to be performed by the PDS(SR)

**3.21**
**SIL capability**
maximum SIL that can be claimed to have been achieved by the design of a PDS(SR) in terms of the systematic safety integrity and the architectural constraints on hardware safety integrity

NOTE Each of the designated safety functions that a PDS(SR) is intended to perform can be associated with a different SIL capability.

**3.22**
**subsystem**
part of the top-level architectural design of a safety-related system, failure of which results in failure of a safety function

NOTE 1 A PDS(SR) can itself be a subsystem, or be made up from a number of separate subsystems, which when put together implement the safety function under consideration. A subsystem can have more than one channel.

NOTE 2 Examples of subsystems of a PDS(SR) are encoder, power section, control section (see Figure 1).

**3.23**
**systematic failure**
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE Examples of causes of systematic failures include human error in:

- the safety requirements specification;
- the design, manufacture, installation, operation of the hardware;
- the design, implementation of the software.

(IEC 61508-4:1998; definition 3.6.6)

**3.24**
**systematic safety integrity**
part of the safety integrity of safety-related systems relating to systematic failures in a dangerous mode of failure

(IEC 61508-4:1998; definition 3.5.4)

NOTE Systematic safety integrity cannot usually be quantified.

**3.25**
**validation**
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

(IEC 61508-4:1998; definition 3.8.2)

NOTE Validation is the activity of demonstrating that the PDS(SR), before or after installation, meets in all respects the safety requirements specification.

**3.26**
**verification**
confirmation by examination and provision of objective evidence that the requirements have been fulfilled

(IEC 61508-4:1998; definition 3.8.1)

## 4 Designated safety functions

### 4.1 General

This clause describes functions of a PDS(SR) that may be designated as safety-related by the PDS(SR) supplier. The designated safety functions in this clause are not considered to form an exhaustive list. In some cases, further safety-related systems external to the PDS(SR) (for example a mechanical brake) may be necessary to maintain the safe condition when electrical power is removed.

The technical measures required to implement these functions depend on the SIL capability and the required probability of dangerous hardware failure, as indicated in the safety requirements specification. The technical measures are described in Clause 6.

Each safety function may require safe input and/or output signalling in order to accomplish necessary communication with (or activation of) other functions, subsystems or systems (which may or may not be safety-related). The integrity of the interfaces shall be included in the determination of the SIL of the associated safety function.

Some of the safety functions perform monitoring tasks only, some perform a safety relevant control or other actions. Therefore, a distinction must be made between:

– the reaction on violation of limits (only relevant for monitoring functions):

  the reaction function when a violation of limits is detected during the correct operation of the safety function; and

– the fault reaction function:

  the reaction function when diagnostics detect a fault within the safety function.

Both reaction functions shall take into account the possible safe states for the application.

On selecting the appropriate reaction function, it has to be considered that parts of the PDS(SR) may not be functioning.

Timing requirements for the actions required following detection of a fault are specified in the safety requirements specification (see 5.4.2).

The names of the safety functions include the words “safe” or “safely” to indicate that these functions may be used in a safety-related application on the grounds of a judgement (i.e. risk

analysis) of that specific application, resulting in safety-relevant functions and their integrity to be performed by the PDS(SR).

## 4.2 Safety functions

### 4.2.1 Limit values

Where a safety function relies on limit value(s) for any parameter(s), the maximum tolerance(s) for the limit value(s) shall be defined.

NOTE Specification of any limit value should take into account possible exceeding of the limit value in case of violation of the limit. For example, specification of the position limit value(s) in 4.2.3.8 should take into account the maximum allowable overtravel distance(s).

A particular safety function may have one or more specified limit values, which can be selected during operation.

### 4.2.2 Stopping functions

#### 4.2.2.1 General

A variety of stopping methods is available for every type of PDS.

The control requirements for initiating the stopping sequence and maintaining a hold mode upon reaching standstill are application-specific. Separate manual operations and connections to control circuits may be necessary to achieve the desired performance of the stop functions.

Any particular requirements for stopping performance should be specified by the installation designer. The following examples of stop functions are often used in practice.

#### 4.2.2.2 Safe torque off (STO)

Power, that can cause rotation (or motion in the case of a linear motor), is not applied to the motor. The PDS(SR) will not provide energy to the motor which can generate torque (or force in the case of a linear motor).

NOTE 1 This safety function corresponds to an uncontrolled stop in accordance with stop category 0 of IEC 60204-1.

NOTE 2 This safety function may be used where power removal is required to prevent an unexpected start-up.

NOTE 3 In circumstances where external influences (for example, falling of suspended loads) are present, additional measures (for example, mechanical brakes) may be necessary to prevent any hazard.

NOTE 4 Electronic means and contactors are not adequate for protection against electric shock, and additional measures for isolation may be necessary.

#### 4.2.2.3 Safe stop 1 (SS1)

The PDS(SR) either

a) initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the STO function (see 4.2.2.2) when the motor speed is below a specified limit; or

b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit; or

c) initiates the motor deceleration and initiates the STO function after an application specific time delay.

NOTE This safety function corresponds to a controlled stop in accordance with stop category 1 of IEC 60204-1.

#### 4.2.2.4 Safe stop 2 (SS2)

The PDS(SR) either

a) initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function (see 4.2.3.1) when the motor speed is below a specified limit; or

b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit; or

c) initiates the motor deceleration and initiates the safe operating stop function after an application specific time delay.

NOTE This safety function corresponds to a controlled stop in accordance with stop category 2 of IEC 60204-1.

### 4.2.3 Other safety functions

#### 4.2.3.1 Safe operating stop (SOS)

The SOS function prevents the motor from deviating more than a defined amount from the stopped position. The PDS(SR) provides energy to the motor to enable it to resist external forces.

NOTE This description of an operational stop function is based on implementation by means of a PDS(SR) without external (for example mechanical) brakes.

#### 4.2.3.2 Safely-limited acceleration (SLA)

The SLA function prevents the motor from exceeding the specified acceleration limit.

#### 4.2.3.3 Safe acceleration range (SAR)

The SAR function keeps the motor acceleration and/or deceleration within specified limits.

#### 4.2.3.4 Safely-limited speed (SLS)

The SLS function prevents the motor from exceeding the specified speed limit.

#### 4.2.3.5 Safe speed range (SSR)

The SSR function keeps the motor speed within specified limits.

#### 4.2.3.6 Safely-limited torque (SLT)

The SLT function prevents the motor from exceeding the specified torque (or force, when a linear motor is used) limit.

#### 4.2.3.7 Safe torque range (STR)

The STR function keeps the motor torque (or force, when a linear motor is used) within the specified limits.

#### 4.2.3.8 Safely-limited position (SLP)

The SLP function prevents the motor shaft from exceeding the specified position limit(s).

#### 4.2.3.9 Safely-limited increment (SLI)

The SLI function prevents the motor shaft from exceeding the specified limit of position increment.

NOTE In this function, the PDS(SR) controls the incremental movements of a motor as follows.

- An input signal (for example start) initiates an incremental movement with a specified maximum travel.
- After completing the travel required for this increment, the motor is stopped and maintained in this state, as appropriate for the application.

#### 4.2.3.10 Safe direction (SDI)

The SDI function prevents the motor shaft from moving in the unintended direction.

#### 4.2.3.11 Safe motor temperature (SMT)

The SMT function prevents the motor temperature(s) from exceeding a specified upper limit(s).

#### 4.2.3.12 Safe brake control (SBC)

The SBC function provides a safe output signal(s) to control an external brake(s).

#### 4.2.3.13 Safe cam (SCA)

The SCA function provides a safe output signal to indicate whether the motor shaft position is within a specified range.

#### 4.2.3.14 Safe speed monitor (SSM)

The SSM function provides a safe output signal to indicate whether the motor speed is below a specified limit.

## 5 Management of functional safety

### 5.1 Objective

The objective of this clause is to identify the management activities and information that are necessary for the overall development process of the PDS(SR), in order to ensure that the functional safety objectives are met.

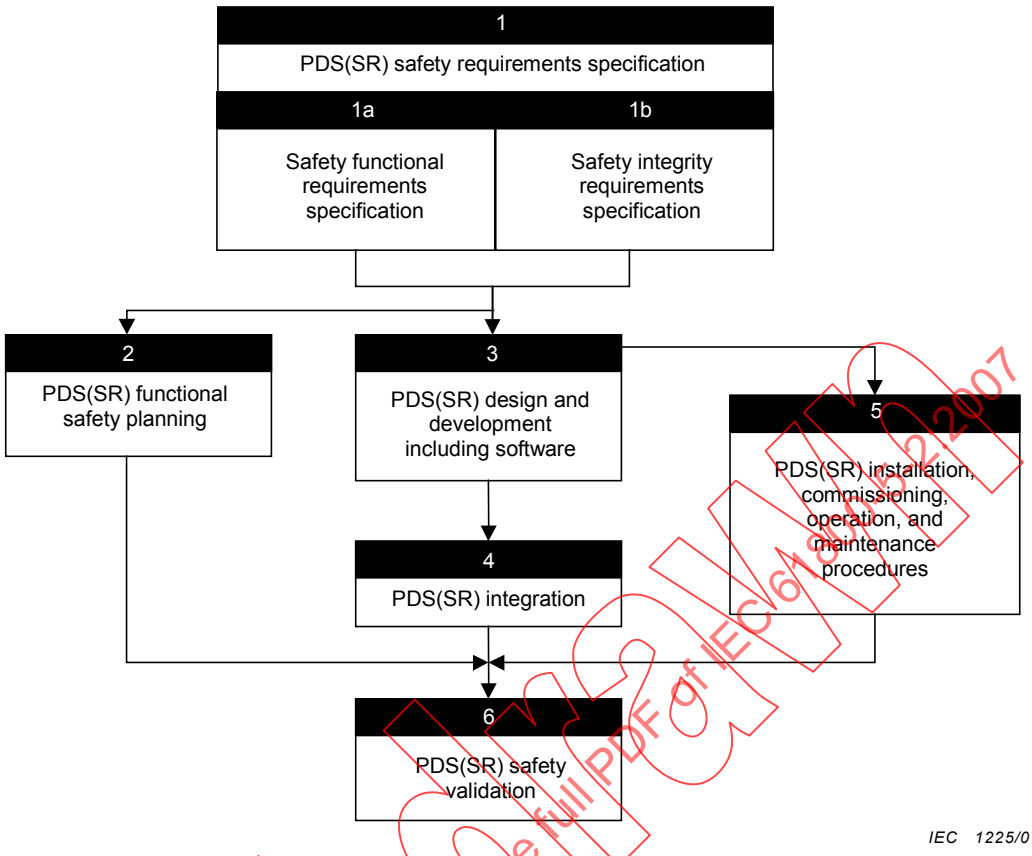
NOTE This clause is solely aimed at the achievement of the functional safety of the PDS(SR) and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

### 5.2 PDS(SR) development lifecycle

Figure 2 shows the PDS(SR) development lifecycle, with cross-references to the relevant subclauses of this standard.

NOTE This corresponds to the realisation phase (phase 9) of the overall safety lifecycle of IEC 61508-1.

Annex A shows this information in the form of a sequential task table.




| | | | |
|---|---|---|---|
| For phase 1, see 5.4. | For phase 1a, see 5.4.2. | For phase 1b, see 5.4.3. | For phase 2, see 5.3. |
| For phase 3, see Clause 6. | For phase 4, see 6.5. | For phase 5, see Clause 7. | For phase 6, see 8.3. |

**Figure 2 – PDS(SR) development lifecycle**

## 5.3 Functional safety planning

A functional safety plan shall be generated and updated as necessary throughout the entire development of the PDS(SR). The plan shall define the activities required to satisfy Clauses 5 to 10, and identify the persons, department(s), or organization(s) responsible for completing these activities. The functional safety plan may be incorporated as a section titled "functional safety plan" in the overall quality plan for the PDS(SR), or it may be a separate document titled "functional safety plan."

In particular, the functional safety plan shall consider or include the following, as appropriate for the complexity of the PDS(SR).

a) Generation of the safety requirements specification (see 5.4), including factors such as:
   - the consideration of requirements from guidelines and standards for specific target applications of the PDS(SR);
   - the choice of methods for the avoidance of mistakes during generation of the safety requirements specification;
   - the personnel responsible for generation and maintenance of the safety requirements specification;
   - the personnel responsible for verification of the safety requirements specification;
   - the process for changing the safety requirements specification after development has started.

b) Design and development of the safety function(s) in the PDS(SR), including (where applicable) factors such as:
   - the consideration of applicable functional safety guidelines and standards for the design of target application equipment such as process control equipment or machinery which incorporates the PDS(SR);
   - the selection of product development and project management methodologies (see B.1.1 of IEC 61508-7:2000);
   - the personnel responsible for design and development;
   - the project documentation methodology (see B.1.2 of IEC 61508-7:2000);
   - the application of structured design techniques (see B.3.2 of IEC 61508-7:2000);
   - the use of simulation or other computer-based design tools;
   - the design verification methodology;
   - the integration and functional test techniques, regression testing, and responsible personnel;
   - the design change management (both hardware and software).

c) A verification plan for the safety function(s) including factors such as:
   - the selection of verification strategies and techniques;
   - the selection of verification activities;
   - the personnel responsible for verification;
   - the selection and utilization of test equipment;
   - the evaluation of verification results gained from verification equipment and from tests.

d) A validation plan for the safety function(s) comprising the following:
   - the personnel responsible for validation testing;
   - the identification of the relevant modes of operation of the PDS(SR);
   - the technical strategy for validation, for example analytical methods or statistical tests;
   - the acceptance criteria;
   - the action to be taken in the event of failure to meet the acceptance criteria.

e) Planning for installation and commissioning comprising the following (where applicable):
   - the special instructions for installation and sequence of installation;
   - the personnel responsible for installation and commissioning;
   - the commissioning activities and tests related to functional safety;
   - the reporting methodology for commissioning tests and results;
   - the mechanism for resolution of test failures and issues.

f) Planning for safety-related user documentation including:
   - a list of significant safety-related information which must be provided;
   - the personnel responsible for user documentation;
   - the review process to insure the accuracy of documentation

g) Where assessment is required (see Clause 8 of IEC 61508-1:1998), a functional safety assessment plan comprising the following shall be available:
   - the scope of the functional safety assessment;
   - the personnel responsible for the functional assessment;
   - the stages at which the functional safety assessment activities are to be carried out (for example, after the safety requirements specification has been developed, after the safety-related control system has been designed);
   - the information that shall be generated as a result of the functional safety assessment activity;

- the resources required to complete the functional safety assessment activity;
- the level of independence of the assessment team;
- the means by which the functional safety assessment shall be revalidated after modifications to the PDS(SR).

## 5.4 Safety requirements specification (SRS) for a PDS(SR)

### 5.4.1 General

A safety requirements specification for a PDS(SR) shall be documented and shall comprise:

- a safety functionality requirements specification (see 5.4.2); and
- a safety integrity requirements specification (see 5.4.3).

These shall be written so that they are:

- clear;
- precise;
- unequivocal;
- feasible.
- verifiable;
- testable;
- maintainable.

For the avoidance of mistakes during the compilation of these specifications, appropriate techniques and measures shall be applied (see Table B.1 of IEC 61508-2:2000).

### 5.4.2 Safety functionality requirements specification

The safety functionality requirements specification shall provide comprehensive detailed requirements sufficient for the design and development of the PDS(SR).

The safety functionality requirements specification shall describe, as appropriate:

a) all safety functions to be performed;

b) all possible states of the PDS(SR) that can be used to achieve a safe state for intended applications;

c) the operating modes of the PDS(SR) – for example setting, start-up, maintenance, normal intended operation;

d) all required modes of behaviour of the PDS(SR);

e) the priority of those functions that are simultaneously active and can conflict with each other;

f) the required action(s) when a violation of limits is detected during the correct operation of a safety function (i.e. the reaction on violation of limits (see 4.1));

g) the fault reaction function(s) (see 4.1 and 6.3);

h) the maximum fault reaction time to enable the corresponding fault reaction to be performed before a hazard occurs in intended applications (only required where *diagnostic tests* are used to achieve the SIL capability);

i) the maximum response time of each safety-related function (i.e. both safety and fault reaction functions (see 6.3));

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

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

k) all means by which the operator interacts with the PDS(SR), that can influence the safety-related functions (i.e. both safety and fault reaction functions);

l) all interfaces between the PDS(SR) and any other systems (either directly associated within, or outside, the installation).

### 5.4.3 Safety integrity requirements specification

The safety integrity requirements specification for a PDS(SR) shall contain:

a) for each safety-related function (or group of simultaneously used safety functions), both a SIL capability and a maximum probability of dangerous random hardware failure;

NOTE 1 SIL capability is relevant if the PDS(SR) is to be considered as a component which implements a safety function in conjunction with other components.

NOTE 2 In order to accommodate the probability of *dangerous failure* of other involved components, the probability of dangerous random hardware failure of the PDS(SR) will usually have to be lower than the target failure measure associated with the SIL allocated to the complete safety function. However, it may also be higher, if the PDS(SR) is to be used to implement the safety function in a redundant configuration with other components.

NOTE 3 Where a PDS(SR) implements a safety function completely within itself, the safety integrity requirements specification will identify a SIL, not a SIL capability.

NOTE 4 Where common hardware is used to implement more than one safety function, and the safety functions are used simultaneously, the probability of dangerous random hardware failure of the common hardware should be considered only once when determining the overall probability of dangerous random hardware failure.

NOTE 5 For a multi-axis PDS(SR), where a safety function is required for more than one axis, the probability of dangerous random hardware failure of common hardware should be considered only once when determining the overall probability of dangerous random hardware failure.

b) the extremes of all environmental conditions (including electromagnetic) that are likely to be encountered by the PDS(SR) during storage, transport, testing, installation, commissioning, operation and maintenance;

NOTE This information may have been obtained in order to satisfy the requirements of IEC 61800-1, IEC 61800-2 or IEC 61800-4 and in this case need not be documented again.

c) any requirement for increased EM immunity (see 6.2.5).

## 6 Requirements for design and development of a PDS(SR)

### 6.1 General requirements

#### 6.1.1 Change in operational status

Any change in the operational status of a PDS(SR) that can lead to a hazardous situation (for example by unexpected start-up) shall only be initiated in response to a deliberate action by the operator.

NOTE For example, any failure of a PDS(SR) whilst in a hold state should not lead to an unexpected start-up of machinery and/or plant items.

#### 6.1.2 Design standards

The PDS(SR) shall be designed in accordance with IEC 61800-5-1 and, as necessary, other applicable standards of the IEC 61800 series.

### 6.1.3 Realisation

The PDS(SR) shall be realised in accordance with its safety requirements specification (see 5.4).

### 6.1.4 Safety integrity and fault detection

The PDS(SR) shall comply with all of a) to c) as follows:

a) the requirements for hardware safety integrity comprising:
   - the architectural constraints on hardware safety integrity (see 6.2.2), and
   - the requirements for the probability of dangerous random hardware failures per hour (see 6.2.1);

b) the requirements for systematic safety integrity comprising:
   - the requirements for the avoidance of failures (see 6.2.4.1), and the requirements for the control of systematic faults (see 6.2.4.2), or
   - evidence that components used are 'proven-in-use'. In this case the components shall fulfil the relevant requirements of IEC 61508-2;

c) the requirements for behaviour on detection of a fault (see 6.3).

### 6.1.5 Safety and non-safety functions

Where a PDS(SR) is to perform both safety and non-safety functions, then all of its hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not cause a *dangerous failure* of the safety-related functions).

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

### 6.1.6 SIL to be used

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

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

### 6.1.7 Software requirements

If software is used to implement a safety function of the PDS(SR) with a specific SIL or SIL capability (see 5.4.3), then this software shall be implemented in accordance with the requirements defined by IEC 61508-3 for that specific SIL.

### 6.1.8 Review of requirements

The requirements for safety-related hardware and software shall be reviewed to ensure that they are adequately specified. In particular, the following shall be considered:

a) safety functions;

b) safety integrity requirements;

c) equipment and operator interfaces.

### 6.1.9 Design documentation

Besides the documentation of the design and realisation, the PDS(SR) design documentation shall indicate those techniques and measures used to achieve the SIL claim (for example failure mode and effects analysis, fault tree analysis).

## 6.2 PDS(SR) design requirements

### 6.2.1 Requirements for probability of dangerous random hardware failures per hour (PFH)

#### 6.2.1.1 General requirements

##### 6.2.1.1.1 PFH for each safety function

The PFH of each safety function (or group of simultaneously used safety functions) to be performed by the PDS(SR), estimated according to 6.2.1.1.2 and Annex B, shall be equal to or less than the target failure measure (see Table 2) as specified in the safety integrity requirements specification (see 5.4.3).

The PFH value as defined by the SIL refers to a complete safety function. If a PDS(SR) is intended to perform only a part of a safety function within a safety related control system then the PFH of the drive should be sufficiently lower than the value defined by the SIL.

NOTE 1 The target failure measure, expressed in terms of the PFH, is determined by the SIL of the safety function (see IEC 61508-1:1998, Table 3), unless there is a requirement in the PDS(SR) safety integrity requirements specification (see 5.4.3) for the safety function to meet a specific target failure measure, rather than a specific SIL.

**Table 2 – Safety integrity levels: target failure measures for a PDS(SR) safety function**

| Safety integrity level | PFH |
|---|---|
| 3 | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ to $< 10^{-5}$ |
| NOTE The PFH is sometimes referred to as the frequency of *dangerous failures*, or *dangerous failure* rate, in units of *dangerous failures* per hour. | |

The PFH of each safety function (or group of simultaneously used safety functions) of the PDS(SR) shall be estimated separately.

NOTE 2 Different safety functions may have common components and/or unique components, resulting in different PFH for each safety function (or group of simultaneously used safety functions).

NOTE 3 A number of modelling methods are available and the most appropriate method is a matter for the analyst and will depend on the circumstances. Available methods include:

– fault tree analysis (see IEC 61025);

– Markov models (see IEC 61165);

– reliability block diagrams (see IEC 61078).

See also IEC 60300-3-1.

NOTE 4 The mean time to restoration (see IEV 191-13-08) that is considered in the reliability model will need to take into account the diagnostic and proof test intervals, the repair time and any other delays prior to restoration, and the mission time.

NOTE 5 Failures due to common cause effects and data communication processes may result from effects other than actual failures of hardware components (for example decoding errors). However, such failures are considered, for the purposes of this standard, as random hardware failures. (See Annex D of IEC 61508-6:2000)

NOTE 6 Annex B of IEC 61508-6:2000, describes a simplified approach which may be used to estimate the probability of *dangerous failure* of a safety function due to random hardware failures in order to determine that an architecture meets the required target failure measure.

#### 6.2.1.1.2 Estimation of PFH

The PFH of each safety function (or group of simultaneously used safety functions) to be performed by the PDS(SR), due to random hardware failures shall be estimated using Annex A of IEC 61508-2:2000, taking into account:

a) the architecture of the PDS(SR) as it relates to each safety function under consideration;

b) the estimated failure rate of each subsystem of the PDS(SR) in any modes which would cause a *dangerous failure* of the PDS(SR) but which are detected by *diagnostic tests*;

c) the estimated failure rate of each subsystem of the PDS(SR) in any modes which would cause a *dangerous failure* of the PDS(SR) which are undetected by the *diagnostic tests*;

d) the susceptibility of the PDS(SR) to *common cause failures* (see Annex D of IEC 61508-6:2000);

e) the *diagnostic coverage* (DC) of the *diagnostic tests* (determined according to Annexes A and C of IEC 61508-2:2000) and the associated *diagnostic test* interval;

NOTE 1 When establishing the *diagnostic test* interval, the intervals between all of the tests which contribute to the *diagnostic coverage* will need to be considered.

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

NOTE 2 In practice, proof testing may be difficult to implement for certain parts of the PDS(SR). In such cases, the proof test interval may be assumed to be the mission time of those parts or of the PDS(SR) itself. It should be noted that a mission time of 20 years may be required by many machinery applications.

g) the repair times for detected failures;

NOTE 3 The repair time will constitute one part of the mean time to restoration (see IEV 191-13-08), which will also include the time taken to detect a failure and any time period during which repair is not possible (see Annex B of IEC 61508-6:2000 for an example of how the mean time to restoration can be used to calculate the probability of failure). For situations where the repair can only be carried out during a specific period of time, for example while the EUC is shut down and in a safe state, it is particularly important that full account is taken of the time period when no repair can be carried out, especially when this is relatively large.

h) the probability of *dangerous failure* of any data communication process (see 6.4).

#### 6.2.1.1.3 Failure rate data

Component failure rate data shall be obtained from:

– a recognised source; or

– estimates based upon those components that are considered to be “proven in use” (see 7.4.7.6 to 7.4.7.12 of IEC 61508-2:2000).

The expected average operating temperature for a component should be used when estimating its failure rate.

Any failure rate data used should have a confidence level of at least 60 %.

NOTE 1 Data can be derived from that published in a number of industry sources (see Annex C).

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

NOTE 3 Although a constant failure rate is assumed by most probabilistic estimation methods, this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time), the results of most probabilistic calculation methods are therefore meaningless. Thus, any probabilistic estimation should include a specification of the components’ useful lifetimes. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolytic capacitors can be very sensitive). Experience has shown that the useful lifetime

often lies within a range of 8 years to 12 years. It can, however, be significantly less if components are operated near to their specification limits.

NOTE 4 The fault lists given in Annex D can be used to assist in determination of failure modes.

#### 6.2.1.1.4 *Diagnostic test* interval

The *diagnostic test* interval of any subsystem of the PDS(SR) shall be such as to enable the PDS(SR) to meet the requirement for the PFH (see 6.2.1.1.1).

Where a dangerous fault can lead to loss of the safety function, detection of this fault within the DC limits and initiation of a fault reaction is required in order to prevent a hazard. Diagnostic and fault reaction functions shall be performed within the specified maximum fault reaction time (see 5.4.2).

#### 6.2.1.1.5 Test interval when hardware fault tolerance zero

The *diagnostic test* interval of any subsystem of a PDS(SR) having a hardware fault tolerance of zero, on which a safety function is entirely dependent, shall be such that the sum of the *diagnostic test* interval and the time to perform the specified action (fault reaction function) to achieve or maintain a safe state is less than the specified maximum fault reaction time.

### 6.2.2 Architectural constraints

#### 6.2.2.1 Limitations of SIL

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware fault tolerance and safe failure fraction of the subsystems of a PDS(SR) that carry out that safety function. A hardware fault tolerance of *N* means that *N*+1 faults could cause a loss of the safety function. Table 3 and Table 4 specify the highest safety integrity level that can be claimed for a safety function which uses a subsystem, taking into account the hardware fault tolerance and safe failure fraction of that subsystem (see Annex C of IEC 61508-2:2000). The requirements of Table 3 or Table 4, whichever is appropriate, shall be applied to each subsystem carrying out a safety function and hence every part of the PDS(SR); 6.2.2.2.1 and 6.2.2.2.2 specify which one of Table 3 or Table 4 applies to any particular subsystem. With respect to these requirements,

a) In determining the hardware fault tolerance, no account shall be taken of other measures (such as diagnostics) that may control the effects of faults;

b) where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault;

c) in determining hardware fault tolerance, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented (see Note 3).

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

NOTE 2 The architecture of the subsystem, derived to meet the hardware fault tolerance requirements, is that used under normal operating conditions. The fault tolerance requirements may be relaxed while the PDS(SR) is being repaired on-line. However, the key parameters relating to any relaxation must have been previously evaluated (for example, mean time to restoration compared to the probability of a demand).

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

#### 6.2.2.2 Type A and Type B subsystems

##### 6.2.2.2.1 Type A

A subsystem can be regarded as type A if, for the components required to achieve the safety function:

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

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

c) there is sufficient dependable failure data from field experience to show that the claimed failure rates for detected and undetected *dangerous failure*s are met.

NOTE Annex D lists faults and fault exclusions that may be considered.

##### 6.2.2.2.2 Type B

A subsystem shall be regarded as type B if, for the components required to achieve the safety function, one or more of the criteria of 6.2.2.2.1 is not satisfied.

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

NOTE 2 For example, the control section consisting of micro controllers etc is considered as a type B subsystem.

NOTE 3 Annex D lists faults and fault exclusions that may be considered.

#### 6.2.2.3 Architectural constraints

The architectural constraints of either Table 3 or Table 4 shall apply: Table 3 applies for every type A subsystem forming part of the PDS(SR). Table 4 applies for every type B subsystem forming part of the PDS(SR).

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

| Safe failure fraction [a] | Hardware fault tolerance *N* (see 6.2.2.1) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | SIL1 | SIL2 | SIL3 |
| 60 % to < 90 % | SIL2 | SIL3 | SIL3 [b] |
| 90 % to < 99 % | SIL3 | SIL3 [b] | SIL3 [b] |
| ≥ 99 % | SIL3 | SIL3 [b] | SIL3 [b] |

[a] See 6.2.3 for details of how to estimate safe failure fraction.

[b] This part of IEC 61800 only applies to safety functions with a SIL not greater than SIL 3. For SIL 4 safety functions, the requirements of IEC 61508 should be applied.

**Table 4 – Hardware safety integrity: architectural constraints on type B safety-related subsystems**

| Safe failure fraction [a] | Hardware fault tolerance *N* (see 6.2.2.1) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | Not allowed | SIL1 | SIL2 |
| 60 % to < 90 % | SIL1 | SIL2 | SIL3 |
| 90 % to < 99% | SIL2 | SIL3 | SIL3 [b] |
| ≥ 99 % | SIL3 | SIL3 [b] | SIL3 [b] |

[a] See 6.2.3 for details of how to estimate safe failure fraction.

[b] This part of IEC 61800 only applies to safety functions with a SIL not greater than SIL 3. For SIL 4 safety functions, the requirements of IEC 61508 should be applied.

### 6.2.3 Estimation of safe failure fraction (SFF)

#### 6.2.3.1 Methods of analysis

To estimate the SFF of a subsystem, an analysis (for example fault tree analysis or failure mode and effects analysis) shall be performed to determine all relevant faults and their corresponding failure modes. The probability of each failure mode of the subsystem shall be determined based on the probability of the associated fault(s).

#### 6.2.3.2 Basis of data

The estimation of SFF shall be based upon either:

– statistically significant failure rate data collected from field experience; or

– component failure data from a recognised source.

See also 6.2.1.1.3.

NOTE See Annex C for an informative list of known sources.

#### 6.2.3.3 Safety relays

In a subsystem with hardware fault tolerance of zero, when a safety relay with a positively guided feedback contact is used to provide a safety function and *diagnostic coverage* of that function, the safety integrity due to architectural constraints of that subsystem is constrained to a SIL 2 claim limit.

#### 6.2.3.4 Calculation of SFF

The safe failure fraction of a subsystem shall be calculated using Annexes A and C of IEC 61508-2:2000.

### 6.2.4 Requirements for systematic safety integrity of a PDS(SR) and PDS(SR) subsystems

#### 6.2.4.1 Requirements for the avoidance of failures

##### 6.2.4.1.1 General

Techniques and measures shall be used which minimize the introduction of faults during the design and development of the hardware of the PDS(SR).

Tests, as planned according to 6.2.4.1.4, shall be performed. See also Clause 9.

#### 6.2.4.1.2 Choice of design methods

In accordance with the required safety integrity level, the design method chosen shall promote:

a) transparency, modularity and other features which minimize complexity and enhance understandability of the design;
b) clear and precise specification of
   – functionality,
   – subsystem interfaces,
   – sequencing and time-related information,
   – concurrency and synchronisation;
c) clear and precise documentation and communication of information;
d) verification and validation.

#### 6.2.4.1.3 Design measures

The following design measures shall be applied.

a) Proper design of the PDS(SR) and/or subsystems including
   – the use of components within manufacturers specifications, for example temperature, loading, power supply, power rating, and timing parameters;
   – the derating of design parameters to improve reliability where necessary to achieve target failure rates;
   – the proper combination and assembly of subsystems, for example cabling, wiring and any interconnections;
   – the use of reviews and inspections for early detection of design defects.
b) Compatibility:
   – use subsystems with compatible operating characteristics.
c) Withstanding specified environmental conditions:
   – design the PDS(SR) so that it is capable of safe operation in all specified environments, for example temperature, humidity, vibration, EM phenomena, pollution degree, overvoltage category, altitude.

#### 6.2.4.1.4 Test planning

During the design, the following different types of testing shall be planned as necessary:

a) subsystem testing;
b) integration testing;
c) validation testing;
d) configuration testing (see 7.1).

Documentation of the test planning shall include:

e) types of tests to be performed and procedures to be followed;
f) test environment, tools, configuration and programs;
g) pass/fail criteria.

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

NOTE The integrity of such tools can be demonstrated by specific testing, by an extensive history of satisfactory use or by independent verification of their output for the particular PDS(SR) that is being designed.

#### 6.2.4.1.5 Design maintenance requirements

A process for design maintenance and retesting, to ensure the safety integrity of the PDS(SR) remains at the required level during subsequent design revisions, shall be defined at the design stage.

### 6.2.4.2 Requirements for the control of systematic faults

#### 6.2.4.2.1 Design features

For controlling systematic faults, the design shall possess features that make the PDS(SR) and its subsystems tolerant against:

a) residual design faults in the hardware, unless the possibility of hardware design faults can be excluded by applying Clause A.3 and Table A.16 of IEC 61508-2:2000;

b) environmental stresses, including electromagnetic disturbances, by applying Clause A.3 and Table A.17 of IEC 61508-2:2000;

c) mistakes made by the operator of the PDS(SR) (see Clause A.3 and Table A.18 of IEC 61508-2: 2000);

d) residual design faults in the software (see 7.4.3 of IEC 61508-3:1998 and associated Table);

e) errors and other effects arising from any data communication process (see 6.4).

#### 6.2.4.2.2 Testability and maintainability

Testability and maintainability shall be considered during the design and development activities in order to facilitate implementation of these properties in the final PDS(SR).

#### 6.2.4.2.3 Human constraints

The design of the PDS(SR) shall take into account human capabilities and limitations and be suitable for the actions assigned to operators and maintenance staff. The design of operator interfaces shall follow good human-factor practice and shall accommodate the likely level of training or awareness of operators.

#### 6.2.4.2.4 Protection against unintentional modification

The PDS(SR) shall incorporate measures to protect (or facilitate protection) against unintentional modifications to safety-related software, hardware, parameterisation and configuration of the PDS(SR).

NOTE See B.4.8 of IEC 61508-7:2000.

#### 6.2.4.2.5 Input acknowledgement and operator mistakes

The design of the PDS(SR) shall incorporate input acknowledgement to control operational failures. The design shall also protect against operator mistakes (related to the safety functions of the PDS(SR)) via plausibility checks.

NOTE See B.4.6 and B.4.9 of IEC 61508-7:2000.

#### 6.2.4.2.6 Loss of electrical supply

The PDS(SR) shall be specified and designed taking into account the effects of the loss of electrical supply.

### 6.2.5 Electromagnetic (EM) immunity requirement of a PDS(SR)

#### 6.2.5.1 General

The performance criterion that shall be applied when making EM immunity tests on the PDS(SR) is specified in 6.2.5.3. This criterion does not apply to the normal (non-safety related) functions of the equipment (functional electromagnetic compatibility (EMC) of the PDS(SR) is achieved when it complies with the requirements of IEC 61800-3).

#### 6.2.5.2 Intended environment

The EM environment specified or anticipated for intended use of a PDS(SR) shall be used to determine the test levels for EM immunity.

Where the EM environment is not known by the PDS(SR) manufacturer, the test levels of IEC 61800-3 shall be used for immunity tests.

#### 6.2.5.3 Performance criterion

The following performance criterion shall be satisfied by the dedicated safety functions of a PDS(SR). The behaviour of all non-safety related functions of the PDS(SR) is not considered, except that 6.2.5.4 applies.

(FS) Functions of the PDS(SR) intended for safety applications:

– do not deviate outside their specified limits for functional safety, or

– may deviate temporarily or permanently outside their specified limits for functional safety if the PDS(SR) reacts to the EM disturbance in such a way that a defined safe state of the PDS(SR) is maintained or achieved within the specified maximum fault reaction time.

Permanent degradation of the safety function or destruction of components is allowed provided that a safe state is maintained or achieved within the specified maximum fault reaction time.

This criterion applies to all EM phenomena relevant to the PDS(SR) in its intended application.

#### 6.2.5.4 Introduction of hazards

When an EM immunity test is applied, no unsafe conditions or hazards shall be introduced by the PDS(SR).

#### 6.2.5.5 Verification

When EM immunity tests are performed, the specified mitigation measures shall be in place.

Depending on the analysis of the EM environment of the intended application of the PDS(SR), in order to verify increased immunity (as required by IEC 61508-2), either:

– where necessary (dependent on the EM phenomena and the required SIL), increase the test level, and/or the duration of the test, and/or the number of test cycles; or

– verify the effectiveness of any additional mitigation measures (see A.11.3 of IEC 61508-7:2000) that have been specified.

### 6.3 Behaviour on detection of fault

#### 6.3.1 Fault detection

The detection of faults within a PDS(SR) can be performed by *diagnostic tests*.

When a dangerous fault that can lead to loss of the safety function is detected, a fault reaction function shall be initiated in order to prevent a hazard. Diagnostics and fault reaction functions shall be performed within the specified maximum fault reaction time.

### 6.3.2 Fault tolerance greater than zero

The detection of a dangerous fault (by *diagnostic tests* or by any other means) in any subsystem which has a hardware fault tolerance greater than zero shall result in either:

a) a fault reaction function, or

b) the isolation of the faulty part of the subsystem to allow continued safe operation of the machinery and/or plant items whilst the faulty part is repaired. If the repair is not completed within the mean time to restoration (MTTR) assumed in the calculation of the probability of dangerous random hardware failure (see 6.2.1), then a fault reaction function shall be initiated.

### 6.3.3 Fault tolerance zero

The detection of a dangerous fault (by *diagnostic tests* or by any other means) in any subsystem having a hardware fault tolerance of zero and on which a safety function is entirely dependent shall result in a fault reaction function.

## 6.4 Additional requirements for data communications

When data communication is used in the implementation of a safety function then the probability of undetected failure of the communication process shall be estimated taking into account transmission errors, repetitions, deletion, insertion, resequencing, corruption, delay and masquerade. This probability shall be taken into account when estimating the *PFH* of the safety function due to random failures (see 6.2.1.1.2).

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

The measures necessary to ensure the required failure measure of the communication process shall be implemented according to the requirements of IEC 61508-2 and of IEC 61508-3. This allows two possible approaches:

a) the communication channel shall be designed, implemented and validated according to IEC 61508 throughout (so-called 'white channel' see Figure 3 a)). or

b) parts of the communication channel are not designed or validated according to IEC 61508 (so-called 'black channel' see Figure 3 b)). In this case, the measures necessary to ensure the failure performance of the communication process shall be implemented in the PDS(SR) safety-related components that interface with the communication channel. The implementation shall be in accordance with IEC 62280 as appropriate.

Where the data communication is used to exchange safety related data with subsystems external to the PDS(SR) the above requirements apply to the PDS(SR) together with the related subsystems.

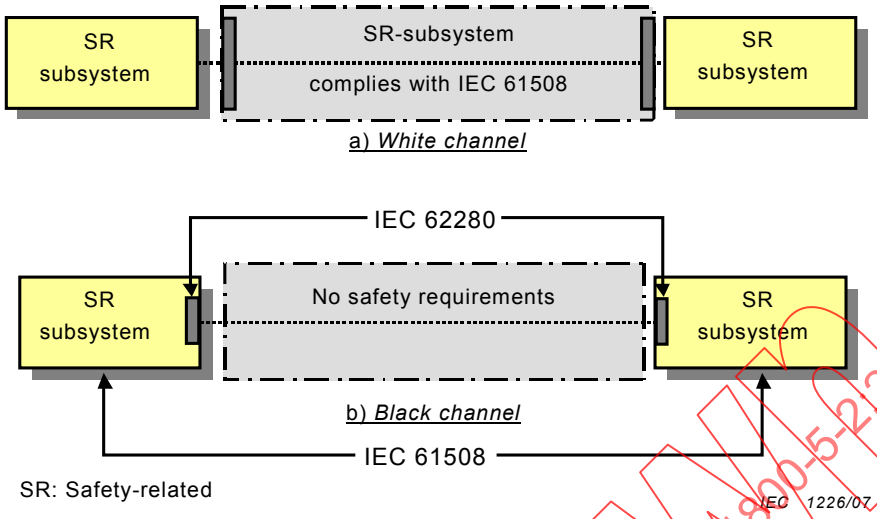



**Figure 3 – Architectures for data communication: a) White channel; b) Black channel)**

## 6.5 PDS(SR) integration and testing requirements

### 6.5.1 Hardware integration

The PDS(SR) shall be integrated according to its specified design. As part of the integration of all subsystems and components into the PDS(SR), the PDS(SR) shall be tested according to the specified integration tests. These tests are specified on the verification plan and shall show that all modules interact correctly to perform their intended function and not perform unintended functions.

Alternatively, the requirements for hardware integration are covered when the type testing of the PDS(SR) according to 6.2.5 and IEC 61800-5-1 and in addition IEC 61800-1 or IEC 61800-2 or IEC 61800-4 (as appropriate) is successfully passed.

### 6.5.2 Software integration

The integration of safety-related software part/module into the PDS(SR) shall be carried out according to IEC 61508-3. It shall include tests that are specified on the software verification plan to ensure the compatibility of the software with the hardware such that the functional and safety performance requirements are satisfied.

NOTE This does not imply testing of all input combinations. Testing all equivalence classes (see B.5.2 of IEC 61508-7:2000) may suffice. Static analysis (see B.6.4 of IEC 61508-7:2000), dynamic analysis (see B.6.5 of IEC 61508-7:2000) or failure analysis (see B.6.6 of IEC 61508-7:2000) may reduce the number of test cases to an acceptable level.

### 6.5.3 Modifications during integration

During the integration, any modification or change to the PDS(SR) shall be subject to an impact analysis, which shall identify all components affected, and additional verification.

### 6.5.4 Applicable integration tests

The integration test(s) shall be specified in a verification plan. A functional test shall be applied, in which input data or set values, which adequately characterise the normally expected operation, are given to the PDS(SR). The safety function is requested (for example, by activation of STO or speed limit violation for SLS), and its resulting operation is observed and compared with that given by the specification. (See also Clause 9.)

### 6.5.5 Test documentation

During PDS(SR) integration testing, the following shall be documented:

a) the version of the test plan used;
b) the criteria for acceptance of the integration tests;
c) the type and version of the PDS(SR) being tested;
d) the tools and equipment used along with calibration data;
e) the results of each test;
f) any discrepancy between expected and actual results.

## 7 Information for use

### 7.1 Information and instructions for safe application of a PDS(SR)

The following information shall be documented by the manufacturer and made available to the user.

a) A functional specification of each function and interface which is available for use in the implementation of safety functions. This shall comprise:
   - a detailed description of the safety function (including the reaction(s) to a violation of limits);
   - the fault reaction function;
   - the response time of each safety-related function and of the associated fault reaction functions;
   - the condition(s) (for example, operating mode) in which the safety function is intended to be active or disabled;
   - the priority of those functions that are simultaneously active and can conflict with each other.
b) The safety integrity information for each safety function, including:
   - the *SIL capability*;
   - the PFH value.
c) A definition of the environmental and operating conditions (including electromagnetic) under which the PDS(SR) is intended to be used (see also IEC 61800-1 or IEC 61800-2 or IEC 61800-4, IEC 61800-3 and IEC 61800-5-1). This shall take into account storage, transport, installation, commissioning, testing, operation and maintenance.
d) An indication of any constraints on the PDS(SR) for:
   - the environment which should be observed in order to maintain the validity of the estimated failure rates;
   - the mission time of the PDS(SR) and proof test interval(s), as appropriate;
   - any testing, calibration or maintenance requirements;
   - any limits on the application of the PDS(SR) which should be observed in order to avoid systematic failures;
   - the *SIL capability*; of each safety function
   - any information which is required to identify the hardware and software configuration of the PDS(SR) in order to enable configuration management in accordance with Clause 4.
e) The installation and commissioning guidance (see Clause 6 of IEC 61800-5-1:2003), including setting and parameterisation.

f) The requirements for configuration test of safety functions, in cases where the integrity of the means of configuration of a safety function cannot be ensured (for example, PC configuring tools).

The configuration test is carried out after the commissioning or modification of a specific application, to ensure that the used safety functions of the PDS(SR) are configured as intended. In particular, the test confirms the intended values of the parameters within the PDS(SR). The test is normally carried out and documented by the party responsible for commissioning the PDS(SR), using test procedures provided by the PDS(SR) manufacturer.

The configuration test manual shall require at least the following items to be recorded:

- a description of the application including a figure;
- a description of the safety related components (including software versions) that will be used in the application;
- a list of safety functions that will be used in the application of the PDS(SR);
- the results of each test of these safety functions, using given test procedures;
- a list of all safety relevant parameters and their values in the PDS(SR);
- the check sums, date of tests and confirmation by test personnel.

Configuration testing for PDS(SR)s in replicated applications may be carried out as a single type test of the replicated application, provided that it can be ensured that the safety functions will be configured as intended in all units.

g) The *diagnostic tests* to be performed either by the user or by parts of an installation that includes a PDS(SR) (for example, PLC, supervisory controller).

h) PDS(SR) operation and maintenance procedures shall be provided which shall specify the following:

- the routine actions which need to be carried out to maintain the functional safety of the PDS(SR), including replacement of components with a limited life (for example cooling fans, batteries, etc.);
- the actions and constraints necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event;
- the maintenance procedures to be followed when faults or failures occur in the PDS(SR), including:
  - the procedures for fault diagnosis and repair; and
  - the procedures for revalidation.
- the tools necessary for maintenance and revalidation, and procedures for maintaining the tools and equipment.

NOTE The PDS(SR) operation and maintenance procedures should be continuously upgraded following, for example:

- functional safety audits;
- tests on the PDS(SR).

## 8 Verification and validation

### 8.1 General

The objective of this subclause is to ensure the compliance with the functional safety plan (see 5.3).

### 8.2 Verification

During the design process, it shall be checked after each design phase that the requirements of that design phase have been fulfilled. Verification can be performed using assessment, analysis, examination, review, and/or testing.

### 8.3 Validation

After the design process, it shall be checked that the PDS(SR) fulfils all requirements of the safety requirements specification. Validation can be performed using assessment, analysis, examination, review, and/or testing. Recommendations for the avoidance of faults during validation are given in Table B.5 of IEC 61508-2:2000.

### 8.4 Documentation

Appropriate documentation concerning PDS(SR) verification and validation shall be produced, including:

a) the version(s) of the verification and validation plan(s) being used;

b) the safety function(s) under test (or analysis), along with the reference to the requirement(s) specified during PDS(SR) safety verification and validation planning;

c) the tools and equipment used;

d) the results of each verification and validation.

## 9 Test requirements

### 9.1 Planning of tests

Testing of the safety functions of the PDS(SR) shall be planned concurrently with each phase of the development process.

The test plan shall be documented, and shall include a detailed description of:

a) the functional testing of each safety function;

b) the functional testing of each diagnostics function for each safety function;

c) the acceptance criteria.

Tests may be either "black-box", where no account is taken of the internal implementation of the safety function, or "white-box", where specific knowledge of the implementation is used to determine the test (for example, fault insertion).

Testing may be waived or replaced by other verification or validation methods if permitted by the relevant requirements.

### 9.2 Test documentation

During PDS(SR) testing for safety functions, the following details shall be documented:

a) the version of the test plan used;

b) the criteria for acceptance of tests;

c) the type and version of the PDS(SR) being tested;

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

e) the conditions of the test;

f) the test personnel;

g) the detailed results of each test;

h) any discrepancy between expected and actual results;

i) the conclusion of the test: either it has been passed or the reasons for failure.

# 10 Modification

## 10.1 Objective

The objective of this clause is to ensure the functional safety of the PDS(SR) is maintained when design modifications are made after the original design is released for manufacture.

## 10.2 Requirements

Prior to carrying out any modification activity, procedures shall be planned. Modifications shall be performed with at least the same level of expertise, automated tools, and planning and management as the initial development of the PDS(SR). Modification shall be carried out as planned.

### 10.2.1 Modification request

The modification shall be initiated only by the issue of a modification request under the procedures for the management of functional safety (see Clause 5). The request shall detail the following:

a) the reasons for the change;

b) the proposed change (both hardware and software).

### 10.2.2 Impact analysis

An assessment shall be made of the impact of the proposed modification on the functional safety of the PDS(SR). The assessment shall include an analysis sufficient to determine the breadth and depth to which a return to appropriate development steps according to 5.2 will need to be undertaken.

### 10.2.3 Authorization

Authorization to carry out the requested modification shall be dependent on the results of the impact analysis.

### 10.2.4 Documentation

Appropriate documentation shall be established and maintained for each PDS(SR) modification activity. The documentation shall include:

a) the detailed specification of the modification;

b) the results of the impact analysis;

c) all approvals for changes;

d) the test cases for components including revalidation data;

e) the PDS(SR) configuration management history (hardware and software);

f) the deviation from previous operations and conditions;

g) the necessary changes to information for use;

h) all applicable development steps according to 5.2.

# Annex A
(informative)

## Sequential task table

According to the lifecycle described in IEC 61508 the following design procedure is appropriate for PDS(SR). The order of the necessary development steps is shown and reference is made to the appropriate clause or subclause in this standard or in IEC 61508.

NOTE 1 The lifecycle design and development has been split into “concept“ and ”design and development“ as it is common practice in design engineering.

NOTE 2 When third-party certification is desired, contact between the PDS(SR) manufacturer and the certification body should be established at the start of the design procedure.

NOTE 3 In the following table, references to IEC 61508 apply to the first edition of the part cited. Clause numbers may change in subsequent editions.

| | Tasks | References |
|---|---|---|
| **1** | **General requirements** | |
| | All relevant documents should be under the control of an appropriate document control scheme<br>Description of project management<br>Certification quality management system | IEC 61508-1:1998, §5<br>IEC 61508-2:2000, §7.3, 7.7, 7.8, 7.9<br>IEC 61508-3:1998, §6, 7.3, 7.4.2.1, 7.7, 7.8, 7.9 |
| **2** | **Specification of PDS(SR) safety requirements** | Phase 1 of PDS(SR) safety lifecycle (see 5.2 of this standard) |
| | Development of a safety requirements specification (SRS) including safety functions requirements and safety integrity requirements | See 5.4 of this standard<br>IEC 61508-1:1998, §7.6<br>IEC 61508-2:2000, §7.2, Tables B.1, B.6<br>IEC 61508-2:2000, §7.4.4-6, Annex A<br>IEC 61508-3:1998, §7.2,Tables A.1, B.7<br>IEC 61508-3:1998, §7.4.2/4, Tables A.3, B.1<br>IEC 61508-7:2000, Table C.1<br>Examples in IEC 61508-5,<br>Examples in IEC 61508-6:2000, Annex A |
| **3** | **Verification of PDS(SR) safety requirements specification** | |
| | a) Reviews of the safety requirements specification<br>b) Check by independent person or department where required | a) See 8.2 of this standard<br>b) IEC 61508-2:2000 and IEC 61508-3:1998, §7.9 |
| **4** | **Concept** | Phase 3 of PDS(SR) safety lifecycle (see 5.2 of this standard) |
| | **a) Hardware design on an architectural level, including**<br>• Block diagrams of safety related hardware<br>• User and process interfaces<br>• Safety relevant signal paths<br>• Power supply<br>• Separation of independent channels to achieve fault tolerance<br>• Communication links between independent channels to achieve *diagnostic coverage* | a) See Clause 6 of this standard<br>IEC 61508-2:2000, §7.4, Annex A, Tables B.2, B.6<br>Examples in IEC 61508-6:2000, Annexes A and D |

| | Tasks | References |
|---|---|---|
| | **b) Software design on an architectural level, including:**<br>• description of the functions provided by the safety related software<br>• interaction with hardware<br>• state machine diagrams of the intended behaviour of the software<br>• user and process interfaces<br>• fault detection possibilities and fault reactions<br>• overview of software structure, for example- with block diagram<br>• control and storage of safety related data<br>• version procedures<br>• used tools, for example compiler, code checker, etc. | b) IEC 61508-2:2000, §7.2.3.1(h)<br>IEC 61508-3:1998, §7.2.2.8, 7.2.2.10, 7.4.2/3, Tables A.2, B.1, B.7, B.9<br>IEC 61508-7:2000, Table C.1 |
| | **c) Recommendation**<br>Pre-estimation of the probability of failure of safety functions due to random hardware failures on a level of functional block diagrams | c) IEC 61508-1:1998, Table 2<br>IEC 61508-2:2000, §7.4.3, Tables 3, A.1, Annex C<br>IEC 61508-3:1998, Table B.4 (FMEA)<br>Examples in IEC 61508-6:2000, Annexes C and D |
| **5** | **Verification of concept** | |
| | a) Reviews of system design<br>b) Check by independent person or department where required | a) See 8.2 of this standard<br>b) IEC 61508-2:2000 and IEC 61508-3:1998, §7.9 |
| **6** | **Validation planning** | Phase 2 of PDS(SR) safety lifecycle (see 5.2 of this standard) |
| | a) Detailed planning of the validation of safety related PDS(SR).<br>b) The validation plan should be generated in parallel to Phase 9.3 Design and Development. | a) See 8.3 of this standard<br>b) IEC 61508-2:2000, §7.3, Table B.5<br>IEC 61508-3:1998, §7.3, Tables A.7, B.3, B.5 |
| **7** | **Verification of validation plan** | |
| | a) Reviews of the validation plan<br>b) Check by independent person or department where required | a) See 8.2 of this standard<br>b) IEC 61508-2:2000 and IEC 61508-3:1998, §7.9 |
| **8** | **Design and development** | Phase 3 of PDS(SR) safety lifecycle (see 5.2 of this standard) |
| | a) Hardware design<br>b) Software design<br>c) Reliability Prediction (calculation of the probability of failure of safety functions due to random hardware failures) including:<br>• type of PDS(SR)<br>• SFF<br>• functional block diagram<br>• reliability model<br>• data basis of the model (device lists)<br>• PFH calculation<br>• mission time<br>• repair interval, proof test interval (if relevant) | See Clause 6 of this standard<br>a) IEC 61508-2:2000, §7.4, Annex A, Table B.2, B.3, B.6<br>b) IEC 61508-3:1998, §7.4.5, 7.4.6, Table A.4<br>c) IEC 61508-1:1998, Table 2<br>IEC 61508-2:2000, §7.4.3, 7.4.7, Table 3, A.1, Annex C<br>IEC 61508-3:1998, Table B.4 (FMEA)<br>Examples in IEC 61508-6:2000, Annexes C and D |

| | Tasks | References |
|---|---|---|
| **9** | **Verification of the design** | |
| | a) Reviews of the system design<br>b) Functional tests on module level<br>c) Check by independent person or department where required | a) See 8.2 of this standard<br>c) IEC 61508-2:2000, §7.9<br>IEC 61508-3:1998, §7.4.7, 7.4.8, 7.5, 7.9, Tables A.5, A.9 |
| **10** | **PDS(SR) integration** | Phase 4 of PDS(SR) safety lifecycle (see 5.2 of this standard) |
| | Integration and test of the safety related PDS(SR). | See 6.5 of this standard |
| **11** | **Verification of integration** | |
| | Review of HW/SW integration test results and documentation | See 8.2 of this standard<br>IEC 61508-2:2000, §7.5, 7.9, Tables B.3, B.6<br>IEC 61508-3:1998, §7.4.3.2(f), 7.4.5.5, 7.4.6.2, 7.4.7, 7.5, 7.9, Tables A.5, A.6, A.9 |
| **12** | **Installation, commissioning and operation (user documentation)** | Phase 5 of PDS(SR) safety lifecycle (see 5.2 of this standard) |
| | Develop user documentation describing PDS(SR) installation, commissioning, operation and maintenance. | See Clause 7 of this standard<br>IEC 61508-2:2000, §7.6, Table-.B.4 |
| **13** | **Verification of user documentation** | |
| | a) Reviews of user documentation describing PDS(SR) installation, commissioning, operation and maintenance.<br>b) Check by independent person or department where required | a) See 8.2 of this standard<br>b) IEC 61508-2:2000 and IEC 61508-3:1998, §7.9 |
| **14** | **Validation of PDS(SR)** | Phase 6 of PDS(SR) safety lifecycle (see 5.2 of this standard) |
| | a) Provide all necessary information needed for PDS(SR) validation<br>b) Complete software and appropriate documentation<br>c) Validation tests and procedures according to the validation plan<br>d) Documentation of the results of the validation tests<br>e) Prepare appropriate documentation for third party validation where necessary | a) See 8.3 of this standard<br>c) IEC 61508-2:2000, §7.7, Tables B.5, B.6<br>IEC 61508-3:1998, §7.5.2.7, 7.7, 7.9, Table A.7 |
| **15** | **PDS(SR) modification procedure** | |
| | a) Modification request and analysis<br>b) Appropriate documentation of all modified parts of the PDS(SR)<br>c) Re-verification of modified parts<br>d) Update of reliability prediction if modification has impact on fault tolerance, probability of dangerous faults, *diagnostic coverage* or *common cause failure*<br>e) Re-validation of at least modified parts of the PDS(SR)<br>f) Software-modification | a) See Clause 10 of this standard<br>b) IEC 61508-1:1998, §7.16<br>IEC 61508-2:2000, §7.5.2.5, 7.8<br>Example in IEC 61508-1:1998, Figure 9<br>f) IEC 61508-3:1998, § 7.1.2.8, 7.5.2.6,7.6.2, 7.8.2, Table A.8 |

# Annex B
(informative)

# Example for determination of *PFH*

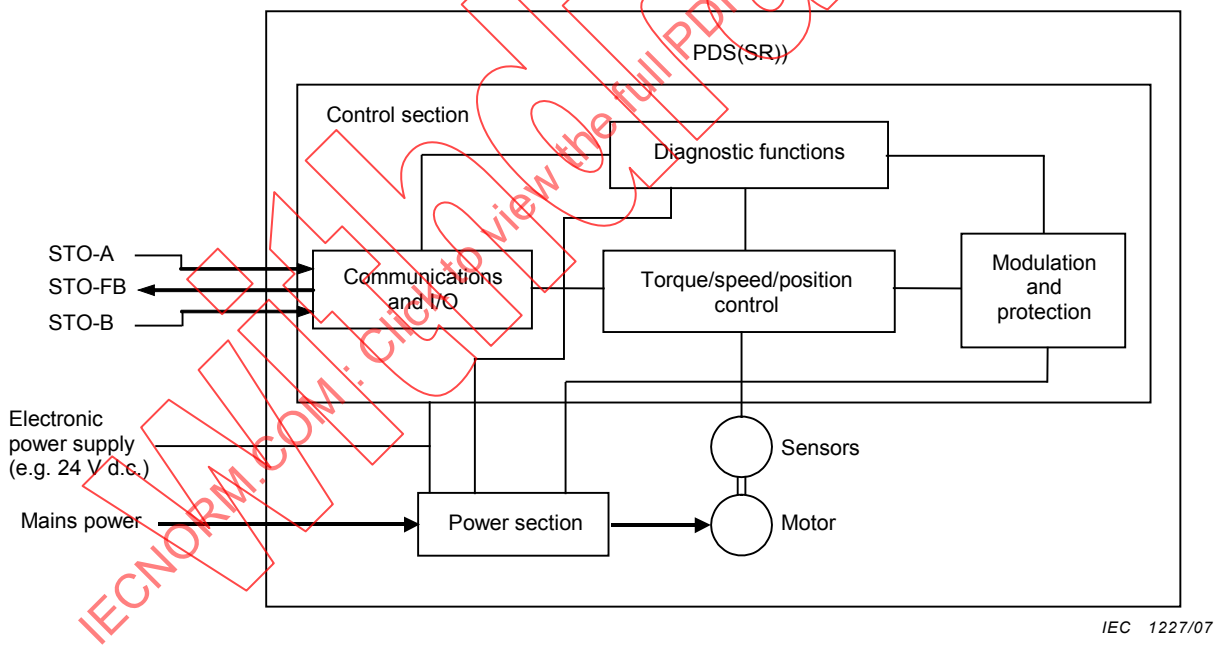
## B.1 General

This clause describes the determination of the *PFH* of an example PDS(SR) with the safety function safe torque off (STO). All the necessary requirements for, and the internal structural parts of, the PDS(SR) are given to show in detail how the PFH value can be calculated.

## B.2 Example PDS(SR) structure

### B.2.1 General

The PDS(SR) described in this clause includes the safety function STO, which is triggered by two redundant digital input interfaces and gives a single feedback signal through a digital output interface (see Figure B.1).




NOTE STO-A: STO trigger input channel A; STO-B: STO trigger input channel B; STO-FB: STO feedback output.

**Figure B.1 – Example PDS(SR)**

The example requirements are:

– SIL 2;

– continuous mode of operation.

Within the PDS(SR), the safety function STO is implemented together with the standard functionality of the PDS(SR) using only a few safety function exclusive components.

Due to the internal single channel power supply, the PDS(SR) is split in two independent subsystems: the two-channel subsystem A/B and the power supply/voltage monitor subsystem PS/VM (see Figure B.2).

The PFH value of the safety function STO of this example PDS(SR) is calculated as follows:

$PFH_{PDS(SR)} = PFH_{A/B} + PFH_{PS/VM}$

where $PFH_{A/B}$ and $PFH_{PS/VM}$ are the PFH values of subsytems A/B and PS/VM respectively.

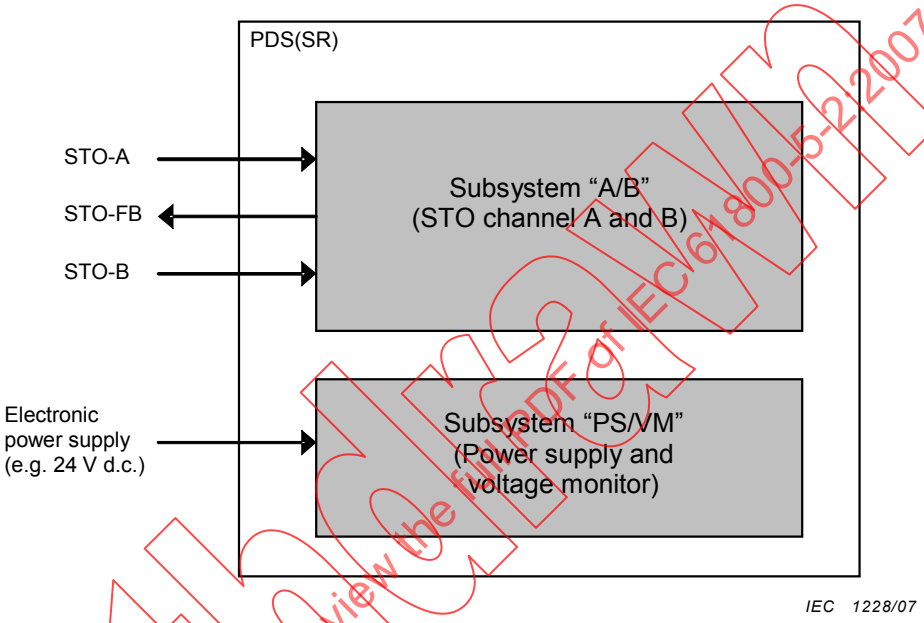



**Figure B.2 – Subsystems of the PDS(SR)**

### B.2.2 Subsystem A/B

The safety function STO is implemented with two channels to achieve the hardware fault tolerance of 1 and is modelled by the subsystem "A/B", for which an independent PFH value is computed. The realisation of the subsystem provides the following system properties regarding the safety function:

– type B (complex hardware);
– hardware fault tolerance of 1 (two channel implementation).

The architectural constraints of a type B subsystem (see 6.2.2.3) show that, for SIL 2 and hardware fault tolerance 1, the safe failure fraction (SFF) must be at least 60 %.

### B.2.3 Subsystem PS/VM

As the internal power supply (PS) has only a single channel, a voltage monitor (VM) is implemented. The internal power supply and the voltage monitor are modelled as a separate subsystem "PS/VM", for which an independent PFH value is computed. The realisation of the subsystem provides the following system properties regarding the safety function:

– type B (complex hardware);
– hardware fault tolerance of 0 (single channel implementation).

The architectural constraints of a type B subsystem (see 6.2.2.3) show that, for SIL 2 and hardware fault tolerance 0, the safe failure fraction (SFF) must be at least 90 %.

## B.3 Example PDS(SR) PFH value determination

### B.3.1 Subsystem "A/B" (main subsystem)

#### B.3.1.1 Function block division

Within the PDS(SR), the subsystem A/B is part of the implementation of the safety function STO and consists of 2 channels as necessary for the hardware fault tolerance of 1. Figure B.3 shows the schematic block diagram of the PDS(SR), highlighting the parts involved in executing the safety function STO.

In order to calculate the PFH value, the subsystem A/B is further subdivided into function blocks, and the failure rate of each is determined. Due to the minimal count of components of the digital trigger input circuitry and the switch off circuitry, only two function blocks are necessary.

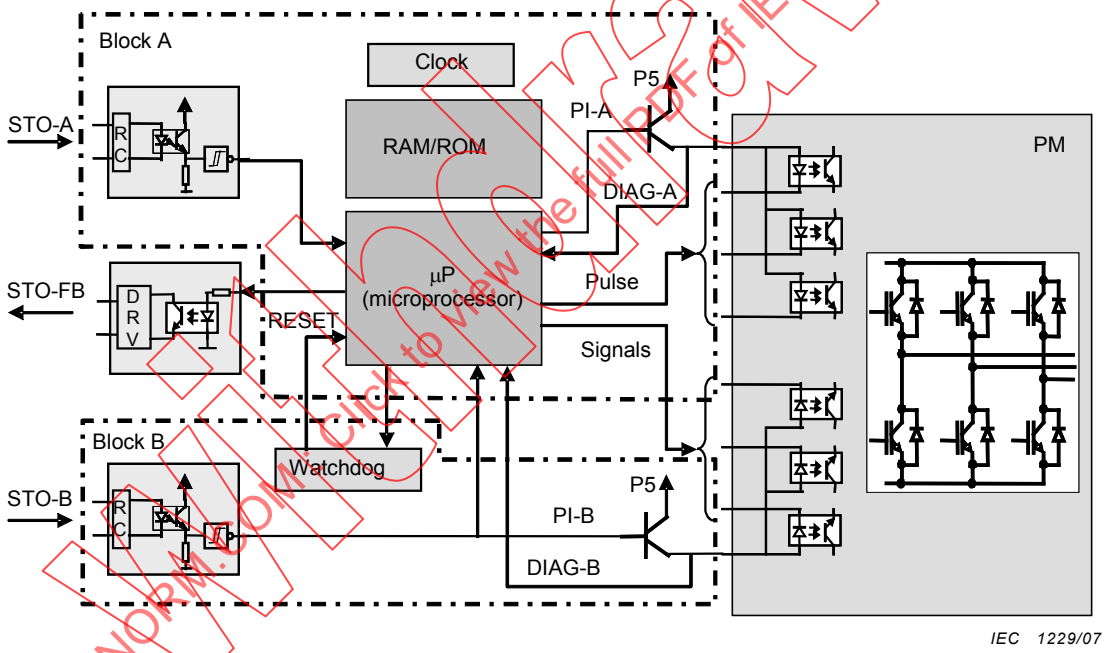



**Figure B.3 – Function blocks of subsystem A/B**

NOTE 1 P5: supply voltage 5V; PI-A(B): Pulse inhibition channel A(B); DIAG-A(B): Diagnosis signal channel A(B); RC: resistor capacitor filter; DRV: output driver; PM: power module.

NOTE 2 Component failures within the power module itself do not cause a loss of the safety function. Therefore, the power module does not have to be included in any subsystem contributing to the PFH value.

#### B.3.1.2 Determination of failure rates of function blocks

##### B.3.1.2.1 Function block analysis

For each function block, it is necessary to define what kind of failures shall be regarded as *dangerous failure*s. The result gives means to the following FMEA (failure mode effects analysis) of the components of the function block.

#### B.3.1.2.2 Component FMEA

The FMEA of the components of the circuit of the function block determines which components are regarded as relevant for the safety function and then allocates every failure mode of each safety relevant component the attribute safe or dangerous using the criteria determined in the function block analysis of B.3.1.2.1. For simple components, if dependable data is not available about the proportion of safe and dangerous failure modes, a single dangerous failure mode leads to the overall component failure being considered as dangerous. For complex components, Annex C of IEC 61508-6:2000 assumes a 50 % portion of safe and a 50 % portion of *dangerous failure* modes.

In addition, the FMEA identifies the proportion of the *dangerous failure* rate of each component which is detected by the available diagnosis functionality. For complex components, the portion of detected *dangerous failure*s has to be defined using the tables in IEC 61508-2. This proportioning defines the failure rates $\lambda_{DD}$ (dangerous detectable) and $\lambda_{DU}$ (dangerous undetectable) of the component.

The total failure rates of the function block ($\lambda_S$, $\lambda_{DD}$, $\lambda_{DU}$) are generated by summing up the safe failure rates, the detectable *dangerous failure* rates and the undetectable *dangerous failure* rates of all the safety related components of the function block.

#### B.3.1.2.3 Simplified method of determination of the differentiated failure rates

In complex hardware circuits with high component count, the FMEA on a component by component basis is not always practical. Therefore, a generally accepted simplified method, following Annex C of IEC 61508-6:2000, may be selected.

The failure rate of a total function block with complex circuit, calculated as sum of the failure rates of all components, is divided in a 50 % portion of safe failures and a 50 % portion of *dangerous failure*s. The portion of detected failures is determined by using the tables of IEC 61508-2.

This method will also lead to the failure rates $\lambda_S$, $\lambda_{DD}$ and $\lambda_{DU}$ of the function block.

### B.3.1.3 Safe failure fraction

Using the simplified method shown in B.3.1.2.3, the failure rates of the function blocks are determined as follows:

– safe failure proportion of failures of printed board circuits: 50 % (see NOTE).

NOTE The proportion of the *dangerous failure*s of printed board circuits is then also 50 %.

The *diagnostic coverage* (DC) is estimated by using the tables of IEC 61508-2.

**Table B.1 – Determination of DC factor of subsystem A/B**

| Method (IEC 61508-2) | DC level claim | Diagnostic test implementation |
|---|---|---|
| Table A.3 Failure detection by online monitoring | 90 % | Cyclic test checks redundant channels |
| Table A.3 Monitored redundancy | 99 % / 90 % | Cyclic test checks redundant channels |
| Table A.4 Self-test by software (walking bit) (one channel) | 90 % | Self-test of the microprocessor |
| Table A.6 RAM test “galpat” | 90 % | Done by the microprocessor |
| Table A.10 Watchdog with separate time base and time-window (also table A.12) | 90 % | Watchdog design |
| Table A.8 Inspection using test patterns | 99 % | Done by RAM-test |
| Table A.15 Cross monitoring of multiple actuators | 99 % | Cyclic test monitors both switch off actuators |

– $DC_A$ for function block A: 90 % (see Table B.1);

– $DC_B$ for function block B: 90 % (see Table B.1).

Failure rates of the circuitry of the function blocks A and B (realistic example values, expressed as failures in time (FIT), with units $10^{-9}$/h):

| | | | | |
|---|---|---|---|---|
| Block A: | $\lambda_A$ | (total failure rate) | | 450 FIT |
| | $\lambda_{AS}$ | (proportion of safe failures) | 0,5*450 FIT | 225 FIT |
| | $\lambda_{AD}$ | (proportion of *dangerous failures*) | 0,5*450 FIT | 225 FIT |
| | $\lambda_{ADD}$ | $DC_A$*$\lambda_{AD}$ | 0,9*225 FIT | 202,5 FIT |
| | $\lambda_{ADU}$ | (1-$DC_A$)*$\lambda_{AD}$ | (1-0,9)*225 FIT | 22,5 FIT |
| Block B: | $\lambda_B$ | (total failure rate) | | 70 FIT |
| | $\lambda_{BS}$ | (proportion of safe failures) | 0,5*70 FIT | 35 FIT |
| | $\lambda_{BD}$ | (proportion of *dangerous failures*) | 0,5*70 FIT | 35 FIT |
| | $\lambda_{BDD}$ | $DC_B$*$\lambda_{BD}$ | 0,9*35 FIT | 31,5 FIT |
| | $\lambda_{BDU}$ | (1-$DC_B$)*$\lambda_{BD}$ | (1-0,9)*35 FIT | 3,5 FIT |

The Safe Failure Fraction of subsystem A/B, calculated according to item g) of Clause C.1 of IEC 61508-2:2000, is:

$SFF_{A/B}$ = $[(\lambda_{AS}+ \lambda_{BS}) + (DC_A * \lambda_{AD}) + (DC_B * \lambda_{BD})] / [(\lambda_{AS}+ \lambda_{BS}) + (\lambda_{AD}+ \lambda_{BD})]$

= [(225 + 35) + (0,9 * 225) + (0,9 * 35)] FIT / [(225 + 35) + (225 + 35)T] FIT

= 494 FIT / 520 FIT;

$SFF_{A/B}$ = 95 %;

### B.3.1.4 *Common cause failure* factor $\beta_{A/B}$

The *common cause failure* factor $\beta_{A/B}$ is estimated by using Table D.4 of Annex D of IEC 61508-6:2000.

$\beta_{A/B}$ = 2 %;

### B.3.1.5 Reliability model (Markov)

The reliability model of the subsystem A/B is implemented as a Markov model, the state graph of which is shown in Figure B.4.

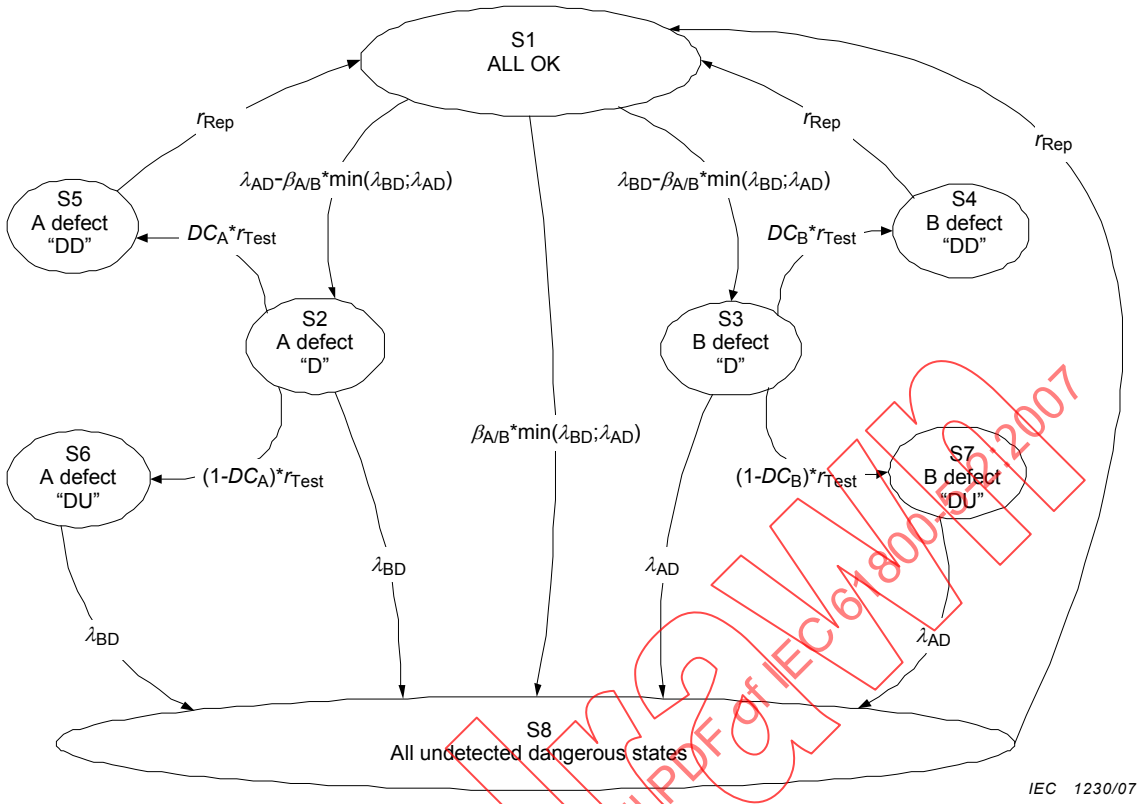



**Figure B.4 – Reliability model (Markov) of subsystem A/B**

NOTE 1 The above Markov model should be regarded as an approximation, as the transition processes corresponding to diagnostic tests and event triggered repairs, due to their nature, do not comply with the necessary conditions for the Markov technique in a mathematically strict sense.

NOTE 2 The model shown in Figure B.4 shows the inclusion of diagnostic tests in a detailed manner. Due to the usual magnitude of failure rates and test rates, the model could be simplified. Normally, it is not significant whether the test rate is 1/8 h or 1/168 h (see Table B.2).

NOTE 3 In Figure B.4, min($\lambda_{BD}$;$\lambda_{AD}$) means $\lambda_{BD}$ or $\lambda_{AD}$, whichever is smaller.

The model does not take account of "safe" failures because they have no important influence on the PFH value. The model assumes that the PDS(SR) is switched off line and repaired after detection of a failure.

The *common cause failure* rate is determined by the factor $\beta_{A/B}$ and the lower value of the *dangerous failure* rates of function block A and B. (see NOTE 3).

NOTE 4 The rate of simultaneous failure of both blocks can never be greater than the lower of the both failure rates.

In state S2, the function block A has failed dangerously. Depending on the operation of the diagnostic test, three possible states can follow.

– S5 follows, if the diagnostic test detects the failure, and the function block is repaired.
– S6 follows, if the diagnostic test does not detect the failure.
– S8 follows if function block B fails before the diagnostic test detects the failure in function block A.

In state S6, the function block A has failed undetected dangerously. S8 follows if block B fails dangerously.

State S8 represents the dangerous situation where the safety function is no more available and no test is effective any longer. Since continuous mode of operation is assumed for the PDS(SR), state S8 also represents the "hazardous event" resulting from a dangerously failed PDS(SR) confronted with demand of the safety function.

### B.3.1.6 PFH value calculation

$\lambda$ values, DC and $\beta$ factors are given in B.3.1.3 and B.3.1.4:

Additional determinations:

— $r_{Test}$ = 1/8 h, 1/24 h, 1/168 h,... (diagnostic test rate)

— $r_{Rep}$ = 1/8 h (repair rate)

— $T_M$ = 10 years or 20 years (mission time)

To determine the PFH value, the time dependent progression of the probability [ $p_i(t)$ ] of each state [ S$i$ ] of the Markov model has to be calculated. The starting probability value of all states except state S1 is equal to zero. The starting probability value of state S1 is equal to one. The calculation has to be done up to the mission time $T_M$.

$$PFH_{A/B} = \frac{1}{T_M} \int_0^{T_M} [\beta_{A/B} \cdot \min(\lambda_{AD}, \lambda_{BD}) \cdot p_1(t) + \lambda_{BD} \cdot p_2(t) + \lambda_{AD} \cdot p_3(t) + \lambda_{BD} \cdot p_6(t) + \lambda_{AD} \cdot p_7(t)]\,dt$$

Results of calculations for different values of the parameters $\beta_{A/B}$, $r_{Rep}$, $r_{Test}$ and $T_M$ are shown in Table B.2.

**Table B.2 – PFH value calculation results for subsystem A/B**

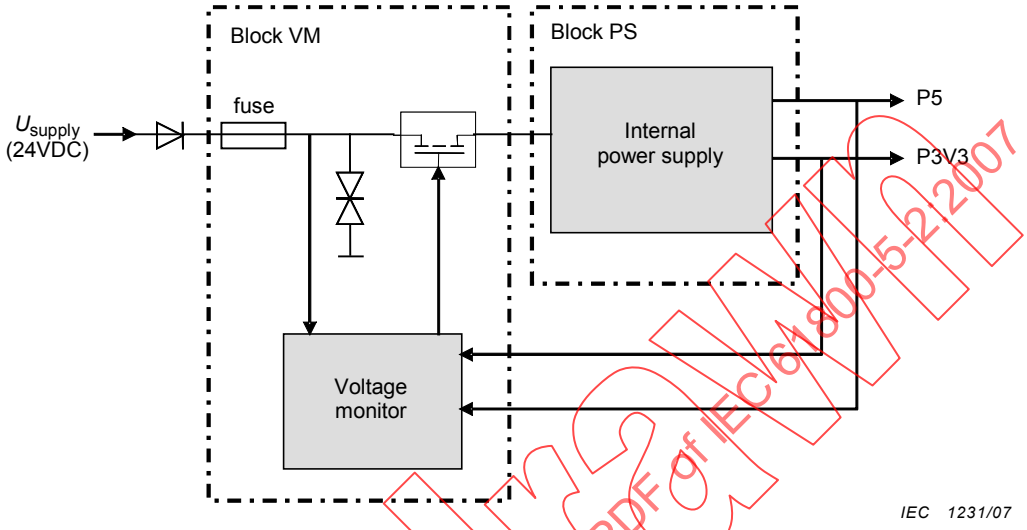
| $\beta_{A/B}$ | $r_{Rep}$ | $r_{Test}$ | $T_M$ (years) | $PFH_{A/B}$ |
|---|---|---|---|---|
| 2 % | 1/8 h | 1/8 h | 10 | $6.84 \times 10^{-10}$ /h |
| 2 % | 1/8 h | **1/24 h** | 10 | $6.84 \times 10^{-10}$ /h |
| 2 % | 1/8 h | **1/168 h** | 10 | $6.86 \times 10^{-10}$ /h |
| 2 % | 1/8 h | **1/672 h** | 10 | $6.91 \times 10^{-10}$ /h |
| 2 % | 1/8 h | **1/8760 h** | 10 | $7.72 \times 10^{-10}$ /h |
| 2 % | **1/8760 h** | 1/8 h | 10 | $6.83 \times 10^{-10}$ /h |
| 2 % | 1/8 h | 1/8 h | **20** | $7.38 \times 10^{-10}$ /h |
| 2 % | 1/8 h | **1/672 h** | 20 | $7.46 \times 10^{-10}$ /h |
| **3 %** | 1/8 h | 1/8 h | 20 | $1.05 \times 10^{-9}$ /h |
| **5 %** | 1/8 h | 1/8 h | 20 | $1.68 \times 10^{-9}$ /h |
| NOTE Values in bold characters give the modified value regarding the previous line. | | | | |

The results in Table B.2 show the influence of the test rate, the mission time and the *common cause failure* factor regarding the PFH value. The variation of the parameters is given to show the influence of each parameter to the PFH value.

### B.3.2 Subsystem "PS/VM"

#### B.3.2.1 Function block division

For the safety function STO, the subsystem PS/VM comprises one channel with a dedicated monitor. Figure B.5 shows the subsystem further subdivided into two function blocks which contain the internal single power supply (PS) and the voltage monitor circuit (VM).




NOTE P5: supply voltage 5 V; P3V3: supply voltage 3,3 V.

**Figure B.5 – Function blocks of subsystem PS/VM**

#### B.3.2.2 Failure rates of function blocks

The failure rates of each function block are determined using the methods of B.3.1.2.

#### B.3.2.3 Safe failure fraction

Using the simplified method shown in B.3.1.2.3, the failure rates of the function blocks are determined as follows:

– safe failure proportion of failures of printed board circuits: 50 % (see Note).

NOTE The proportion of the *dangerous failure*s of printed board circuits is then also 50 %.

The *diagnostic coverage* (DC) can be estimated by using the tables of Annex A of IEC 61508-2:2000.

**Table B.3 – Determination of DC factor of subsystem A/B**

| Method (IEC 61508- 2) | DC level claim | Method implementation |
|---|---|---|
| Table A.9 Voltage control (secondary) or power down with safety shut-off or switch-over to second power unit | High | Voltage monitor powers down the PDS(SR) |

– DC for function block PS: 99 % (see Table B.3).

– DC for function block VM: 0 % (no monitor of the voltage monitor available).

Failure rates of the circuitries of the function blocks PS and VM (realistic example values):

| | | | |
|---|---|---|---|
| Block PS: | $\lambda_{PS}$ (total failure rate) | | 250 FIT |
| | $\lambda_{PSS}$ (proportion of safe failures) | 0,5*250 FIT | 125 FIT |
| | $\lambda_{PSD}$ (proportion of *dangerous failures*) | 0,5*250 FIT | 125 FIT |
| | $\lambda_{PSDD}$ $DC_{PS}$ * $\lambda_{PSD}$ | 0,99*125 FIT | 123,75 FIT |
| | $\lambda_{PSDU}$ (1-$DC_{PS}$) * $\lambda_{PSD}$ | 0,01*125 FIT | 1,25 FIT |
| Block VM: | $\lambda_{VM}$ (total failure rate) | | 250 FIT |
| | $\lambda_{VMS}$ (proportion of safe failures) | 0,5*250 FIT | 125 FIT |
| | $\lambda_{VMD}$ (proportion of *dangerous failures*) | 0,5*250 FIT | 125 FIT |

The safe failure fraction of subsystem PS/VM is calculated according to item g) of Clause C.1 of IEC 61508-2:2000 (see NOTE):

$SFF_{PS/VM}$ = [$\lambda_{PSS}$ + ($\lambda_{PSD}$ * $DC_{PS}$)] / $\lambda_{PS}$

= [125 + (125 * 0,99)] FIT / 250 FIT

$\boldsymbol{SFF_{PS/VM}}$ = 99,5 %

NOTE The monitor block does not contribute to the SFF.

### B.3.2.4 *Common cause failure* factor $\beta_{PS/VM}$

The *common cause failure* factor $\beta_{PS/VM}$ is estimated by using Table D.4 of Annex D of IEC 61508-6:2000.

$\beta_{PS/VM}$ = 2 %.

### B.3.2.5 Reliability model (Markov)

The reliability model of the subsystem PS/VM is implemented as a Markov model the state graph of which is shown in Figure B.6.

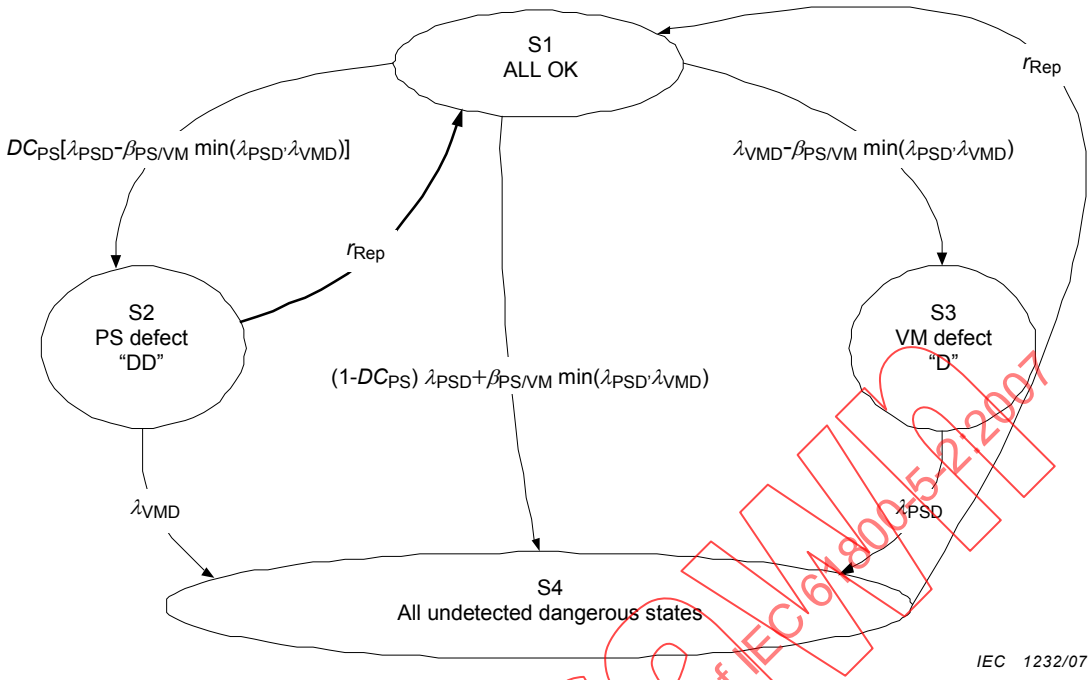



**Figure B.6 – Reliability model (Markov) of subsystem PS/VM**

NOTE 1 The above Markov model should be regarded as an approximation, as the transition processes corresponding to diagnostic tests and event triggered repairs, due to their nature, do not comply with the necessary conditions for the Markov technique in a mathematically strict sense.

NOTE 2 The voltage monitor provides continuous supervision of the power supply circuit. Therefore, no test rate appears in the model. Due to the usual magnitude of the failure rates and repair rates, the model could be simplified. The depicted version is intended for clarity.

The model shows the possible dangerous states but not the safe states which do not contribute to the PFH value but would increase the complexity of the model. The model assumes that the PDS(SR) is switched off line and repaired after detection of a failure.

The *common cause failure* is determined by the factor $\beta_{PS/VM}$ and the lower of the *dangerous failure* rates of function block PS and VM (see Note).

NOTE 3 For clarification: due to the fact that the *common cause failure* represents the failure of block PS and VM simultaneously within the different failure rates of the blocks, the *common cause failure* rate can never be greater than the lower of the both failure rates.

In state S2, the function block PS has failed detected dangerously. If the function block VM fails before the repair occurs, state S4 follows.

In state S3, the function block VM failed dangerously, which is not noticed due to the fact that there is no monitor for this function block. State S4 follows if function block PS fails dangerously.

If function block PS fails undetected dangerously, or both function blocks fail simultaneously, state S4 follows and the safety function is no more available

State S4 represents the dangerous situation where the safety function is no more available and no test is effective any longer. Since continuous mode of operation is assumed for the PDS(SR), state S4` represents the "hazardous event" resulting from a dangerously failed PDS(SR) confronted with demand of the safety function.

### B.3.2.6 PFH value calculation

$\lambda$ values, DC and $\beta$ factors are given in B.3.2.3 and B.3.2.4:

Additional determinations:

- $r_{Rep}$ = 1/8 h (repair rate)
- $T_M$ = 10 years or 20 years; (mission time).

To determine the PFH value, the time dependent progression of the probability of each state of the Markov model has to be calculated. The starting probability value of all states except state S1 is equal to zero. The starting probability value of state S1 is equal to one. The calculation has to be done up to the mission time $T_M$.

$$PFH_{PS/VM} = \frac{1}{T_M} \int_0^{T_M} [((1 - DC_{PS}) \cdot \lambda_{PSD} + \beta_{PS/VM} \cdot \min(\lambda_{PSD}, \lambda_{VMD})) \cdot p_1(t) + \lambda_{VMD} \cdot p_2(t) + \lambda_{PSD} \cdot p_3(t)] dt$$

Results of calculations for different values of the parameters $\beta_{PS/VM}$, $r_{Rep}$ and $T_M$ are shown in Table B.4.

**Table B.4 – PFH value calculation results for subsystem PS/VM**

| $\beta_{PS/VM}$ | $r_{Rep}$ | $T_M$ (years) | $PFH_{PS/VM}$ |
|---|---|---|---|
| 2 % | 1/8 h | 10 | 4,39 × $10^{-9}$ /h |
| 2 % | 1/8 h | **20** | 5,03 × $10^{-9}$ /h |
| **3 %** | 1/8 h | 20 | 6,25 × $10^{-9}$ /h |
| **5 %** | 1/8 h | 20 | 8,70 × $10^{-9}$ /h |
| NOTE Values in bold characters give the modified value regarding the previous line. | | | |

### B.3.3 PFH value of the safety function STO of PDS(SR)

Example PFH values with $r_{Rep}$ = 1/8 h and varied parameter $T_M$:

$PFH_{STO/PDS(SR)} = PFH_{A/B} + PFH_{PS/VM}$ (values from Table B.2 and Table B.4);

$PFH_{STO/PDS(SR)}$ ($T_M$ = 10 years) = (6,84 × $10^{-10}$/h + 4,39 × $10^{-9}$/h) = 5,074 × $10^{-9}$/h;

$PFH_{STO/PDS(SR)}$ ($T_M$ = 20 years) = (7,38 × $10^{-10}$/h + 5,03 ×$10^{-9}$/h) = 5,768 × $10^{-9}$/h;

# Annex C
(informative)

# Available failure rate databases

## C.1 Databases

The following bibliography is a non-exhaustive list, in no particular order, of sources of failure rate data for electronic and non-electronic components. It should be noted that these sources do not always agree with each other, and therefore care should be taken when applying the data.

- **IEC/TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment**, identical to RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l'Electricité et de la Communication (www.ute-fr.com).
- **Siemens Standard SN 29500, Failure rates of components**, (parts 1 to 14); can be obtained from: Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.
- **Reliability Prediction of Electronic Equipment, MIL-HDBK-217E**, Department of Defense, Washington DC, 1982.
- **Reliability Prediction Procedure for Electronic Equipment**, Telcordia SR-332, Issue 01, May 2001 (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06).
- **EPRD – Electronic Parts Reliability Data (RAC-STD-6100)**, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).
- **NNPRD-95 – Non-electronic Parts Reliability Data (RAC-STD-6200)**, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).
- **British Handbook for Reliability Data for Components used in Telecommunication Systems**, British Telecom (HRD5, last issue).
- **Chinese Military Standard GJB/z 299B**.
- **AT&T reliability manual** – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors,I, AT&T Reliability Manual, Van Nostrand Reinhold, 1990, ISBN:0442318480.
- **FIDES** – (FIDES is a new (January 2004) reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA). FIDES is available on request at fides@innovation.net.
- **IEEE Gold book** – The IEEE Gold book IEEE recommended practice for the design of reliable, industrial and commercial power systems provides data concerning equipment reliability used in industrial and commercial power distribution systems. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Phone: +1 800 678 IEEE (in the US and Canada) +1 732 981 0060 (outside of the US and Canada), FAX: +1 732 981 9667 e-mail: customer.service@ieee.org.
- **IRPH ITALTEL Reliability Prediction Handbook** – is the Italian telecommunication companies version of CNET RDF. The standards are based on the same data sets with only some of the procedures and factors changed. The Italtel IRPH handbook is available on request from: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy.
- **PRISM** (RAC / EPRD) – The PRISM software is available from the address below, or is incorporated within several commercially available reliability software packages: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

## C.2 Helpful standards concerning component failure

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

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60319, *Presentation and specification of reliability data for electronic components*

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60721-1, *Classification of environmental conditions – Part 1: Environmental parameters and their severities*

IEC 61709, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

# Annex D
(informative)

# Fault lists and fault exclusions

## D.1 General

The lists in Table D.1 to Table D.16 express some fault models, fault exclusions and their rationale.

For validation, both permanent and non-permanent faults should be considered.

The precise instant that the fault occurs may be critical. A theoretical analysis and, if necessary, tests should be carried out to determine worst case, for example at rest, during system start-up, during the course of operation.

## D.2 Remarks applicable to fault exclusions

### D.2.1 Validity of exclusions

All fault exclusions are only valid if the parts operate within their specified ratings.

### D.2.2 Tin whisker growth

If lead-free processes and products are applied, electrical short circuits due to tin whiskers (see Note 1) could occur. The risk of whiskers should be evaluated (See Note 2) and considered when applying the fault exclusion "short circuit …" of any component (see Notes 3 and 4).

NOTE 1 Tin whisker growing is a phenomenon related mainly to pure bright tin finishes. The needle-like protrusions may grow to several 100 µm length and can cause electrical shorts. Prevailing theory is that whiskers are caused by compressive stress buildup in tin plating.

NOTE 2 The following publications may be helpful for evaluation:

Test Method for Measuring Whisker Growth on Tin and Tin Alloy Surface Finishes, JESD22A121.01, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, www.jedec.org/download/search/22a121-01.pdf

Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes, JESD201, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, www.jedec.org/DOWNLOAD/search/**JESD201**.pdf

NOTE 3 Example: If the risk of whisker growing is considered high, the fault exclusion "Short circuit of a resistor" is useless, since a short between the contacts of this component has to be regarded.

NOTE 4 Whiskers on printed circuit boards have not been reported yet. Tracks usually consist of copper without tin coating. Pads may be coated with tin alloy, but the production process seems not to stimulate the susceptibility to whisker growing.

### D.2.3 Short-circuits on PWB-mounted parts

Short circuits for parts which are mounted on a printed wiring board (PWB) can only be excluded if the fault exclusion "short circuit between two adjacent tracks/pads" as described in Table D.2 is made.

## D.3 Fault models

**Table D.1 – Conductors/cables**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Short-circuit between any two conductors | Short-circuits between conductors which are:<br>- permanently connected (fixed) and protected against external damage, for example by cable ducting, armouring; or<br>- separate multicore cables, or<br>- within an electrical enclosure (see remark 1)), or<br>- individually shielded with earth connection. | 1) Provided both the conductors and enclosure meet the appropriate requirements (see IEC 60204-1). |
| Open-circuit of any conductor | None | |
| Short-circuit of any conductor to an exposed conductive part or to earth or to the protective bonding conductor | Short circuits between conductors which are within an electrical enclosure (see remark 1)). | |

**Table D.2 – Printed wiring boards/assemblies**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Short-circuit between two adjacent tracks/pads | Short-circuits between adjacent conductors in accordance with remarks 1) to 3). | 1) The base material of the PWB complies with the requirements of IEC 61800-5-1.<br>2) The creepage distances and clearances are dimensioned to at least IEC 60664-1 with pollution degree 2/ installation category III; if both tracks are powered by a SELV/PELV supply, pollution degree 2/ installation category II apply with a minimum clearance of 0,1 mm.<br>3) The assembled board is mounted in an enclosure giving protection against conductive contamination, e.g an enclosure with protection to at least IP54, and the printed side(s) are coated with an ageing-resistant varnish or protective layer covering all conductor paths.<br>NOTE 1 Experience has shown that a solder mask is satisfactory as a protective layer.<br>NOTE 2 A further protective layer covering according to IEC 60664-3 can reduce the creepage distances and clearances dimensions. |
| Open-circuit of any track | None | — |

**Table D.3 – Terminal block**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Short-circuit between adjacent terminals | Short-circuit between adjacent terminals in accordance with remarks 1) or 2). | 1) The terminals and connections used are in accordance with the requirements of IEC 61800-5-1.<br>2) Guaranteed by design, for example shaping shrink down plastic tubing over connection point. |
| Open-circuit of individual terminals | None | — |

**Table D.4 – Multi-pin connector**

| Faults considered | Fault exclusion | Remarks |
|---|---|---|
| Short-circuit between any two adjacent pins | Short-circuit between adjacent pins in accordance with remark 1).<br>Remark 2) also applies if the connector is mounted on a PWB. | 1) By using ferrules or other suitable means for multi-stranded wires. Creepage distances and clearances and all gaps should be dimensioned to at least IEC 60664-1:1992 with installation category III.<br>2) The assembled board should be mounted in an enclosure of at least IP 54 (see EN 60529) and the printed side(s) of the assembled board is covered with an ageing-resistant varnish or a protective layer covering all conductor paths in accordance with IEC 60664-3. |
| Interchanged or incorrectly inserted connector when not prevented by mechanical means | None | — |
| Short-circuit of any conductor (see remark 3)) to earth or a conductive part or to the protective conductor | None | 3) The core of the cable is considered as a part of the multi-pin connector. |
| Open-circuit of individual connector pins | None | — |

**Table D.5 – Electromechanical devices (for example relay, contactor relays)**

| Fault considered | Exclusions | Remarks |
|---|---|---|
| All contacts remain in the energised position when the coil is de-energized (for example due to mechanical fault) | None | — |
| All contacts remain in the de-energised position when power is applied (for example due to mechanical fault, open circuit of coil) | None | |
| Contact will not open | None | |
| Contact will not close | None | |
| Simultaneous short-circuit between the three terminals of a change-over contact | Simultaneous short-circuit can be excluded if remarks 1) and 2) are fulfilled. | 1) The creepage and clearance distances are dimensioned to at least IEC 60664-1:1992 with pollution degree 2 / overvoltage category III.<br>2) Conductive parts which become loose cannot bridge the insulation between contacts and the coil. |
| Short-circuit between two pairs of contacts and/or between contacts and coil terminal | Short-circuit can be excluded if remarks 1) and 2) are fulfilled. | |
| Simultaneous closing of normally open and normally closed contacts | Simultaneous closing of contacts can be excluded if remark 3) is fulfilled. | 3) Positively driven (or mechanically linked) contacts are used. |

**Table D.6 – Transformers**

| Faults considered | Fault exclusion | Remarks |
|---|---|---|
| Open circuit of individual winding | None | — |
| Short-circuit between different windings | Short-circuits between different windings can be excluded if remark 1) and 2) are fulfilled. | 1) The requirements of the relevant parts of IEC 61558 should be met.<br>2) Between different windings, doubled or reinforced insulation or a protective screen applies. Testing according to Clause 18 of IEC 61558-1 applies. Appropriate test voltages are given in Table 8a of IEC 61558-1.<br>Short-circuits in coils and windings need to be avoided by taking appropriate steps, for example:<br>▪ impregnating the coils so as to fill all the cavities between individual coils and the body of the coil and the core; and<br>▪ using winding conductors well within their insulation and high temperature ratings.<br>3) In the event of a secondary short-circuit, heating above a specified operating temperature should not occur. |
| Short-circuit in one winding | A short-circuit in one winding can be excluded if remark 1) is fulfilled. | |
| Change in effective turns ratio | Change in effective turns ratio can be excluded if remark 1) is fulfilled. See also the guidance in remark 3). | |

### Table D.7 – Inductances

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Open-circuit | None | – |
| Short-circuit | Short-circuit can be excluded if remark 1) is fulfilled. | 1) Coil is single layered, enamelled or potted and with axial wire connections and axial mounted. |
| Random change of value<br>$0,5L_N < L < L_N$ + tolerance<br>where $L_N$ is the nominal value of inductance (see remark 2)) | None | 2) Depending upon the type of construction, other ranges can be considered. |

### Table D.8 – Resistors

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Open-circuit | None | — |
| Short-circuit | Short-circuit can be excluded if remark 1) or remark 2) is fulfilled. | 1) The resistor is of the film type, or wirewound type with protection to prevent unwinding of wire in the event of breakage, with axial wire connections, axial mounted and varnished.<br>2) Resistors in surface-mount technology must be a thin film metal type in package types MELF, miniMELF or µMELF. |
| Random change of value<br>$0,5R_N < R < 2R_N$<br>where $R_N$ is the nominal value of resistance (see remark 3)) | None | 3) Depending upon the type of construction, other ranges can be considered. |

### Table D.9 – Resistor networks

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Open-circuit | None | — |
| Short-circuit between any two connections | None | |
| Short-circuit between any connections. | None | |
| Random change of value<br>$0,5R_N < R < 2R_N$<br>where $R_N$ is the nominal value of resistance (see remark 1)) | None | 1) Depending upon the type of construction, other ranges can be considered. |

**Table D.10 – Potentiometers**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Open-circuit of individual connection | None | — |
| Short-circuit between all connections | None | |
| Short-circuit between any two connections | None | |
| Random change of value<br>$0{,}5\ R_p < R < 2\ R_p$<br>where $R_p$ = nominal value of resistance (see remark 1)) | None | 1) Depending upon the type of construction, other ranges can be considered. |

**Table D.11 – Capacitors**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Open-circuit | None | — |
| Short-circuit | None | |
| Random change of value<br>$0{,}5\ C_N < C < C_N$ + tolerance<br>where $C_N$ = nominal value of capacitance (see remark 1)) | None | 1) Depending upon the type of construction, other ranges can be considered. |
| Changing value tan $\delta$ | None | — |

**Table D.12 – Discrete semiconductors (for example diodes, Zener diodes, transistors, triacs, GTO thyristors, IGBTs, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs])**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Open-circuit of any connection | None | — |
| Short-circuit between any two connections | None | |
| Short-circuit between all connections | None | |
| Change in characteristics | None | |
| Explosion of device case | Can be excluded if remark 1) is fulfilled | 1) Supply line short-circuit power is limited to the device case strength capability |

**Table D.13 – Optocouplers**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| Open-circuit of individual connection | None | — |
| Short-circuit between any two input connections | None | |
| Short-circuit between any two output connections | None | |
| Short-circuit between any two connections of input and output | Short-circuit between input and output can be excluded if remarks 1) and 2) are fulfilled. | 1) The optocoupler is built in accordance wih over-voltage category III according to IEC 61800-5-1 and IEC 60664-1:1992 Table 1. If a SELV/PELV power supply is used, pollution degree 2/ over-voltage category II applies.<br>2) Measures are taken to ensure that an internal failure of the optocoupler cannot result in excessive temperature of its insulating material. |

**Table D.14 – Non-programmable integrated circuits**

| Fault considered | Fault exclusions | Remarks |
|---|---|---|
| Open-circuit of each individual connection | None | — |
| Short-circuit between any two connections | None | |
| Stuck-at-fault (i.e. short-circuit to 1 and 0 with isolated input or disconnected output). Static "0" and "1" signal at all inputs and outputs, either individually or simultaneously | None | |
| Parasitic oscillation of outputs | None | |
| Changing values (for example input/ output voltage of analogue devices) | None | |
| NOTE In this standard, ICs with less than 1 000 gates and/or less than 24 pins, operational amplifiers, shift registers and hybrid modules are considered to be non-complex. This definition is arbitrary. | | |

**Table D.15 – Programmable and/or complex integrated circuits**

| Fault considered | Fault exclusions | Remarks |
|---|---|---|
| Faults in all or part of the function | None | — |
| Open-circuit of each individual connection | None | |
| Short-circuit between any two connections | None | |
| Stuck-at-fault (i.e. short-circuit to 1 and 0 with isolated input or disconnected output) Static "0" and "1" signal at all inputs and outputs, either individually or simultaneously | None | |
| Parasitic oscillation of outputs | None | |
| Changing value, for example input/output voltage of analogue devices | None | |
| Undetected faults in the hardware which go unnoticed because of the complexity of integrated circuit | None | |
| NOTE In this standard, an IC is considered to be complex if it consists of more than 1 000 gates and/or more than 24 pins. This definition is arbitrary. The analysis should identify additional faults which should be considered if they influence the operation of the safety function. | | |

**Table D.16 – Motion and position feedback sensors**

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| **General** | | |
| Short-circuit between any two conductors of the connecting cable | Table D.1 applies | |
| Open-circuit of any conductor of the connecting cable | None | |
| Input or output stuck at 0 or 1, single or on several inputs/outputs at the same time | None | |
| Open circuit or high-impedance state of single or several inputs/outputs at the same time. | None | |
| Decrease or increase of output amplitude | None | |
| Oscillation on one or several outputs [a] | None | Oscillations on several outputs are considered in phase |
| Change of phase shift between output signals [a] | None | For example, due to a contaminated encoder disc |
| Loss of attachment during standstill:<br>- sensor housing from motor chassis<br>- sensor shaft from motor shaft | Preparing FMEA and prove long-term integrity of mechanical fixings | Output signal equals standstill<br>If fault exclusion is claimed, the design of the sensor housing to chassis and sensor shaft to motor shaft mountings usually withstands an overstress factor of approximately 20, and specific maintenance information should be provided. |
| Loss or loosening of attachment during motion:<br>- sensor housing from motor chassis<br>- sensor shaft from motor shaft | Preparing FMEA and prove long-term integrity of mechanical fixings | Possible effects:<br>- static offset of sensor shaft<br>- dynamic slip of sensor shaft<br>- wrong output signal/zero speed signal<br>If fault exclusion is claimed, the design of the sensor housing to chassis and sensor shaft to motor shaft mountings usually withstands an overstress factor of approximately 20, and specific maintenance information should be provided. |
| Loosening of solid measure [a] (e.g. optical encoder disc). | None | Output indicates wrong position |
| No light from diode | None | |
| **Additionally for rotary sensors with Sin/Cos – output signals, analogue signal generation** | | |
| Static input and output, on one single or several signals, amplitude within power supply voltage | None | |
| Change of signal's shape | None | For example, no Sin/Cos – type signal, signal offset |
| Exchange of Sin and Cos output signal | Fault exclusion allowed if there are no electronic components applied to select an output signal from several sources | |
| **Additionally for incremental rotary sensor with square wave output signals** | | |
| Oscillation on output | None | |
| Output signal stops | None | For example, due to scratched disc |
| Zero pulse fails, is too short, too long or repeated | None | For example, due to mechanical damage |

**Table D.16 – Motion and position feedback sensors *(continued)***

| Fault considered | Fault exclusion | Remarks |
|---|---|---|
| **Additionally for encoder with incremental and absolute signals** | | |
| Concurrently wrong position change from incremental and absolute signal | Fault exclusion if incremental and absolute data are generated independently | Applies for example, on sin/cos-encoder with additional outputs for absolute position and/or commutation |
| **Additionally for rotary sensors with processor based interface** | | |
| Communication faults:<br>- repeating<br>- loss<br>- insertion<br>- wrong order<br>- wrong data<br>- delay | None | Equals fault model for communication busses |
| **Additionally for rotary sensor, multiturn** | | |
| Wrong number of revolutions | None | May be without impact on single turn signals |
| **Additionally for rotary sensors with synthesised output signals** | | |
| Wrong output signal due to synthesiser failure | None | |
| **Additionally for rotary sensors with position value acquired by counter** | | |
| Wrong position due to incorrect count | None | |
| **Additionally for linear sensors** | | |
| Mounting of the read sensor broken | Preparing FMEA and prove long-term integrity of mechanical fixings | If fault exclusion is claimed, the design of the sensor mountings usually withstands overstress, and specific maintenance information should be provided. |
| Static offset of solid measure (e.g. optical encoder strip) | None | |
| Damaged solid measure (e.g. optical encoder strip) | None | Shape of pulses changed, pulses fail at incremental sensors |
| **Additionally for resolver with signal processing/reference generator** | | |
| Cross coupling of the reference frequency | None | |
| - Central timer fails<br>- No conversion start for A/D converter<br>- Wrong timing of Sample & Hold | None | |
| A/D converter generates wrong values | None | For example due to overmodulation caused by too high reference voltage or electromagnetic influence |
| A/D converter generates no values | None | |
| No frequency on reference generator | None | |
| Wrong frequency on reference generator | None | |
| No periodic signal from reference generator | None | |
| Gain error or oscillation in signal processing (Ref, Sin, Cos) | None | |
| Magnetic influence on point of installation | Appropriate shielding on point of installation | For example, due to magnetic field of an electromagnetic brake |
| [a] N. A. on resolver | | |
| NOTE This table has been written assuming the use of optical sensors. If other sensors (for example inductive sensors) are used, corresponding faults apply. | | |

## Bibliography

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60300-3-1, *Application guide – Analysis techniques for dependability: Guide on methodology*

IEC 60664-1:1992, *Insulation coordination for equipment within low-voltage systems – Part 1: Principles, requirements and tests*

IEC 60664-3, *Insulation coordination for equipment within low-voltage systems – Part 3: Use of coating, potting or moulding for protection against pollution*

IEC 61025, *Fault tree analysis (FTA)*

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

IEC 61165, *Application of Markov techniques*

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

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 61558 (all parts), *Safety of power transformers, power supplies, reactors and similar products*

IEC 61558-1:2005, *Safety of power transformers, power supplies, reactors and similar products – Part 1: General requirements and tests*

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

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

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

ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

ENV 50129, *Railway applications – Safety-related electronic systems for signalling*

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

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# ENTRAÎNEMENTS ÉLECTRIQUES DE PUISSANCE À VITESSE VARIABLE –

## Partie 5-2: Exigences de sécurité – Fonctionnelle

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61800-5-2 a été établie par le sous-comité 22G: Systèmes d'entraînement électrique à vitesse variable, comprenant des convertisseurs à semi-conducteurs, du comité d'études 22 de la CEI: Systèmes et équipements électroniques de puissance.

La présente version bilingue (2013-01) correspond à la version anglaise monolingue publiée en 2007-07.

Le texte anglais de cette norme est issu des documents 22G/179/FDIS et 22G/182/RVD.

Le rapport de vote 22G/182/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61800, publiées sous le titre général *Entraînements électriques de puissance à vitesse variable*, est disponible sur le site internet de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. À cette date, la publication sera

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

**IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.**

# INTRODUCTION

Du fait de l'automatisation, de la demande croissante de la production et de la réduction des efforts physiques produits par les opérateurs, les systèmes de commande des machines et des usines jouent un rôle croissant dans l'accomplissement de la sécurité globale. Ces systèmes de commande utilisent de plus en plus d'appareillages et de systèmes électriques/ électroniques/électroniques programmables complexes.

Bien placés, parmi ces appareillages et ces systèmes, se situent les entraînements électriques de puissance à vitesse variable (PDS), utilisables dans des applications relatives à la sécurité (PDS(SR)).

Exemples d'applications industrielles:

- machines-outils, robots, équipements d'essai en production, bancs d'essai;
- machines à papier, machines de production textile, calandres pour l'industrie du caoutchouc;
- lignes de processus des plastiques, de la production chimique ou métallique, moulins;
- machines de concassage du ciment, fours à ciment, mixeurs, centrifugeuses, machines d'extrusion;
- machines de forage;
- convoyeurs, machines de maniement de matériaux, équipements de levage (grues, portiques, etc.);
- pompes, ventilateurs, etc.

Les développeurs utilisant PDS(SR) peuvent également se référer à la présente norme pour d'autres applications.

Il convient que les utilisateurs de la présente norme aient connaissance du fait que certaines normes de type C applicables aux machines font actuellement référence à l'ISO 13849-1 pour les systèmes de commande relatifs à la sécurité. Dans ce cas, les fabricants de PDS(SR) peuvent être invités à fournir des informations supplémentaires (par exemple, le niveau de performance et/ou la catégorie) afin de faciliter l'intégration d'un PDS(SR) dans les systèmes de commande relatifs à la sécurité pour les machines concernées.

NOTE Les «normes de type C» sont définies dans l'ISO 12100-1 comme des normes de sécurité des machines traitant des exigences de sécurité détaillées s'appliquant à une machine particulière ou à un groupe de machines particulier.

Auparavant, en l'absence de normes, il y avait une réticence à accepter des appareillages et des systèmes électroniques dans des fonctions relatives à la sécurité, et en particulier des appareillages et des systèmes électroniques programmables, en raison de l'incertitude liée aux performances de sécurité d'une telle technologie.

Il existe de nombreuses situations où des systèmes de commande incorporant un PDS(SR) sont utilisés, en tant qu'élément de mesures de sécurité par exemple qui ont été prévues pour accomplir une réduction du risque. Le verrouillage de protection est un cas typique qui permet de sortir le personnel d'une situation dangereuse afin que l'accès à la zone dangereuse soit uniquement possible lorsque les parties tournantes ont atteint un état sûr. La présente partie de la CEI 61800 fournit une méthodologie afin d'identifier la contribution apportée par un PDS(SR) aux fonctions de sécurité identifiées, de permettre la conception appropriée du PDS(SR) et de vérifier qu'elle satisfait aux performances demandées

Des mesures sont indiquées afin de coordonner la performance de sécurité du PDS(SR) avec la réduction attendue du risque en prenant en compte les probabilités et les conséquences de ses défaillances systématiques et aléatoires.

# ENTRAÎNEMENTS ÉLECTRIQUES DE PUISSANCE À VITESSE VARIABLE –

## Partie 5-2: Exigences de sécurité – Fonctionnelle

## 1 Domaine d'application et objet

La présente partie de la CEI 61800 spécifie des exigences et donne des recommandations pour la conception et le développement, l'intégration et la validation des PDS(SR), en considération de leur sécurité fonctionnelle. Elle s'applique aux entraînements électriques de puissance à vitesse variable couverts par les autres parties de la série CEI 61800.

NOTE 1 Le terme «intégration» se rapporte au PDS(SR) lui-même, non pas à son incorporation dans l'application relative à la sécurité.

Cette norme internationale est applicable uniquement lorsque la sécurité fonctionnelle d'un PDS(SR) est exigée et que le PDS(SR) fonctionne en forte demande ou en mode continu (voir 3.10). Pour les applications à faible demande, voir la CEI 61508.

La présente partie de la CEI 61800, qui est une norme de produit, expose des considérations relatives à la sécurité des PDS(SR) prises dans le cadre de la CEI 61508 et présente des exigences pour les PDS(SR) en tant que sous-systèmes d'un système relatif à la sécurité. Elle est destinée à faciliter la réalisation des éléments électriques/ électroniques/ électroniques programmables (E/E/PE) d'un PDS(SR) en liaison avec la performance de sécurité d'une ou des fonctions de sécurité d'un PDS.

En se référant aux exigences normatives de la présente partie de la CEI 61800, les fabricants et les fournisseurs de PDS(SR) indiqueront aux utilisateurs la performance de sécurité pour l'équipement (intégrateurs de systèmes de commande, concepteurs de machines et d'usines, etc.). Ceci facilitera l'incorporation d'un PDS(SR) dans un système de commande relatif à la sécurité utilisant les principes de la CEI 61508 ou ses applications sectorielles spécifiques (par exemple la CEI 61511, la CEI 61513, la CEI 62061) ou l'ISO 13849.

La conformité à la présente partie de la CEI 61800 satisfait à toutes les exigences de la CEI 61508 nécessaires à un PDS(SR).

La présente partie de la CEI 61800 ne spécifie pas d'exigences pour:

- l'analyse des dangers et des risques pour une application particulière;
- l'identification des fonctions de sécurité pour cette application;
- l'attribution initiale des SIL pour ces fonctions de sécurité;
- l'équipement entraîné, à l'exception des aménagements de l'interface;
- des phénomènes dangereux secondaires (issus par exemple d'une défaillance d'un processus de production ou de fabrication);
- les considérations de sécurité électrique, thermique et d'énergie, qui sont couvertes par la CEI 61800-5-1;
- le processus de fabrication du PDS(SR);
- la validité des signaux et des commandes du PDS(SR).

NOTE 2 Les exigences en sécurité fonctionnelle d'un PDS(SR) sont dépendantes de l'application et il faut qu'elles soient considérées comme une partie de l'évaluation globale du risque de l'installation. Lorsque le fournisseur du PDS(SR) n'est pas responsable de l'équipement entraîné, le concepteur de l'installation est alors

responsable de l'évaluation du risque et de la spécification des exigences fonctionnelles et d'intégrité de sécurité du PDS(SR).

NOTE 3 Bien que des actions malveillantes puissent avoir un effet sur la sécurité fonctionnelle du PDS(SR), les considérations de sécurité ne sont pas abordées dans la présente norme.

La présente partie de la CEI 61800 s'applique uniquement aux PDS(SR) incorporant des fonctions de sécurité dont le SIL n'est pas supérieur au SIL 3.

La Figure 1 montre les éléments fonctionnels d'un PDS(SR) qui sont considérés dans la présente partie de la CEI 61800.

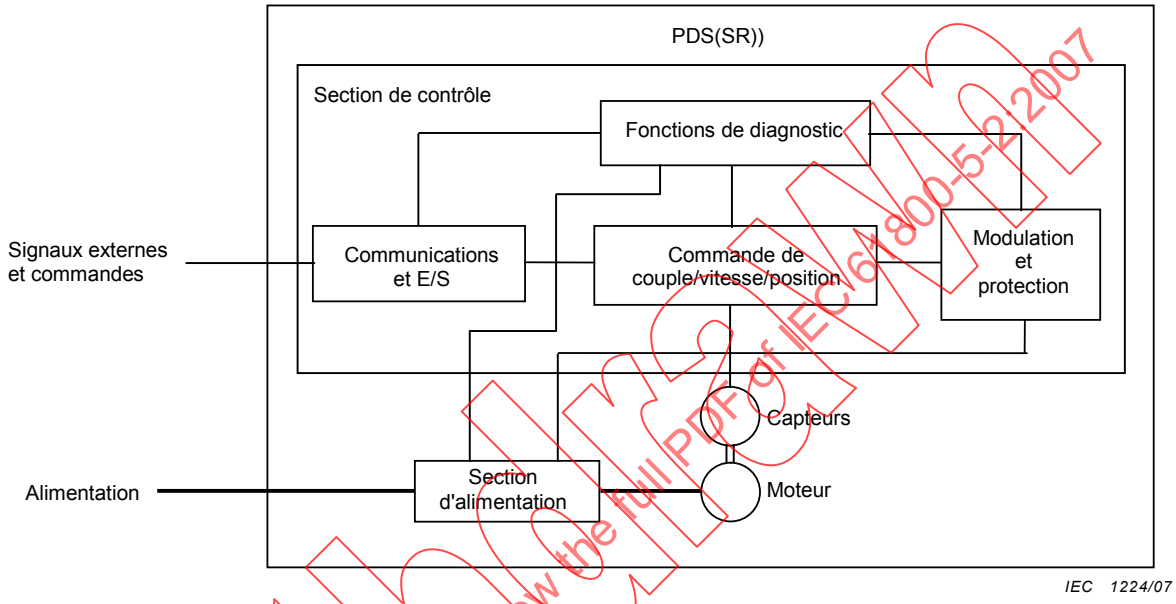



**Figure 1 – Éléments fonctionnels d'un PDS(SR)**

NOTE La Figure 1 n'est pas une description physique d'un PDS(SR) mais une représentation logique.

## 2 Références normatives

Les documents de référence suivants sont indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

NOTE 1 Cela ne signifie pas que la conformité à tous les articles des documents de référence soit exigée, mais plutôt que le présent document constitue une référence qui ne peut pas être comprise en l'absence des documents de référence.

NOTE 2 Les références aux diverses parties de la CEI 61508 sont non datées, sauf lorsque des articles spécifiques sont indiqués.

CEI 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*

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

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

CEI 61508-2:2000, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

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

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

CEI 61508-6:2000, *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*

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

CEI 61800-1, *Entraînements électriques de puissance à vitesse variable – Partie 1: Exigences générales – Spécifications de dimensionnement pour systèmes d'entraînement de puissance à vitesse variable en courant continu et basse tension*

CEI 61800-2, *Entraînements électriques de puissance à vitesse variable – Partie 2: Exigences générales – Spécifications de dimensionnement pour systèmes d'entraînement de puissance à vitesse variable en courant alternatif et basse tension*

CEI 61800-3, *Entraînements électriques de puissance à vitesse variable – Partie 3: Exigences de CEM et méthodes d'essais spécifiques*

CEI 61800-4, *Entraînements électriques de puissance à vitesse variable – Partie 4: Exigences générales – Spécifications de dimensionnement pour systèmes d'entraînements de puissance en courant alternatif de tension supérieure à 1 000 V alternatif et ne dépassant pas 35 kV*

CEI 61800-5-1:2003, *Entraînements électriques de puissance à vitesse variable – Partie 5-1: Exigences de sécurité – Électrique, thermique et énergétique*

CEI 62280 (toutes les parties), *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement*



## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

NOTE 1 Pour une liste alphabétique des définitions, voir le Tableau 1.

**Tableau 1 – Liste alphabétique des définitions**

| Terme | Numéro de la définition | Terme | Numéro de la définition |
|---|---|---|---|
| capacité SIL | 3.21 | niveau d'intégrité de sécurité (SIL) | 3.18 |
| couverture du diagnostic (DC) | 3.3 | PDS(SR) | 3.11 |
| défaillance dangereuse | 3.2 | PFH | 3.12 |
| défaillance de cause commune | 3.1 | phénomène dangereux | 3.7 |
| défaillance en sécurité | 3.14 | proportion de défaillances en sécurité (SFF) | 3.15 |
| défaillance systématique | 3.23 | sécurité fonctionnelle | 3.6 |
| durée de mission | 3.9 | sous-système | 3.22 |
| fonction de réaction au défaut | 3.5 | spécification des exigences de sécurité (SRS) | 3.20 |
| fonction(s) de sécurité (d'un PDS(SR)) | 3.16 | système relatif à la sécurité | 3.19 |
| installation | 3.8 | essai(s) de diagnostic | 3.4 |
| intégrité de sécurité | 3.17 | essai périodique | 3.13 |
| intégrité de sécurité systématique | 3.24 | validation | 3.25 |
| mode de fonctionnement | 3.10 | vérification | 3.26 |

NOTE 2 Dans l'ensemble de la présente norme internationale, les références aux définitions suivantes sont indiquées en *italique*.

**3.1**
**défaillance de cause commune**
défaillance résultant d'un ou de plusieurs événements qui, provoquant des défaillances simultanées de deux ou de plusieurs canaux séparés dans un système multicanal, conduit à la défaillance de la *fonction de sécurité*

[CEI 61508-4:1998, définition 3.6.10]

**3.2**
**défaillance dangereuse**
défaillance qui a la potentialité de mettre le *système relatif à la sécurité* dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

[CEI 61508-4:1998, définition 3.6.7]

**3.3**
**couverture du diagnostic**
**DC (diagnostic coverage)**
fraction exprimant la décroissance de la probabilité de défaillance dangereuse du matériel résultant du fonctionnement des *essais de diagnostic* automatiques

[CEI 61508-4:1998, définition 3.8.6]

NOTE 1 Cette couverture peut également être exprimée par le rapport entre la somme des taux de *défaillance dangereuse* $\lambda_{DD}$ détectés et la somme des taux de *défaillance dangereuse* totaux $\lambda_D$: $DC = \Sigma\lambda_{DD}/\Sigma\lambda_D$.

NOTE 2 La *couverture du diagnostic* peut se rapporter à tout ou partie du *système relatif à la sécurité*. Elle peut, par exemple, être disponible pour les capteurs et/ou le système logique et/ou les éléments terminaux.

**3.4**
**essai(s) de diagnostic**
essai(s) visant à détecter d'éventuels défauts ou défaillances et à produire des informations ou activités spécifiques au moment de la détection d'un défaut ou d'une défaillance

**3.5**
**fonction de réaction au défaut**
fonction initiée au moment de la détection, au sein du PDS(SR), d'un défaut ou d'une défaillance susceptible de causer une perte de la fonction de sécurité. La fonction de réaction au défaut vise à maintenir la sûreté de l'installation ou à prévenir l'émergence de situations dangereuses dans l'installation

**3.6**
**sécurité fonctionnelle**
sous-ensemble de la sécurité globale se rapportant à l'EUC (équipement sous contrôle) et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes E/E/PE (électriques/électroniques/électroniques programmables) relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque

[CEI 61508-4:1998, définition 3.1.9]

NOTE La présente norme ne prend en considération que les aspects de la définition de la sécurité fonctionnelle qui dépendent du fonctionnement correct du PDS(SR).

**3.7**
**phénomène dangereux**
source potentielle de dommage

[définition 3.5 de l'ISO/CEI Guide 51:1999]

NOTE 1 Le terme prend en compte les dangers à court terme envers les personnes (par exemple, les incendies et explosions) ainsi que ceux qui ont un effet à long terme sur la santé d'une personne (par exemple, la libération d'une substance toxique).

NOTE 2 La CEI 61508-4:1998 (modifiée) donne la définition suivante d'une **situation dangereuse**: situation dans laquelle une personne, une propriété ou un environnement est exposé à un ou des phénomènes ou événements dangereux.

**3.8**
**installation**
équipement ou équipements incluant au moins le PDS(SR) et l'équipement entraîné

NOTE Le terme «installation» est également utilisé dans la présente norme internationale pour désigner le processus d'installation d'un PDS(SR). Dans ces cas-là, le terme n'apparaît pas en italique.

**3.9**
**durée de mission**
durée spécifiée de fonctionnement du PDS(SR), cumulée au cours de l'ensemble de son cycle de vie

**3.10**
**mode de fonctionnement**
utilisation prévue d'un système relatif à la sécurité, en rapport avec la fréquence des demandes

[CEI 61508-4:1998, définition 3.5.12, modifiée]

NOTE 1 La CEI 61508 considère les deux modes de fonctionnement suivants:

- **mode de demande faible:** lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité n'est pas plus grande que une par an et au plus égale à deux fois la fréquence des essais périodiques;
- **mode de demande élevée ou mode continu**: lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité est plus grande que une par an ou supérieure à la fréquence des essais périodiques.

En général, le mode de fonctionnement de demande faible est considéré inadapté aux applications PDS(SR). De ce fait, la présente norme considère que les PDS(SR) fonctionnent uniquement dans les modes de demande élevée ou continu.

NOTE 2 Le mode de demande signifie qu'une fonction de sécurité n'est effectuée qu'en cas de demande de transfert de l'installation dans un état spécifié.

NOTE 3 Le mode continu signifie qu'une fonction de sécurité est effectuée en continu. Ainsi, le PDS(SR) contrôle continuellement l'installation et une défaillance (dangereuse) de sa fonction peut entraîner un phénomène dangereux.

**3.11**
**PDS(SR)**
entraînement électrique de puissance à vitesse variable, utilisable dans des applications relatives à la sécurité

**3.12**
**PFH**
probabilité de panne matérielle dangereuse aléatoire par heure

NOTE Dans la CEI 62061:2005, l'abréviation $PFH_D$ est utilisée.

**3.13**
**essai périodique**
essai périodique destiné à détecter les défaillances d'un système relatif à la sécurité de telle sorte que, lorsque nécessaire, le système peut être rétabli dans une condition "comme neuf'' ou dans une condition aussi proche que possible de celle-ci

NOTE En temps normal, les essais périodiques sont effectués dans le but de révéler des défaillances dangereuses qui ne sont pas détectées par les *essais de diagnostic*. L'efficacité d'un essai périodique dépend de jusqu'à quel point le système est rétabli dans une condition «comme neuf». Pour que l'essai soit complètement efficace, il est nécessaire de détecter 100 % des défaillances dangereuses. Bien que dans la pratique il ne soit pas facile d'atteindre 100 % pour tout système autre qu'un système de faible complexité, il convient de garder cet objectif.

[CEI 61508-4:1998, définition 3.8.5, modifiée]

**3.14**
**défaillance en sécurité**
défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

(CEI 61508-4:1998, définition 3.6.8)

**3.15**
**proportion de défaillances en sécurité**
**SFF (safe failure fraction)**
rapport entre le taux moyen de défaillance en sécurité, ajouté aux *défaillances dangereuses* détectées d'un sous-système PDS(SR), et le taux total moyen de défaillances de ce sous-système

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

NOTE Voir l'Annexe C de la CEI 61508-2:2000.

**3.16**
**fonction(s) de sécurité (d'un PDS(SR))**
fonction(s), selon une performance de sécurité spécifiée, dont tout ou partie est à réaliser par un PDS(SR) et qui vise à maintenir l'état sûr de l'installation ou à prévenir l'émergence de toute condition dangereuse dans l'installation

**3.17**
**intégrité de sécurité**
probabilité pour qu'un PDS(SR) exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées

NOTE 1 Plus le niveau d'intégrité de sécurité des PDS(SR) est élevé, plus la probabilité d'une défaillance des PDS(SR) dans l'exécution des fonctions de sécurité requises est faible.

NOTE 2 L'intégrité de sécurité peut ne pas être la même pour chaque fonction de sécurité réalisée par le PDS(SR).

(CEI 61508-4:1998, définition 3.5.2, modifiée)

**3.18**
**niveau d'intégrité de sécurité**
**SIL (safety integrity level)**
niveau discret (parmi quatre possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer (tout ou partie) à un PDS(SR)

NOTE 1 Le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas.

NOTE 2 Le SIL 4 n'est pas pris en compte dans la présente norme car il ne s'applique pas aux exigences de réduction des risques qui sont normalement associées aux PDS(SR). Pour les exigences relatives au SIL 4, voir la CEI 61508.

(CEI 61508-4:1998, définition 3.5.6, modifiée)

**3.19**
**système relatif à la sécurité**
système qui, à la fois

– met en œuvre les fonctions de sécurité requises pour atteindre un état de sécurité de l'EUC ou pour maintenir un tel état; et
– est prévu pour atteindre, par lui-même ou grâce à des systèmes E/E/PE relatifs à la sécurité ou des systèmes relatifs à la sécurité basés sur une autre technologie ou des dispositifs externes de réduction de risque, le niveau d'intégrité de sécurité nécessaire à la mise en œuvre des fonctions de sécurité requises

**3.20**
**spécification des exigences de sécurité**
**SRS (safety requirements specification)**
spécification contenant l'ensemble des exigences des fonctions de sécurité que le PDS(SR) est tenu d'assurer

**3.21**
**capacité SIL**
SIL maximal pouvant être atteint grâce à la conception d'un PDS(SR), en tenant compte de l'intégrité de sécurité systématique et des contraintes architecturales ayant une influence sur l'intégrité de sécurité du matériel

NOTE Une capacité SIL différente peut être associée à chacune des fonctions de sécurité désignées, qu'un PDS(SR) est censé assurer.

**3.22**
**sous-système**
partie de la conception supérieure de l'architecture d'un système relatif à la sécurité; une défaillance de ce sous-système entraîne la défaillance d'une fonction de sécurité

NOTE 1 Un PDS(SR) peut être un sous-système en soi, ou être constitué de plusieurs sous-systèmes distincts qui, une fois assemblés, réalisent la fonction de sécurité attendue. Un sous-système peut disposer de plusieurs canaux.

NOTE 2 Les codeurs, les sections d'alimentation et les sections de commande sont des exemples de sous-systèmes d'un PDS(SR) (voir la Figure 1).

**3.23**
**défaillance systématique**
défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

NOTE Citons comme exemples de causes de défaillances systématiques les erreurs humaines telles que:

- les erreurs de spécification des exigences de sécurité;
- les erreurs de conception, fabrication, installation, exploitation du matériel;
- les erreurs de conception, mise en œuvre du logiciel.

(CEI 61508-4:1998, définition 3.6.6)

**3.24**
**intégrité de sécurité systématique**
partie de l'intégrité de sécurité des systèmes relatifs à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux

(CEI 61508-4:1998, définition 3.5.4)

NOTE L'intégrité de sécurité systématique ne peut normalement pas être quantifiée.

**3.25**
**validation**
confirmation, par examen et apport de preuves tangibles, que les exigences particulières pour un usage spécifique prévu sont satisfaites

(CEI 61508-4:1998, définition 3.8.2)

NOTE La validation est l'activité qui consiste à démontrer que le PDS(SR), avant ou après installation, correspond en tout point à la spécification des exigences de sécurité.

**3.26**
**vérification**
confirmation, par examen et apport de preuves tangibles, que les exigences spécifiées ont été satisfaites

(CEI 61508-4:1998, définition 3.8.1)

## 4 Fonctions de sécurité désignées

### 4.1 Généralités

Cet article décrit les fonctions d'un PDS(SR) qui peuvent être désignées en relation avec la sécurité par le fournisseur du PDS(SR). Les fonctions de sécurité désignées dans cet article ne sont pas considérées comme une liste exhaustive. Dans certains cas, d'autres systèmes relatifs à la sécurité, externes au PDS(SR) (par exemple un frein mécanique), peuvent être nécessaires pour maintenir des conditions sûres lorsque la puissance électrique est supprimée.

Les mesures techniques exigées pour mettre en oeuvre ces fonctions dépendent de la capacité SIL et de l'exigence de probabilité de défaillance matérielle dangereuse, comme indiqué dans la spécification des exigences de sécurité. Les mesures techniques sont décrites à l'Article 6.

Chaque fonction de sécurité peut nécessiter une signalisation d'entrée et/ou de sortie sûre afin d'établir la communication nécessaire avec d'autres fonctions, sous-systèmes ou systèmes (qui ne sont pas forcément relatifs à la sécurité) ou de les activer. L'intégrité des

interfaces doit être incluse dans la détermination de la capacité SIL de la fonction de sécurité associée.

Certaines fonctions de sécurité réalisent uniquement des actions de contrôle, d'autres réalisent une commande de sécurité adéquate ou d'autres tâches. Par conséquent une distinction doit être faite entre:

– la réaction à la violation de limites (pertinent uniquement pour les fonctions de contrôle):

  la fonction de réaction quand une violation de limites est détectée durant le fonctionnement correct de la fonction de sécurité; et

– la fonction de réaction au défaut:

  la fonction de réaction quand des diagnostics détectent un défaut dans la fonction de sécurité.

Ces deux fonctions de réaction doivent prendre en compte les différents états de sécurité possibles de l'application.

En sélectionnant la fonction de réaction appropriée, il est nécessaire de considérer que des parties du PDS(SR) peuvent ne pas fonctionner.

Les exigences liées au temps, pour les actions requises suite à une détection de défaut, sont données par la spécification des exigences de sécurité (voir 5.4.2).

Les noms des fonctions de sécurité contiennent les mots «sûr» ou «sûre» afin d'indiquer que ces fonctions peuvent être utilisées dans une application relative à la sécurité sur les bases du jugement (c'est-à-dire par une analyse du risque) de cette application spécifique, conduisant à la pertinence et à l'intégrité des fonctions de sécurité devant être réalisées par le PDS(SR).

## 4.2 Fonctions de sécurité

### 4.2.1 Valeurs limites

Lorsqu'une fonction de sécurité dépend d'une ou de plusieurs valeurs limites pour un ou des paramètres, la ou les tolérances maximales de ces valeurs limites doivent être définies.

NOTE Il convient que la spécification de toute valeur limite prenne en compte un éventuel dépassement de la valeur limite en cas de violation de cette limite. Par exemple, il convient que la spécification de(s) valeur(s) pour la limite de position en 4.2.3.8 prenne en compte la(les) distance(s) maximale(s) permise(s) pour le dépassement.

Une fonction de sécurité particulière peut avoir une ou plusieurs valeurs limites spécifiées, qui peuvent être sélectionnées durant le fonctionnement.

### 4.2.2 Fonctions d'arrêt

#### 4.2.2.1 Généralités

Diverses méthodes d'arrêt sont applicables à chaque type de PDS.

Les exigences sur la commande d'initialisation d'une séquence d'arrêt et de maintien de ce mode une fois l'arrêt obtenu, sont spécifiques à l'application. Des commandes manuelles séparées et des raccordements distincts des circuits de commande peuvent être nécessaires pour atteindre les performances souhaitées des fonctions d'arrêt.

Il convient que les exigences particulières à la réalisation de l'arrêt soient spécifiées par le concepteur de l'installation. En pratique, les exemples suivants de fonctions d'arrêt sont souvent utilisés.

#### 4.2.2.2 Suppression sûre du couple (STO – safe torque off)

La puissance qui peut entraîner une rotation (ou un mouvement dans le cas d'un moteur linéaire), n'est pas appliquée au moteur. Le PDS(SR) ne fournit plus d'énergie au moteur qui peut générer du couple (ou une force dans le cas d'un moteur linéaire).

NOTE 1 Cette fonction de sécurité correspond à un arrêt non contrôlé conformément à l'arrêt de catégorie 0 de la CEI 60204-1.

NOTE 2 Cette fonction de sécurité peut être utilisée là où la suppression de la puissance est exigée afin d'éviter un démarrage intempestif.

NOTE 3 Dans des circonstances où des influences externes (par exemple, la chute de charges suspendues) sont présentes, des mesures complémentaires (par exemple, des freins mécaniques) peuvent être nécessaires afin de prévenir tout phénomène dangereux.

NOTE 4 Des moyens électroniques et des contacteurs ne sont pas adéquats pour la protection contre des chocs électriques et des mesures complémentaires peuvent être nécessaires pour assurer l'isolation.

#### 4.2.2.3 Arrêt sûr 1 (SS1)

Soit le PDS(SR):

a) initie et commande le taux de décélération du moteur dans des limites établies pour arrêter le moteur et initie la fonction STO (voir 4.2.2.2) lorsque la vitesse du moteur est en dessous d'une limite spécifiée; soit

b) initie et contrôle le taux de décélération du moteur dans des limites établies pour arrêter le moteur, et initie la fonction STO lorsque la vitesse du moteur est en dessous d'une limite spécifiée; soit

c) initie la décélération du moteur et initie la fonction STO après écoulement d'un temps spécifique.

NOTE Cette fonction de sécurité correspond à un arrêt contrôlé conformément à l'arrêt de catégorie 1 de la CEI 60204-1.

#### 4.2.2.4 Arrêt sûr 2 (SS2)

Soit le PDS(SR):

a) initie et commande le taux de décélération du moteur dans des limites établies pour arrêter le moteur et initie la fonction « maintien sûr à l'arrêt » (voir 4.2.3.1) lorsque la vitesse du moteur est en dessous d'une limite spécifiée; soit

b) initie et contrôle le taux de décélération du moteur dans des limites établies pour arrêter le moteur, et initie la fonction « maintien sûr à l'arrêt » lorsque la vitesse du moteur est en dessous d'une limite spécifiée; soit

c) initie la décélération du moteur et initie la fonction « maintien sûr à l'arrêt » après écoulement d'un temps spécifique.

NOTE Cette fonction de sécurité correspond à un arrêt contrôlé conformément à l'arrêt de catégorie 2 de la CEI 60204-1.

### 4.2.3 Autres fonctions de sécurité

#### 4.2.3.1 Maintien sûr à l'arrêt (SOS – safe operating stop)

La fonction SOS empêche le moteur de dévier plus que d'une quantité définie, à partir de la position d'arrêt. Le PDS(SR) fournit de l'énergie au moteur pour lui permettre de résister aux forces externes.

NOTE Cette description d'une fonction d'arrêt opérationnel est basée sur la mise en oeuvre de moyens dans le PDS(SR) sans freins externes (par exemple mécaniques).

#### 4.2.3.2 Limitation sûre de l'accélération (SLA – safely-limited acceleration)

La fonction SLA empêche le moteur de dépasser la limite spécifiée d'accélération.

#### 4.2.3.3 Fenêtre d'accélération sûre (SAR – safe acceleration range)

La fonction SAR maintient l'accélération et/ou la décélération du moteur dans des limites spécifiées.

#### 4.2.3.4 Limitation sûre de la vitesse (SLS – safely-limited speed)

La fonction SLS empêche le moteur de dépasser la limite spécifiée de la vitesse.

#### 4.2.3.5 Fenêtre de vitesse sûre (SSR – safe speed range)

La fonction SSR maintient la vitesse du moteur dans des limites spécifiées.

#### 4.2.3.6 Limitation sûre du couple (SLT – safely-limited torque)

La fonction SLT empêche le moteur de dépasser la limite spécifiée du couple (ou de la force, quand un moteur linéaire est utilisé).

#### 4.2.3.7 Gamme de couple sûre (STR – safe torque range)

La fonction STR maintient le couple moteur (ou la force, quand un moteur linéaire est utilisé) dans les limites spécifiées.

#### 4.2.3.8 Limitation sûre de la position (SLP – safely-limited position)

La fonction SLP empêche l'arbre moteur de dépasser la limite spécifiée de position.

#### 4.2.3.9 Limitation sûre de l'incrément (SLI – safely-limited increment)

La fonction SLI empêche l'arbre moteur de dépasser la limite spécifiée pour l'incrément de position.

NOTE Par cette fonction, le PDS(SR) commande les incréments de mouvements d'un moteur comme suit:

- un signal d'entrée (par exemple marche) initie un incrément de mouvement avec une course maximale spécifiée.
- après accomplissement de la course demandée pour cet incrément, le moteur est arrêté et est maintenu dans cet état, de façon appropriée à l'application.

#### 4.2.3.10 Sens de rotation sûr (SDI – safe direction)

La fonction SDI empêche l'arbre moteur de tourner dans le sens non prévu.

#### 4.2.3.11 Température moteur sûre (SMT – safe motor temperature)

La fonction SMT empêche la ou les températures moteur de dépasser une ou des limites hautes spécifiées.

#### 4.2.3.12 Commande sûre des freins (SBC – safe brake control)

La fonction SBC fournit un ou plusieurs signaux de sortie sûrs pour commander un ou plusieurs freins externes.

#### 4.2.3.13 Position sûre de la came (SCA – safe cam)

La fonction SCA fournit un signal de sortie sûr pour indiquer que la position de l'arbre moteur est à l'intérieur de la tolérance spécifiée.

#### 4.2.3.14 Contrôle sûr de la vitesse (SSM – safe speed monitor)

La fonction SSM fournit un signal de sortie sûr pour indiquer que la vitesse du moteur est en dessous d'une limite spécifiée.

## 5 Gestion de la sécurité fonctionnelle

### 5.1 Objectif

L'objectif de cet article est d'identifier les activités de gestion et d'information qui sont nécessaires au processus complet de développement du PDS(SR), afin de s'assurer que les objectifs de sécurité fonctionnelle sont satisfaits.

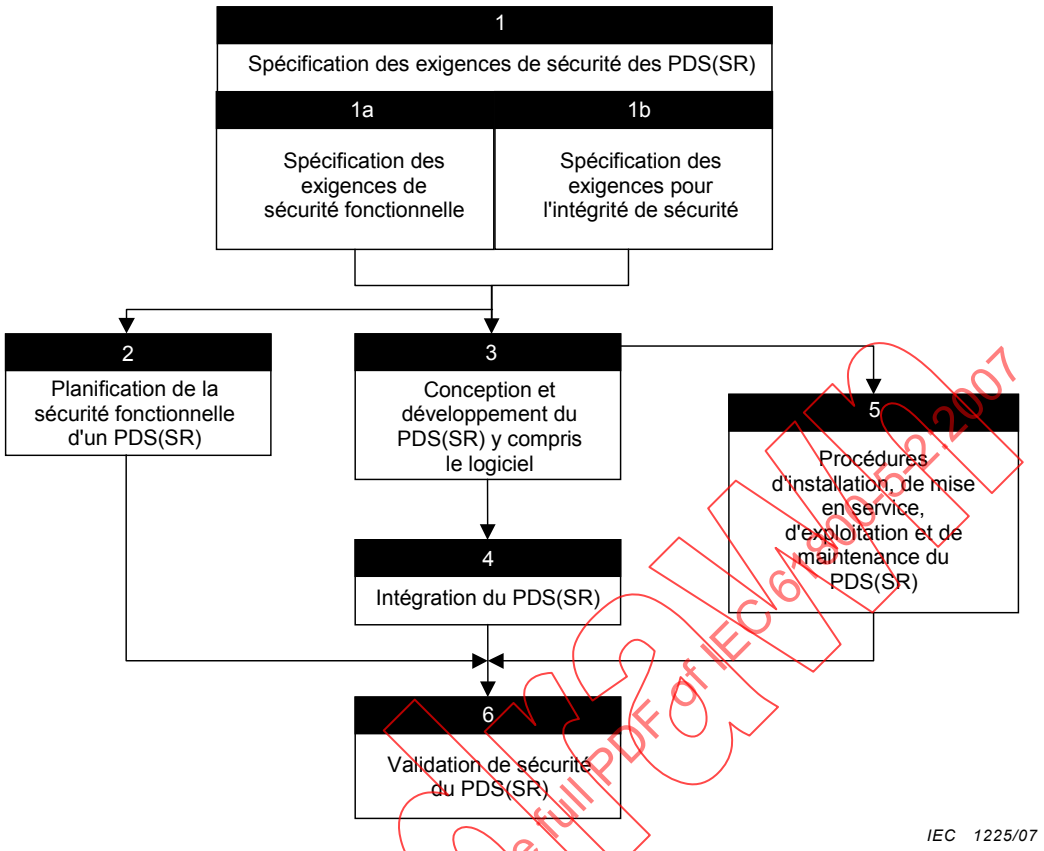
NOTE Cet article a pour unique objectif la réalisation de la sécurité fonctionnelle du PDS(SR) et est distinct et séparé des mesures de santé et de sécurité nécessaires à l'obtention de la sécurité sur le lieu de travail.

### 5.2 Cycle de vie du développement du PDS(SR)

La Figure 2 montre le cycle de vie du développement du PDS(SR) et des références croisées avec les paragraphes de la présente norme.

NOTE Ceci correspond à la phase de réalisation (phase 9) du cycle de vie globale de sécurité de la CEI 61508-1.

L'Annexe A présente ces informations sous la forme d'une table de tâches séquentielles.




| | | | |
|---|---|---|---|
| Pour la phase 1, voir 5.4 | Pour la phase 1a, voir 5.4.2 | Pour la phase 1b, voir 5.4.3 | Pour la phase 2, voir 5.3 |
| Pour la phase 3, voir l'Article 6 | Pour la phase 4, voir 6.5 | Pour la phase 5, voir l'Article 7 | Pour la phase 6, voir 8.3 |

**Figure 2 – Cycle de vie du développement du PDS(SR)**

### 5.3 Planification de la sécurité fonctionnelle

Un plan de sécurité fonctionnelle doit être généré et mis à jour si nécessaire tout au long du développement complet du PDS(SR). Le plan doit définir les activités exigées pour satisfaire aux Articles 5 à 10 et identifier les personnes, le ou les départements, ou la ou les organisations responsables pour accomplir ces activités. Le plan de sécurité fonctionnelle peut être incorporé dans le plan qualité global du PDS(SR) comme une partie intitulée «plan de sécurité fonctionnelle», ou bien il peut être un document séparé intitulé «plan de sécurité fonctionnelle».

En particulier, le plan de sécurité fonctionnelle doit considérer ou inclure les éléments suivants, de façon appropriée à la complexité du PDS(SR).

a) Génération de la spécification des exigences de sécurité (voir 5.4), incluant des facteurs tels que:
   - la considération des exigences provenant de guides et de normes pour des applications cibles spécifiques au PDS(SR);
   - le choix de méthodes pour l'évitement de fautes durant la génération de la spécification des exigences de sécurité;
   - le personnel responsable de la génération et de la maintenance des exigences de sécurité;

- le personnel responsable de la vérification de la spécification des exigences de sécurité;
- le processus pour la modification de la spécification des exigences de sécurité lorsque le développement a débuté.

b) Conception et développement de la ou des fonctions de sécurité dans le PDS(SR), incluant (le cas échéant) des facteurs tels que:

- la considération des guides et des normes de sécurité fonctionnelle applicables à la conception d'équipement incorporant le PDS(SR), dans une application cible, telle qu'un équipement de contrôle de processus ou une machine;
- la sélection des méthodes de développement de produit et de gestion de projet (voir B.1.1 de la CEI 61508-7:2000);
- le personnel responsable de la conception et du développement;
- la méthode de documentation de projet (voir B.1.2 de la CEI 61508-7:2000);
- l'application des techniques structurées de conception (voir B.3.2 de la CEI 61508-7:2000);
- l'utilisation d'outils de conception basés sur la simulation ou sur d'autres méthodes informatisées;
- la méthodologie de vérification de la conception;
- les techniques d'essais d'intégration et fonctionnels, les essais de régression et le personnel responsable;
- la gestion de modifications en conception (aussi bien matérielle que logicielle).

c) Un plan de vérification de la ou des fonctions de sécurité comprenant des facteurs tels que:

- la sélection des techniques et des stratégies de vérification;
- la sélection des activités de vérification;
- le personnel responsable de la vérification;
- la sélection et l'utilisation d'équipements pour les essais;
- l'évaluation des résultats de vérification obtenus par des essais et par l'équipement de vérification.

d) Un plan de validation de la ou des fonctions de sécurité comprenant:

- le personnel responsable des essais de validation;
- l'identification des modes de fonctionnement pertinents pour le PDS(SR);
- la stratégie technique pour la validation, par exemple des méthodes analytiques ou des essais statistiques;
- les critères d'acceptation;
- les actions à mettre en œuvre dans l'éventualité d'un échec à satisfaire aux critères d'acceptation.

e) Planification pour l'installation et la mise en service comprenant les éléments suivants (le cas échéant):

- les instructions spéciales pour l'installation et pour les étapes de l'installation;
- le personnel responsable de l'installation et de la mise en service;
- les activités de mise en service et les essais relatifs à la sécurité fonctionnelle;
- la méthodologie de collecte des résultats et des essais de mise en service;
- le mécanisme de résolution des problèmes et des échecs aux essais.

f) Planification de la documentation de l'utilisateur, relative à la sécurité, incluant:

- une liste d'informations significatives qui doivent être fournies pour la sécurité;
- le personnel responsable de la documentation de l'utilisateur;

– le processus de vérification pour s'assurer de la justesse de la documentation.

g) Lorsqu'une évaluation est exigée (voir l'Article 8 de la CEI 61508-1:1998), un plan d'évaluation de la sécurité fonctionnelle, comprenant les activités suivantes, doit être disponible:

– le domaine d'application de l'évaluation de la sécurité fonctionnelle;

– le personnel responsable de l'évaluation fonctionnelle;

– les étapes durant lesquelles les activités d'évaluation de la sécurité fonctionnelle sont tenues d'être réalisées (par exemple, après que la spécification des exigences de sécurité a été obtenue, après que le système de commande relatif à la sécurité a été conçu);

– les informations qui doivent être produites en tant que résultat de l'activité d'évaluation de la sécurité fonctionnelle;

– les ressources exigées pour finaliser l'activité d'évaluation de la sécurité fonctionnelle;

– le niveau d'indépendance de l'équipe d'évaluation;

– les moyens avec lesquels l'évaluation de la sécurité fonctionnelle doit être à nouveau validée après modifications du PDS(SR).

## 5.4 Spécification des exigences de sécurité (SRS) pour un PDS(SR)

### 5.4.1 Généralités

Une spécification des exigences de sécurité pour un PDS(SR) doit être documentée et doit comprendre:

– une spécification des exigences de sécurité fonctionnelle (voir 5.4.2); et

– une spécification des exigences d'intégrité de sécurité (voir 5.4.3).

Elles doivent être rédigées de telle façon qu'elles soient:

– claires;

– précises;

– non équivoques;

– réalisables;

– vérifiables;

– vérifiables par essai;

– actualisables.

Afin d'éviter des erreurs durant la compilation de ces spécifications, des mesures et des techniques appropriées doivent être employées (voir le Tableau B.1 de la CEI 61508-2:2000).

### 5.4.2 Spécification des exigences de sécurité fonctionnelle

La spécification des exigences de sécurité fonctionnelle doit fournir suffisamment d'exigences complètes et détaillées pour la conception et le développement du PDS(SR).

La spécification des exigences de sécurité fonctionnelle doit décrire, de façon appropriée:

a) toutes les fonctions de sécurité à réaliser;

b) tous les états possibles du PDS(SR) qui permettent d'atteindre un état sûr pour les applications présumées;

c) les modes de fonctionnement du PDS(SR) – par exemple, les réglages, le démarrage, la maintenance, le fonctionnement présumé normal;

d) tous les modes de comportement requis du PDS(SR);

e) les fonctions prioritaires parmi les fonctions actives simultanément et susceptibles d'entrer en conflit;

f) la ou les actions exigées lorsqu'une violation des limites est détectée durant le fonctionnement normal d'une fonction de sécurité (c'est-à-dire la réaction à la violation de limites (voir 4.1);

g) la ou les fonctions de réaction au défaut (voir 4.1 et 6.3);

h) le temps maximal de réaction au défaut nécessaire afin d'activer la réaction au défaut correspondante à réaliser avant qu'un phénomène dangereux ne se produise dans les applications présumées (nécessaire seulement si des *essais de diagnostic* sont utilisés pour atteindre la capacité SIL);

i) le temps de réponse maximal de chaque fonction relative à la sécurité (par exemple, les fonctions de réaction au défaut et de sécurité (voir 6.3);

j) l'importance de toutes les interactions entre matériel et logiciel – le cas échéant, les contraintes nécessaires entre le matériel et le logiciel doivent être identifiées et documentées;

NOTE Lorsque ces interactions ne sont pas connues avant la fin de la conception, seules les contraintes générales peuvent être mentionnées.

k) tous les moyens par lesquels l'opérateur interagit avec le PDS(SR) et qui peuvent avoir une influence sur les fonctions relatives à la sécurité (par exemple, les fonctions de réaction au défaut et de sécurité);

l) toutes les interfaces entre le PDS(SR) et tout autre système (associées directement à l'intérieur ou à l'extérieur de l'installation).

### 5.4.3 Spécification des exigences d'intégrité de sécurité

La spécification des exigences d'intégrité de sécurité relative à un PDS(SR) doit comprendre les éléments suivants:

a) pour chaque fonction relative à la sécurité (ou groupe de fonctions de sécurité utilisées simultanément), une capacité SIL ainsi qu'une probabilité maximale de défaillance matérielle dangereuse aléatoire;

NOTE 1 La capacité SIL est pertinente si le PDS(SR) est à considérer comme un composant qui met en œuvre une fonction de sécurité conjointement avec d'autres composants.

NOTE 2 Afin de tenir compte de la probabilité de *défaillance dangereuse* d'autres composants impliqués, la probabilité de défaillance matérielle dangereuse aléatoire du PDS(SR) est généralement tenue d'être inférieure à la mesure cible de défaillance associée au SIL attribué à la fonction de sécurité complète. Toutefois, elle peut également être supérieure si le PDS(SR) est à utiliser afin d'exécuter la fonction de sécurité dans une configuration redondante, avec d'autres composants.

NOTE 3 Lorsqu'un PDS(SR) exécute une fonction de sécurité entièrement à lui seul, la spécification des exigences d'intégrité de sécurité n'identifie par une capacité SIL mais un SIL.

NOTE 4 En cas d'utilisation de matériel courant pour exécuter plusieurs fonctions de sécurité simultanément, il convient de tenir compte seulement une fois de la probabilité de défaillance matérielle dangereuse aléatoire du matériel courant, lors de la détermination de la probabilité globale de défaillance matérielle dangereuse aléatoire.

NOTE 5 En ce qui concerne les PDS(SR) dotés de plusieurs axes, lorsqu'une fonction de sécurité est nécessaire sur plusieurs axes, il convient de tenir compte seulement une fois de la probabilité de défaillance matérielle dangereuse aléatoire du matériel courant, lors de la détermination de la probabilité globale de défaillance matérielle dangereuse aléatoire.

b) les conditions extrêmes de tout environnement (y compris l'électromagnétisme) auxquelles le PDS(SR) risque d'être soumis lors de son stockage, son transport, ses essais, son installation, sa mise en service, son fonctionnement et sa maintenance;

NOTE Cette information peut avoir été obtenue pour satisfaire aux exigences de la CEI 61800-1, la CEI 61800-2 ou la CEI 61800-4. Dans ce cas, il n'est pas nécessaire d'apporter d'autres précisions.

c) toute exigence relative à l'immunité électromagnétique accrue (voir 6.2.5).

# 6 Exigences relatives à la conception et au développement d'un PDS(SR)

## 6.1 Exigences générales

### 6.1.1 Modification de l'état de fonctionnement

Toute modification de l'état de fonctionnement d'un PDS(SR) susceptible d'entraîner une situation dangereuse (par exemple, à cause d'un démarrage intempestif) ne doit être initiée qu'en réponse à une action voulue par l'opérateur.

NOTE Par exemple, il convient que toute défaillance d'un PDS(SR) qui est en état d'attente ne puisse entraîner de démarrage intempestif des éléments des machines et/ou de l'usine.

### 6.1.2 Normes de conception

Le PDS(SR) doit être conçu conformément à la CEI 61800-5-1 et, le cas échéant, conformément aux autres normes pertinentes de la série CEI 61800.

### 6.1.3 Réalisation

Le PDS(SR) doit être réalisé conformément à la spécification des exigences de sécurité (voir 5.4).

### 6.1.4 Intégrité de sécurité et détection de défaut

Le PDS(SR) doit être conforme à l'ensemble des spécifications données de a) à c), à savoir:

a) les exigences relatives à l'intégrité de sécurité du matériel, notamment:
   - les contraintes architecturales imposées à l'intégrité de sécurité du matériel (voir 6.2.2), et
   - les exigences relatives à la probabilité de défaillance matérielle dangereuse aléatoire par heure (voir 6.2.1);

b) les exigences relatives à l'intégrité de sécurité systématique, notamment:
   - les exigences relatives à l'évitement des défaillances (voir 6.2.4.1) ainsi que les exigences relatives à la maîtrise des défauts systématiques (voir 6.2.4.2), ou
   - les preuves que les composants sont "éprouvés par une utilisation ultérieure". Dans ce cas, les composants doivent répondre aux exigences de la CEI 61508-2 qui s'appliquent;

c) les exigences relatives au comportement à adopter suite à la détection d'un défaut (voir 6.3).

### 6.1.5 Fonctions de sécurité et fonctions non relatives à la sécurité

Lorsqu'un PDS(SR) est tenu d'exécuter à la fois une fonction de sécurité et une fonction non relative à la sécurité, l'ensemble de son matériel et de son logiciel doit alors être traité comme relatif à la sécurité, sauf s'il peut être démontré que la mise en œuvre de la fonction de sécurité et de la fonction non relative à la sécurité est suffisamment indépendante (c'est-à-dire que la défaillance d'une fonction non relative à la sécurité quelconque n'entraîne aucune *défaillance dangereuse* des fonctions relatives à la sécurité).

NOTE Il est admis d'établir que l'indépendance est suffisante en montrant que la probabilité de défaillance dépendante entre les parties relatives à la sécurité et les parties non relatives à la sécurité est suffisamment faible en comparaison à la probabilité de *défaillance dangereuse* avec le niveau d'intégrité de sécurité le plus élevé associé aux fonctions de sécurité impliquées.

### 6.1.6 SIL à considérer

Les exigences relatives aux matériels et logiciels doivent être déterminées selon le niveau d'intégrité de sécurité de la fonction de sécurité dotée du niveau d'intégrité de sécurité le plus

élevé, sauf s'il peut être démontré que la mise en œuvre des fonctions de sécurité des différents niveaux d'intégrité de sécurité est suffisamment indépendante.

NOTE Il est admis d'établir que l'indépendance est suffisante en montrant que la probabilité de défaillance dépendante entre les parties appliquant des fonctions de sécurité de niveaux d'intégrité différents est suffisamment faible en comparaison à la probabilité de *défaillance dangereuse* avec le niveau d'intégrité de sécurité le plus élevé associé aux fonctions de sécurité impliquées.

### 6.1.7 Exigences logicielles

Si un logiciel est utilisé pour mettre en œuvre une fonction de sécurité du PDS(SR) doté d'un SIL ou d'une capacité SIL spécifique (voir 5.4.3), ce logiciel doit alors être mis en oeuvre conformément aux exigences définies dans la CEI 61508-3, relatives à ce SIL spécifique.

### 6.1.8 Revue des exigences

Les exigences relatives aux matériels et logiciels relatifs à la sécurité doivent être revues, afin de s'assurer qu'elles sont spécifiées comme il convient. Les points suivants en particulier doivent être pris en considération:

a) les fonctions de sécurité;

b) les exigences d'intégrité de sécurité;

c) les interfaces des équipements et des opérateurs.

### 6.1.9 Documentation de conception

Outre la documentation relative à la conception et à la réalisation, la documentation de conception du PDS(SR) doit indiquer les techniques et mesures utilisées pour obtenir le SIL revendiqué (par exemple, l'analyse des modes de défaillance et de leurs effets, l'analyse par arbre de panne).

## 6.2 Exigences relatives à la conception du PDS(SR)

### 6.2.1 Exigences relatives à la probabilité de défaillance matérielle dangereuse aléatoire par heure (PFH)

#### 6.2.1.1 Exigences générales

##### 6.2.1.1.1 PFH pour chaque fonction de sécurité

La PFH de chaque fonction de sécurité (ou groupe de fonctions de sécurité utilisées simultanément) à respecter par le PDS(SR), selon l'estimation donnée en 6.2.1.1.2 et dans l'Annexe B, doit être inférieure ou égale à la mesure cible de défaillance (voir le Tableau 2), comme indiqué dans la spécification des exigences d'intégrité de sécurité (voir 5.4.3).

La valeur de PFH, telle que définie par le SIL, se rapporte à une fonction de sécurité complète. Si un PDS(SR) est conçu pour ne réaliser qu'une partie d'une fonction de sécurité au sein d'un système de commande relatif à la sécurité, il convient alors que la PFH de l'entraînement soit suffisamment inférieure à la valeur définie par le SIL.

NOTE 1 La mesure cible de défaillance, exprimée en PFH, est déterminée par le SIL de la fonction de sécurité (voir le Tableau 3 de la CEI 61508-1:1998), sauf si l'une des exigences de la spécification des exigences d'intégrité de sécurité du PDS(SR) (voir 5.4.3) précise que la fonction de sécurité doit respecter une mesure cible de défaillance spécifique, au lieu d'un SIL spécifique.

**Tableau 2 – Niveaux d'intégrité de sécurité: mesures cibles de défaillance de la fonction de sécurité d'un PDS(SR)**

| Niveau d'intégrité de sécurité | PFH |
|---|---|
| 3 | $\geq 10^{-8}$ à $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ à $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ à $< 10^{-5}$ |
| NOTE La PFH est parfois appelée fréquence de *défaillance dangereuse* ou taux de *défaillance dangereuse*, en unités de *défaillances dangereuses* par heure. | |

La PFH doit être estimée séparément pour chaque fonction de sécurité (ou groupe de fonctions de sécurité utilisées simultanément) du PDS(SR).

NOTE 2 Il peut exister des fonctions de sécurité différentes pour des composants communs et/ou uniques. La PFH est alors différente pour chaque fonction de sécurité (ou groupe de fonctions de sécurité utilisées simultanément).

NOTE 3 Il existe plusieurs méthodes de modélisation. Le choix relatif à la méthode la plus appropriée incombe à l'analyste, ce choix dépend des circonstances. Les méthodes possibles sont, entre autres:

- analyse par arbre de panne (voir la CEI 61025);
- modèles de Markov (voir la CEI 61165);
- blocs diagrammes de fiabilité (voir la CEI 61078).

Voir également la CEI 60300-3-1.

NOTE 4 La durée moyenne de panne (voir le VEI 191-13-08) prise en considération dans le modèle de fiabilité nécessite la prise en compte des intervalles des essais de diagnostic et des essais périodiques, du temps de réparation, de tout autre délai précédant la restauration et de la durée de mission.

NOTE 5 Les défaillances dues aux effets de cause commune et aux processus de communication des données peuvent provenir d'effets autres que les défaillances réelles des composants du matériel (par exemple, les erreurs de décodage). Toutefois, pour les besoins de la présente norme, les défaillances de ce type sont considérées comme des défaillances matérielles aléatoires. (Voir l'Annexe D de la CEI 61508-6:2000).

NOTE 6 L'Annexe B de la CEI 61508-6:2000 décrit une approche simplifiée qu'il est admis d'utiliser pour évaluer la probabilité de *défaillance dangereuse* d'une fonction de sécurité à cause d'une défaillance matérielle aléatoire, dans le but de déterminer si une architecture respecte la mesure cible de défaillance requise.

#### 6.2.1.1.2 Estimation de la PFH

La PFH de chaque fonction de sécurité (ou groupe de fonctions de sécurité utilisées simultanément) à réaliser par le PDS(SR), à cause d'une défaillance matérielle aléatoire, doit être estimée conformément à l'Annexe A de la CEI 61508-2:2000 et en tenant compte des éléments suivants:

a) l'architecture du PDS(SR), car elle dépend de chaque fonction de sécurité étudiée;

b) le taux de défaillance estimé de chaque sous-système du PDS(SR), dans tous les modes susceptibles d'entraîner une *défaillance dangereuse* du PDS(SR), mais qui sont détectés par les *essais de diagnostic*;

c) le taux de défaillance estimé de chaque sous-système du PDS(SR), dans tous les modes susceptibles d'entraîner une *défaillance dangereuse* du PDS(SR), mais qui ne sont pas détectés par les *essais de diagnostic;*

d) la susceptibilité du PDS(SR) aux *défaillances de cause commune* (voir l'Annexe D de la CEI 61508-6:2000);

e) la *couverture du diagnostic* (DC) des *essais de diagnostic* (déterminée selon les Annexes A et C de la CEI 61508-2:2000), ainsi que l'intervalle associé aux *essais de diagnostic*;

NOTE 1 Au moment de déterminer l'intervalle des *essais de diagnostic*, il est nécessaire de prendre en considération les intervalles entre chaque essai contribuant à la *couverture du diagnostic*.

f) les intervalles entre la réalisation des essais périodiques, afin de révéler d'éventuelles défaillances dangereuses qui ne sont pas détectées par les *essais de diagnostic*;

NOTE 2 Dans la pratique, il peut s'avérer difficile de mettre en place des essais périodiques pour certaines pièces du PDS(SR). Dans ces cas-là, la durée de mission de ces pièces ou du PDS(SR) lui-même peut servir d'intervalle d'essais périodiques. Il convient de noter qu'une durée de mission de 20 ans peut être requise pour de nombreuses applications de machines.

g) les temps de réparation des défaillances détectées;

NOTE 3 Le temps de réparation comprend une partie de la durée moyenne de panne (voir le VEI 191-13-08), qui inclut également le temps nécessaire pour détecter une défaillance, ainsi que toute période au cours de laquelle aucune réparation n'est possible (l'Annexe B de la CEI 61508-6:2000 donne un exemple de la façon d'utiliser la durée moyenne de panne pour calculer la probabilité de défaillance). Dans les cas où la réparation ne peut être effectuée qu'au cours d'une période spécifique, par exemple alors que l'EUC est hors tension ou dans un état sûr, il est particulièrement important de bien prendre en compte la période rendant toute réparation impossible, surtout lorsque celle-ci est longue.

h) la probabilité de *défaillance dangereuse* de tout processus de communication des données (voir 6.4).

#### 6.2.1.1.3 Données relatives aux taux de défaillance

Les données relatives aux taux de défaillance des composants doivent être obtenues à partir des éléments suivants:

- une source reconnue; ou
- des estimations basées sur les composants considérés comme "éprouvés par une utilisation ultérieure" (voir de 7.4.7.6 à 7.4.7.12 de la CEI 61508-2:2000).

Il convient d'utiliser la température moyenne de fonctionnement attendue pour un composant lors de l'estimation de son taux de défaillance.

Il convient que le niveau de confiance de toutes les données relatives aux taux de défaillance utilisées soit égal à au moins 60 %.

NOTE 1 Les données peuvent être déduites des données publiées dans certaines sources industrielles (voir l'Annexe C).

NOTE 2 Si les données relatives aux défaillances spécifiques à un site sont connues, ces données sont à privilégier. A défaut, les données génériques peuvent être utilisées.

NOTE 3 Bien que les méthodes d'estimation les plus probabilistes supposent un taux de défaillance constant, cela ne s'applique qu'à condition que le cycle de vie utile des composants ne soit pas dépassé. Au-delà de ce cycle de vie utile (sachant que la probabilité de défaillance augmente considérablement avec le temps), les résultats des méthodes de calcul les plus probabilistes ne sont donc plus représentatifs. Ainsi, il convient que toute estimation probabiliste comprenne une spécification du cycle de vie utile des composants. Ce dernier dépend en grande partie du composant lui-même et de ses conditions de fonctionnement, en particulier la température (les condensateurs électrolytiques par exemple peuvent y être très sensibles). L'expérience a permis de montrer que le cycle de vie utile est souvent compris entre 8 ans et 12 ans. Il peut néanmoins être bien plus court si les composants sont exploités à des valeurs proches de leurs limites spécifiées.

NOTE 4 Les listes de pannes données dans l'Annexe D peuvent être utilisées pour faciliter la détermination des modes de défaillance.

#### 6.2.1.1.4 Intervalle des *essais de diagnostic*

L'intervalle des *essais de diagnostic* de tout sous-système du PDS(SR) doit être tel que le PDS(SR) puisse satisfaire à l'exigence relative à la PFH (voir 6.2.1.1.1).

Lorsqu'une panne dangereuse peut entraîner une perte de la fonction de sécurité, il est nécessaire de détecter cette panne dans les limites de couverture de diagnostic et d'initier une réaction au défaut afin de prévenir tout danger. Les fonctions de diagnostic et de réaction au défaut doivent être exécutées conformément au temps maximal de réaction au défaut qui est spécifié (voir 5.4.2).

#### 6.2.1.1.5 Intervalle des essais pour une tolérance zéro aux défauts du matériel

Pour tout sous-système d'un PDS(SR) présentant une tolérance zéro aux défauts du matériel, dont dépend entièrement une fonction de sécurité, l'intervalle des *essais de diagnostic* doit être tel que la somme de l'intervalle des *essais de diagnostic* et de la durée de réalisation d'une action donnée (fonction de réaction au défaut) pour atteindre ou maintenir un état sûr soit inférieure au temps maximal de réaction au défaut qui est spécifié.

### 6.2.2 Contraintes architecturales

#### 6.2.2.1 Limitations du SIL

Dans le contexte de l'intégrité de sécurité du matériel, le niveau d'intégrité de sécurité le plus élevé qui peut être annoncé pour une fonction de sécurité donnée est limité par la tolérance aux défauts du matériel et la proportion de défaillances en sécurité des sous-systèmes d'un PDS(SR) qui réalisent la fonction de sécurité. Une tolérance aux défauts du matériel *N* signifie que *N*+1 défauts risquent d'entraîner la perte de la fonction de sécurité. Le Tableau 3 et le Tableau 4 spécifient le niveau d'intégrité de sécurité le plus élevé qui peut être annoncé pour une fonction de sécurité qui utilise un sous-système, en tenant compte de la tolérance aux défauts du matériel et de la proportion de défaillances en sécurité de ce sous-système (voir l'Annexe C de la CEI 61508-2:2000). Les exigences du Tableau 3 ou du Tableau 4, selon celui qui convient, doivent être appliquées à chaque sous-système réalisant une fonction de sécurité et, de ce fait, à chaque partie du PDS(SR). Les paragraphes 6.2.2.2.1 et 6.2.2.2.2 spécifient, parmi le Tableau 3 ou le Tableau 4 celui qui s'applique à un sous-système particulier. Conformément à ces exigences,

a) lors de la détermination de la tolérance aux défauts du matériel, aucune autre mesure susceptible de contrôler les effets des défauts (telles que les diagnostics) ne doit être prise en compte;

b) lorsqu'un défaut est la cause directe d'un ou de plusieurs défauts subséquents, ces derniers sont considérés comme un défaut unique;

c) lors de la détermination de la tolérance aux défauts du matériel, certains défauts peuvent être exclus, à la condition que leur probabilité d'occurrence soit très faible par rapport aux exigences d'intégrité de sécurité du sous-système. Toute exclusion de défauts doit être justifiée et documentée (voir la Note 3).

NOTE 1 Les contraintes architecturales ont été incluses afin d'obtenir une architecture suffisamment robuste, en tenant compte du niveau de complexité du sous-système. Le niveau d'intégrité de sécurité du matériel du PDS(SR) qui est obtenu en appliquant ces exigences correspond au maximum qu'il est permis d'annoncer, même si dans certains cas, un niveau d'intégrité de sécurité supérieur pourrait théoriquement être calculé si une approche uniquement mathématique avait été adoptée pour le PDS(SR).

NOTE 2 L'architecture du sous-système obtenue pour respecter les exigences de tolérance aux défauts du matériel est celle qui est utilisée dans des conditions de fonctionnement normal. Les exigences de tolérance aux défauts peuvent être assouplies lorsque le PDS(SR) est en cours de réparation en ligne. Toutefois, il faut que les paramètres clés relatifs à tout assouplissement éventuel aient été préalablement évalués (par exemple, en comparant la durée moyenne de panne à la probabilité d'une demande).

NOTE 3 C'est une étape nécessaire car s'il est clair qu'un composant possède une très faible probabilité de défaillance, d'après les propriétés inhérentes à sa conception et à son élaboration (par exemple, une liaison mécanique d'actionneur), il est alors normal de considérer qu'il est nécessaire de limiter (en fonction de la tolérance aux défauts du matériel) l'intégrité de sécurité de toute fonction de sécurité utilisant le composant.

#### 6.2.2.2 Sous-systèmes de Type A et de Type B

##### 6.2.2.2.1 Type A

Un sous-système peut être considéré de type A si, pour les composants nécessaires à la réussite de la fonction de sécurité:

a) les modes de défaillance de tous les composants qui le composent sont bien définis; et

b) le comportement du sous-système dans des conditions de défaut peut être entièrement déterminé; et

c) il existe suffisamment de données de défaillance fiables, obtenues à partir d'expériences sur le terrain, pour démontrer que les taux de défaillance annoncés pour les *défaillances dangereuses* détectées et non détectées sont respectés.

NOTE L'Annexe D énumère les défauts exclus et les défauts qui peuvent être pris en considération.

#### 6.2.2.2.2 Type B

Un sous-système doit être considéré de type B si, pour les composants nécessaires à la réussite de la fonction de sécurité, un ou plusieurs des critères de 6.2.2.2.1 ne sont pas satisfaits.

NOTE 1 Ainsi, si au moins l'un des composants d'un sous-système satisfait aux conditions correspondant à un sous-système de type B, l'ensemble du sous-système doit alors être considéré de type B, et non de type A.

NOTE 2 À titre d'exemple, la section de commande constituée notamment de micro-contrôleurs est considérée comme un sous-système de type B.

NOTE 3 L'Annexe D énumère les défauts exclus et les défauts qui peuvent être pris en considération.

### 6.2.2.3 Contraintes architecturales

Les contraintes architecturales du Tableau 3 ou du Tableau 4 doivent être appliquées: le Tableau 3 s'applique à tout sous-système de type A dont est constitué le PDS(SR); le Tableau 4 s'applique à tout sous-système de type B dont est constitué le PDS(SR).

**Tableau 3 – Intégrité de sécurité du matériel: contraintes architecturales des sous-systèmes de type A relatifs à la sécurité**

| Proportion de défaillances en sécurité [a] | Tolérance aux défauts du matériel N (voir 6.2.2.1) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | SIL1 | SIL2 | SIL3 |
| 60 % à < 90 % | SIL2 | SIL3 | SIL3 [b] |
| 90 % à < 99 % | SIL3 | SIL3 [b] | SIL3 [b] |
| ≥ 99 % | SIL3 | SIL3 [b] | SIL3 [b] |

[a] Voir 6.2.3 pour plus de détails sur la façon d'estimer la proportion de défaillances en sécurité.

[b] La présente partie de la CEI 61800 ne s'applique qu'aux fonctions de sécurité dotées d'un SIL inférieur à SIL 3. En ce qui concerne les fonctions de sécurité de SIL 4, il convient d'appliquer les exigences de la CEI 61508.

**Tableau 4 – Intégrité de sécurité du matériel: contraintes architecturales des sous-systèmes de type B relatifs à la sécurité**

| Proportion de défaillances en sécurité [a] | Tolérance aux défauts du matériel N (voir 6.2.2.1) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | Interdite | SIL1 | SIL2 |
| 60 % à < 90 % | SIL1 | SIL2 | SIL3 |
| 90 % à < 99% | SIL2 | SIL3 | SIL3 [b] |
| ≥ 99 % | SIL3 | SIL3 [b] | SIL3 [b] |

[a] Voir 6.2.3 pour plus de détails sur la façon d'estimer la proportion de défaillances en sécurité.

[b] La présente partie de la CEI 61800 ne s'applique qu'aux fonctions de sécurité dotées d'un SIL inférieur à SIL 3. En ce qui concerne les fonctions de sécurité de SIL 4, il convient d'appliquer les exigences de la CEI 61508.

### 6.2.3 Estimation de la proportion de défaillances en sécurité (SFF)

#### 6.2.3.1 Méthodes d'analyse

Pour estimer la SFF d'un sous-système, une analyse (par exemple, une analyse par arbre de panne ou une analyse des modes de défaillance et de leurs effets) doit être effectuée afin d'identifier tous les défauts significatifs, ainsi que leurs modes de défaillance correspondants. La probabilité de chaque mode de défaillance du sous-système doit être déterminée en s'appuyant sur la probabilité du ou des défauts associés.

#### 6.2.3.2 Bases de données

L'estimation de la SFF doit s'appuyer soit:

- sur des données relatives aux taux de défaillance significatives d'un point de vue statistique, obtenues à partir d'expériences sur le terrain; soit
- sur des données relatives aux défaillances des composants, obtenues grâce à une source reconnue.

Voir également 6.2.1.1.3.

NOTE Voir l'Annexe C pour une liste informative des sources connues.

#### 6.2.3.3 Relais de sécurité

Dans un sous-système doté d'une tolérance aux défauts du matériel de zéro, lorsqu'un relais de sécurité à contact de signal de retour guidé positivement est utilisé pour fournir une fonction de sécurité et une *couverture de diagnostic* de cette fonction, l'intégrité de sécurité due aux contraintes architecturales de ce sous-système est définie selon une limite de revendication du SIL 2.

#### 6.2.3.4 Calcul de la SFF

La proportion de défaillances en sécurité d'un sous-système doit être calculée à l'aide des Annexes A et C de la CEI 61508-2:2000.

### 6.2.4 Exigences relatives à l'intégrité de sécurité systématique d'un PDS(SR) et des sous-systèmes d'un PDS(SR)

#### 6.2.4.1 Exigences relatives à l'évitement des défaillances

##### 6.2.4.1.1 Généralités

Des techniques et mesures doivent être utilisées pour réduire le plus possible la présence de défauts lors de la conception et du développement du matériel du PDS(SR).

Des essais, tels que prévus en 6.2.4.1.4, doivent être effectués. Voir également l'Article 9.

##### 6.2.4.1.2 Choix des méthodes de conception

Conformément au niveau d'intégrité de sécurité exigé, la méthode de conception choisie doit favoriser les éléments suivants:

a) transparence, modularité et autres caractéristiques permettant de simplifier au maximum et d'améliorer la compréhension de la conception;

b) spécification claire et précise
   - de la fonctionnalité,
   - des interfaces des sous-systèmes,
   - du séquencement et des informations temporelles,

- de la simultanéité et de la synchronisation,

c) documentation claire et précise et communication d'informations;

d) vérification et validation.

#### 6.2.4.1.3 Mesures de conception

Les mesures de conception suivantes doivent être appliquées.

a) Conception correcte du PDS(SR) et/ou des sous-systèmes, y compris
   - l'utilisation de composants conformes aux spécifications des fabricants, concernant par exemple la température, le chargement, l'alimentation, la puissance assignée et les paramètres de temporisation;
   - le déclassement des paramètres de conception afin d'améliorer la fiabilité si nécessaire, dans le but d'atteindre les taux de défaillance cibles;
   - la combinaison et le montage corrects des sous-systèmes, concernant par exemple le câblage et les interconnexions;
   - le recours à des revues et inspections afin de détecter d'éventuels défauts de conception suffisamment tôt.

b) Compatibilité:
   - Utiliser des sous-systèmes dont les caractéristiques de fonctionnement sont compatibles.

c) Résistance aux conditions environnementales spécifiées:
   - Concevoir le PDS(SR) de sorte que son fonctionnement soit sûr dans tous les environnements spécifiés, par exemple en termes de température, d'humidité, de vibrations, de phénomènes électromagnétiques, de degré de pollution, de catégorie de surtension, d'altitude.

#### 6.2.4.1.4 Planification des essais

Lors de la conception, les différents types d'essais suivants doivent être planifiés selon les besoins:

a) essai des sous-systèmes;

b) essai d'intégration;

c) essai de validation;

d) essai de configuration (voir 7.1).

La documentation relative à la planification des essais doit préciser les points suivants:

e) les types d'essais à effectuer et les procédures à suivre;

f) l'environnement, les outils, la configuration et les programmes d'essai;

g) les critères de réussite/d'échec.

Des outils d'essais automatiques et des outils de développement intégrés doivent être utilisés le cas échéant.

NOTE L'intégrité de ce type d'outils peut être démontrée grâce à des essais spécifiques, à une expérience d'utilisation longue et satisfaisante ou à une vérification indépendante de leurs résultats avec le PDS(SR) en cours de conception.

#### 6.2.4.1.5 Exigences relatives à la maintenance de la conception

Un processus relatif à la maintenance et aux nouveaux essais de la conception doit être défini lors de la phase de conception, afin de s'assurer que l'intégrité de sécurité du PDS(SR) continue à respecter le niveau exigé après les révisions de sa conception.

#### 6.2.4.2 Exigences relatives à la maîtrise des défauts systématiques

##### 6.2.4.2.1 Caractéristiques de conception

Pour la maîtrise des défauts systématiques, la conception doit posséder les caractéristiques permettant au PDS(SR) et à ses sous-systèmes d'éviter les conséquentes suivantes:

a) défauts de conception résiduels du matériel, sauf si l'éventualité de défauts de conception du matériel peut être exclue en appliquant l'Article A.3 et le Tableau A.16 de la CEI 61508-2:2000;

b) contraintes environnementales, notamment les perturbations électromagnétiques, en appliquant l'Article A.3 et le Tableau A.17 de la CEI 61508-2:2000;

c) erreurs imputables à l'opérateur du PDS(SR) (voir A.3 et le Tableau A.18 de la CEI 61508-2:2000);

d) défauts de conception résiduels du logiciel (voir 7.4.3 de la CEI 61508-3:1998 et le tableau associé);

e) erreurs et autres effets causés par tout processus de communication de données (voir 6.4).

##### 6.2.4.2.2 Testabilité et maintenabilité

La testabilité ainsi que la maintenabilité doivent être prises en compte lors des activités de conception et de développement, afin de faciliter la mise en œuvre de ces propriétés dans le PDS(SR) final.

##### 6.2.4.2.3 Contraintes humaines

La conception du PDS(SR) doit prendre en compte les capacités et limites humaines et être adaptée aux tâches qui sont affectées aux opérateurs et au personnel de maintenance. La conception des interfaces des opérateurs doit permettre une utilisation pratique pour l'homme et elle doit tenir compte du niveau probable de formation ou de connaissance des opérateurs.

##### 6.2.4.2.4 Protection contre les modifications non intentionnelles

Le PDS(SR) doit intégrer des mesures visant à le protéger (ou à faciliter sa protection) contre toute modification non intentionnelle de logiciel, matériel, paramétrage et configuration relatifs à la sécurité du PDS(SR).

NOTE Voir B.4.8 de la CEI 61508-7:2000.

##### 6.2.4.2.5 Reconnaissance d'entrée et erreurs de l'opérateur

La conception du PDS(SR) doit intégrer la reconnaissance d'entrée afin de maîtriser les défaillances de fonctionnement. La conception doit également permettre la protection contre d'éventuelles erreurs de l'opérateur (liées aux fonctions de sécurité du PDS(SR)) au moyen de vérifications de plausibilité.

NOTE Voir B.4.6 et B.4.9 de la CEI 61508-7:2000.

##### 6.2.4.2.6 Perte de l'alimentation électrique

Le PDS(SR) doit être spécifié et conçu en tenant compte des effets d'une perte d'alimentation électrique.

### 6.2.5 Exigence relative à l'immunité électromagnétique d'un PDS(SR)

#### 6.2.5.1 Généralités

Le critère de performance qui doit être appliqué lors de la réalisation d'essais d'immunité électromagnétique sur le PDS(SR) est spécifié en 6.2.5.3. Ce critère ne s'applique pas aux fonctions normales (non relatives à la sécurité) de l'équipement (la compatibilité électromagnétique (CEM) fonctionnelle du PDS(SR) est atteinte s'il répond aux exigences de la CEI 61800-3).

#### 6.2.5.2 Environnement présumé

L'environnement électromagnétique spécifié ou anticipé pour l'usage présumé d'un PDS(SR) doit être utilisé afin de déterminer les niveaux d'essai d'immunité électromagnétique.

Lorsque l'environnement électromagnétique est inconnu du fabricant du PDS(SR), les niveaux d'essai de la CEI 61800-3 doivent être utilisés pour les essais d'immunité.

#### 6.2.5.3 Critère de performance

Le critère de performance suivant doit être satisfait par les fonctions de sécurité correspondantes d'un PDS(SR). En ce qui concerne les fonctions du PDS(SR) qui ne sont pas relatives à la sécurité, leurs caractéristiques ne sont pas prises en compte mais le paragraphe 6.2.5.4 s'applique.

Fonctions du PDS(SR) prévues pour les applications de sécurité:

– aucune déviation hors des limites spécifiées pour la sécurité fonctionnelle, ou

– déviation temporaire ou permanente possible hors des limites spécifiées pour la sécurité fonctionnelle, si le PDS(SR) réagit à la perturbation électromagnétique de telle sorte qu'un état sûr défini du PDS(SR) soit maintenu ou atteint, conformément au temps maximal de réaction au défaut spécifié.

La dégradation permanente de la fonction de sécurité ou la destruction des composants est admise, à la condition qu'un état sûr soit maintenu ou atteint, conformément au temps maximal de réaction au défaut spécifié.

Ce critère s'applique à tous les phénomènes électromagnétiques qui peuvent être constatés lors de l'application présumée du PDS(SR).

#### 6.2.5.4 Introduction de phénomènes dangereux

Lorsqu'un essai d'immunité électromagnétique est effectué, aucune condition non sûre, ni phénomène dangereux ne doit être introduit par le PDS(SR).

#### 6.2.5.5 Vérification

Lors de la réalisation des essais d'immunité électromagnétique, les mesures d'atténuation spécifiées doivent être appliquées.

Selon l'analyse de l'environnement électromagnétique de l'application présumée du PDS(SR), pour vérifier l'immunité accrue (conformément aux exigences de la CEI 61508-2), soit:

- le cas échéant (selon le phénomène électromagnétique et le SIL exigé), augmenter le niveau de l'essai et/ou sa durée et/ou le nombre de cycles d'essai; soit
- vérifier l'efficacité de toute mesure d'atténuation supplémentaire (voir A.11.3 de la CEI 61508-7:2000) ayant été spécifiée.

### 6.3 Comportement sur détection de défaut

#### 6.3.1 Détection de défaut

Les défauts d'un PDS(SR) peuvent être détectés au moyen d'*essais de diagnostic*.

En cas de détection d'un défaut dangereux susceptible d'entraîner la perte de la fonction de sécurité, une fonction de réaction au défaut doit être initiée afin de prévenir tout phénomène dangereux. Les diagnostics et les fonctions de réaction au défaut doivent être réalisés conformément au temps maximal de réaction au défaut qui est spécifié.

#### 6.3.2 Tolérance aux défauts supérieure à zéro

La détection d'un défaut dangereux (grâce aux *essais de diagnostic* ou à tout autre moyen) dans tout sous-système doté d'une tolérance aux défauts du matériel supérieure à zéro doit avoir pour résultat soit:

a) une fonction de réaction au défaut, soit

b) l'isolement de la partie défectueuse du sous-système, afin de réussir à maintenir la sécurité du fonctionnement des machines et/ou des pièces d'usine, tandis que la partie défectueuse est en cours de réparation. Si la réparation n'est pas terminée selon la durée moyenne de panne (MTTR) présumée lors du calcul de la probabilité de défaillance matérielle dangereuse aléatoire (voir 6.2.1), une fonction de réaction au défaut doit alors être initiée.

#### 6.3.3 Tolérance zéro aux défauts

La détection d'un défaut dangereux (grâce aux *essais de diagnostic* ou à tout autre moyen) dans tout sous-système doté d'une tolérance aux défauts du matériel égale à zéro, dont la fonction de sécurité dépend entièrement, doit avoir pour résultat une fonction de réaction au défaut.

### 6.4 Exigences particulières relatives à la communication de données

En cas de recours à la communication de données lors de la mise en oeuvre d'une fonction de sécurité, la probabilité de défaillances non détectées au sein du processus de communication doit alors être estimée en tenant compte des erreurs de transmission, des répétitions, des suppressions, des insertions, du re-séquencement, de la corruption, des retards et des usurpations d'identité. Cette probabilité doit être prise en considération lors de l'estimation de la *PFH* de la fonction de sécurité due à des défaillances aléatoires (voir 6.2.1.1.2).

NOTE Le terme «usurpation d'identité» signifie que le véritable contenu d'un message n'a pas été correctement identifié. Par exemple, un message d'un composant non relatif à la sécurité est par erreur identifié comme un message d'un composant relatif à la sécurité.

Les mesures nécessaires pour assurer la mesure de défaillance exigée par le processus de communication doivent être mises en oeuvre conformément aux exigences de la CEI 61508-2 et de la CEI 61508-3. Deux approches sont ainsi possibles:

a) le canal de communication doit être conçu, mis en oeuvre et validé conformément à la CEI 61508 (nommé "canal blanc", voir la Figure 3 a)); ou

b) certaines parties du canal de communication ne sont ni conçues ni validées conformément à la CEI 61508 (nommé "canal noir", voir la Figure 3 b)). Dans ce cas, les mesures nécessaires pour assurer la performance de défaillance du processus de communication doivent être mises en oeuvre au niveau des composants relatifs à la sécurité du PDS(SR) qui sont connectés au canal de communication. La mise en oeuvre de cette mesure doit être conforme à la CEI 62280, le cas échéant.

En cas de recours à la communication de données pour échanger des données relatives à la sécurité avec des sous-systèmes externes au PDS(SR), les exigences ci-dessus s'appliquent au PDS(SR) ainsi qu'aux sous-systèmes concernés.

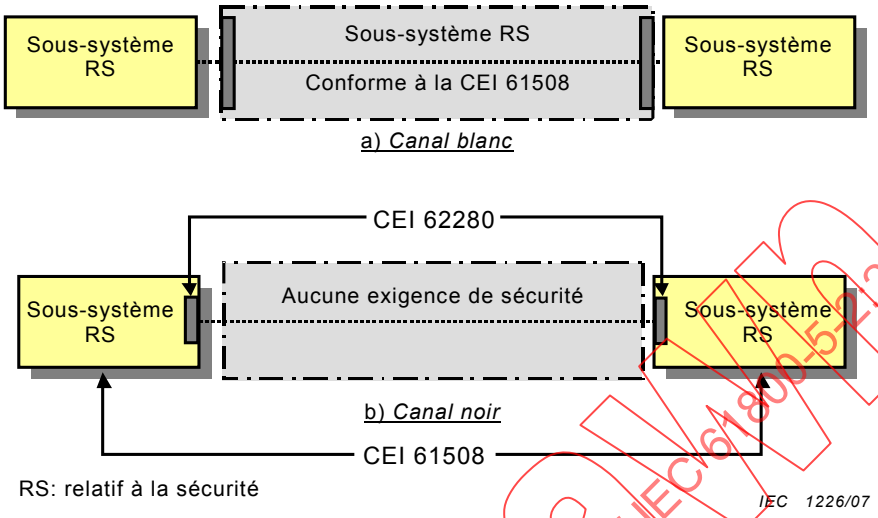



**Figure 3 – Architectures relatives à la communication de données: a) Canal blanc; b) Canal noir**

## 6.5 Exigences relatives à l'intégration et aux essais du PDS(SR)

### 6.5.1 Intégration matérielle

Le PDS(SR) doit être intégré selon la conception qui lui est spécifiée. Lors de l'intégration de tous les sous-systèmes et composants au PDS(SR), ce dernier doit être soumis à l'essai conformément aux essais d'intégration spécifiés. Ces essais sont spécifiés dans le plan de vérification. Ils doivent permettre de montrer que tous les modules sont correctement connectés de façon à réaliser leur fonction présumée, sans réaliser de fonction indésirable.

Les exigences relatives à l'intégration matérielle sont également satisfaites lorsque les essais de type du PDS(SR) sont réussis, conformément à 6.2.5 et à la CEI 61800-5-1, ainsi qu'à la CEI 61800-1, la CEI 61800-2 ou la CEI 61800-4 (selon le cas).

### 6.5.2 Intégration logicielle

L'intégration du module/de la partie de logiciel relative à la sécurité au PDS(SR) doit être effectuée conformément à la CEI 61508-3. Elle doit comporter les essais spécifiés dans le plan de vérification du logiciel, afin d'assurer la compatibilité du logiciel avec le matériel, de façon à satisfaire aux exigences fonctionnelles et de performances de sécurité.

NOTE Il n'est pas nécessaire de soumettre toutes les combinaisons d'entrée à des essais. L'essai de toutes les classes d'équivalence (voir B.5.2 de la CEI 61508-7:2000) peut suffire. Une analyse statique (voir B.6.4 de la CEI 61508-7:2000), une analyse dynamique (voir B.6.5 de la CEI 61508-7:2000) ou une analyse de défaillance (voir B.6.6 de la CEI 61508-7:2000) peut permettre de réduire les cas d'essais à un nombre acceptable.

### 6.5.3 Modifications pendant l'intégration

Pendant l'intégration, toute modification apportée au PDS(SR) doit faire l'objet d'une analyse d'impact qui doit permettre d'identifier tous les composants affectés, puis d'une vérification supplémentaire.

### 6.5.4 Essais d'intégration applicables

Le ou les essais d'intégration doivent être spécifiés dans un plan de vérification. Un essai fonctionnel doit être réalisé, lors duquel les données d'entrée ou valeurs établies qui définissent de façon appropriée le fonctionnement normal présumé sont données au PDS(SR). La fonction de sécurité est demandée (en activant par exemple la fonction STO ou la violation de limite de vitesse de la stabilité en ligne droite) et le fonctionnement constaté est étudié et comparé avec celui qui a été donné par la spécification. (Voir également l'Article 9).

### 6.5.5 Documentation relative aux essais

Lors des essais d'intégration du PDS(SR), les éléments suivants doivent être documentés:

a) la version du plan d'essai utilisé;

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

c) le type et la version du PDS(SR) soumis à essai;

d) les outils et équipements utilisés, ainsi que les données relatives à l'étalonnage;

e) les résultats de chaque essai;

f) tout écart entre les résultats attendus et les résultats obtenus.

## 7 Informations pour l'utilisation

### 7.1 Informations et instructions pour l'application sans risque d'un PDS(SR)

Les informations suivantes doivent être documentées par le fabricant et mises à la disposition de l'utilisateur.

a) Une spécification fonctionnelle pour chaque fonction et chaque interface disponible pour la mise en œuvre des fonctions de sécurité. Elle doit comporter les éléments suivants:
   - une description détaillée de la fonction de sécurité (y compris la ou les réactions en cas de dépassement d'une limite);
   - la fonction de réaction au défaut;
   - le délai de réponse de chaque fonction de sécurité et des fonctions de réaction au défaut associées;
   - la ou les conditions (par exemple, le mode de fonctionnement) dans lesquelles la fonction de sécurité est conçue pour être active ou désactivée;
   - les fonctions les plus prioritaires parmi les fonctions actives simultanément et susceptibles d'entrer en conflit.

b) Les informations relatives à l'intégrité de sécurité de chaque fonction de sécurité, et notamment:
   - la *capacité* SIL;
   - la valeur de la PFH.

c) Une définition des conditions d'environnement et de fonctionnement (notamment électromagnétiques) dans lesquelles le PDS(SR) est conçu pour être utilisé (voir également la CEI 61800-1, la CEI 61800-2, la CEI 61800-4, la CEI 61800-3 et la CEI 61800-5-1). Cette définition doit envisager les aspects suivants: le stockage, le transport, l'installation, la mise en service, les essais, le fonctionnement et la maintenance.

d) Une mention des contraintes auxquelles est soumis le PDS(SR) en ce qui concerne les éléments suivants:
   - l'environnement auquel il convient de soumettre le PDS(SR) afin que les estimations des taux de défaillance restent valables;

- la durée de mission du PDS(SR) et les intervalles des essais périodiques, le cas échéant;
- les exigences relatives aux essais, à l'étalonnage et à la maintenance;
- les limites d'application du PDS(SR) auxquelles il convient de se conformer pour éviter toute défaillance systématique;
- la *capacité SIL* de chaque fonction de sécurité;
- toutes les informations permettant d'identifier la configuration matérielle et logicielle d'un PDS(SR) afin de permettre la gestion de la configuration, conformément aux indications spécifiées à l'Article 4.

e) Les informations relatives à l'installation et la mise en service (voir l'Article 6 de la CEI 61800-5-1:2003), notamment les réglages et les paramètres.

f) Les exigences relatives à l'essai de configuration des fonctions de sécurité, dans les cas où il est impossible de garantir l'intégrité des moyens de configuration d'une fonction de sécurité (par exemple, les outils de configuration PC).

L'essai de configuration est réalisé après la mise en service et après chaque modification d'une application spécifique, afin de garantir que les fonctions de sécurité du PDS(SR) ayant été utilisées sont correctement configurées. L'essai permet en particulier de confirmer les valeurs attendues des paramètres au sein du PDS(SR). L'essai est généralement effectué et documenté par la partie responsable de la mise en service du PDS(SR), en utilisant les procédures d'essai fournies par le fabricant du PDS(SR).

Le manuel de l'essai de configuration doit spécifier que les éléments suivants au minimum soient consignés:

- une description de l'application, notamment une représentation graphique;
- une description des composants relatifs à la sécurité (y compris les versions des logiciels) destinés à être utilisés par l'application;
- une liste des fonctions de sécurité destinées à être utilisées dans l'application du PDS(SR);
- les résultats des essais de ces fonctions de sécurité selon les procédures d'essai spécifiées;
- une liste de tous les paramètres de sécurité pertinents et leur valeur à l'intérieur du PDS(SR);
- les sommes de vérification, la date des essais et la confirmation par le personnel en charge des essais.

Les essais de configuration des PDS(SR) dans les applications répliquées peuvent être réalisés en soumettant l'application répliquée à un essai de type unique, à condition qu'il puisse être démontré que les fonctions de sécurité seront configurées de la manière attendue dans toutes les unités.

g) Les *essais de diagnostic* à réaliser, soit par l'utilisateur, soit par le personnel des installations comprenant un PDS(SR) (par exemple, automate programmable (AP), inspecteur de surveillance).

h) Les procédures fournies relatives au fonctionnement et à la maintenance du PDS(SR) doivent spécifier les éléments suivants:

- les actions courantes requises pour maintenir dans le temps la sécurité fonctionnelle du PDS(SR), notamment le remplacement des composants ayant une durée de vie limitée (par exemple les ventilateurs de refroidissement, les batteries, etc.);
- les actions et contraintes requises pour garantir la sécurité et/ou réduire les conséquences d'un événement dangereux;
- les procédures de maintenance à suivre en cas de défaut ou de défaillance du PDS(SR), y compris;
  - les procédures de diagnostic et de réparation des défauts; et
  - les procédures de revalidation.

– les outils requis pour procéder à la maintenance et à la revalidation et les procédures de maintenance des outils et des équipements.

NOTE Il convient que les procédures de maintenance et de fonctionnement du PDS(SR) soient mises à jour de manière continue, par exemple après:

– des audits de la sécurité fonctionnelle;

– des essais du PDS(SR).

# 8 Vérification et validation

## 8.1 Généralités

L'objet du présent paragraphe est de démontrer la conformité au plan de sécurité fonctionnelle (voir 5.3).

## 8.2 Vérification

Lors de la conception, il doit être vérifié, à l'issue de chaque phase de conception, que les exigences relatives à la phase de conception achevée sont satisfaites. Pour effectuer la vérification, il peut être procédé à une évaluation, une analyse, un examen, une revue et/ou des essais.

## 8.3 Validation

A l'issue de la conception, il doit être vérifié que le PDS(SR) satisfait à toutes les exigences de sécurité décrites dans la spécification. Pour effectuer la validation, il peut être procédé à une évaluation, une analyse, un examen, une revue et/ou des essais. Le Tableau B.5 de la CEI 61508-2:2000 donne des recommandations permettant d'éviter toute anomalie lors de la validation.

## 8.4 Documentation

La documentation appropriée relative à la vérification et à la validation du PDS(SR) doit être fournie et comporter les informations suivantes:

a) la ou les versions du ou des plans de vérification et de validation utilisés;

b) la ou les fonctions de sécurité soumises à essai (ou à analyse), ainsi qu'une référence à la ou les exigences spécifiées lors de la planification de la validation et de la vérification du PDS(SR);

c) les outils et équipements utilisés;

d) le résultat de chaque vérification et de chaque validation.

# 9 Exigences relatives aux essais

## 9.1 Planification des essais

Les essais des fonctions de sécurité du PDS(SR) doivent être planifiés simultanément à chaque phase du processus de développement.

Le plan d'essai doit être documenté et doit comporter tous les détails relatifs aux:

a) essais de fonctionnement de chaque fonction de sécurité;

b) essais de fonctionnement de chaque fonction de diagnostic des fonctions de sécurité;

c) critères d'acceptation.

Les essais peuvent être soit des essais en boîte noire, c'est-à-dire sans tenir compte du fonctionnement interne de la fonction de sécurité, soit des essais en boîte blanche, c'est-à-dire basés sur une connaissance spécifique du fonctionnement de la fonction de sécurité afin de déterminer l'essai (par exemple, insertion de défauts).

Les essais peuvent être supprimés ou remplacés par d'autres méthodes de vérification ou de validation si les exigences pertinentes le permettent.

### 9.2 Documentation d'essai

Durant les essais du PDS(SR) relatifs aux fonctions de sécurité, les détails suivants doivent être documentés:

a) la version du plan d'essai utilisé;

b) les critères d'acceptation des essais;

c) le type et la version du PDS(SR) soumis à essai;

d) les outils et équipements utilisés, ainsi que les données relatives à l'étalonnage;

e) les conditions d'essai;

f) le personnel en charge des essais;

g) les résultats détaillés de chaque essai;

h) tout écart entre les résultats attendus et les résultats obtenus;

i) les conditions d'essai: réussite ou raisons de l'échec.

## 10 Modification

### 10.1 Objectif

L'objectif de cet article est de garantir que la sécurité fonctionnelle du PDS(SR) est maintenue lorsque des modifications de conception sont apportées une fois la conception originale lancée en fabrication.

### 10.2 Exigences

Avant de procéder à une modification, des procédures doivent être planifiées. Les modifications doivent être apportées avec au moins le même niveau d'expertise, les mêmes outils automatiques, la même planification et la même gestion que ceux utilisés lors du développement initial du PDS(SR). Les modifications doivent être réalisées conformément à la planification.

#### 10.2.1 Demande de modification

La modification doit être lancée uniquement après soumission d'une demande de modification, conformément aux procédures de gestion de la sécurité fonctionnelle (voir l'Article 5). La demande doit comporter les indications suivantes:

a) la justification de la modification;

b) la modification proposée (aussi bien matérielle que logicielle).

#### 10.2.2 Analyse d'impact

L'impact de la modification proposée sur la sécurité fonctionnelle du PDS(SR) doit faire l'objet d'une évaluation. Cette dernière doit inclure une analyse permettant de déterminer dans quelle mesure il s'avère nécessaire de revenir aux étapes de développement concernées selon 5.2.

#### 10.2.3 Autorisation

L'autorisation de procéder à la modification demandée doit être basée sur les résultats de l'analyse d'impact.

### 10.2.4 Documentation

Une documentation appropriée concernant les modifications apportées à chaque PDS(SR) doit être établie et tenue à jour. Elle doit comporter les éléments suivants:

a) une spécification détaillée de la modification;

b) les résultats de l'analyse d'impact;

c) les autorisations de modifications;

d) les cas d'essai des composants comportant des données relatives à la revalidation;

e) l'historique relatif à la gestion de la configuration (logicielle et matérielle) du PDS(SR);

f) les écarts par rapport aux fonctionnements et aux conditions précédentes;

g) les modifications à apporter aux informations pour l'utilisation;

h) toutes les étapes de développement s'appliquant conformément aux indications spécifiées en 5.2.

# Annexe A
(informative)

## Table de tâches séquentielles

Conformément au cycle de vie décrit dans la CEI 61508, la procédure de conception suivante s'applique au PDS(SR). L'ordre des étapes de développement requises est indiqué et référence est faite à l'article ou au paragraphe pertinent de la présente norme ou de la CEI 61508.

NOTE 1 La conception et le développement du cycle de vie a été décomposé en «concept» et en «conception et développement», comme c'est la pratique aujourd'hui en ingénierie de conception.

NOTE 2 Lorsqu'une certification par une tierce partie est requise, il convient que le fabricant du PDS(SR) et l'organisme de certification se mettent en contact au début de la procédure de conception.

NOTE 3 Les références à la CEI 61508 contenues dans le tableau ci-dessous s'appliquent à la première édition. La numérotation des articles/paragraphes est susceptible d'être modifiée dans les éditions suivantes.

| | Tâches | Références |
|---|---|---|
| 1 | **Exigences générales** | |
| | Il convient que le contrôle des documents pertinents soit organisé en un système de maîtrise des documents<br><br>Détails relatifs à la gestion de projet<br><br>Système de management de la qualité de la certification | CEI 61508-1:1998, §5<br>CEI 61508-2:2000, §7.3, 7.7, 7.8, 7.9<br>CEI 61508-3:1998, §6, 7.3, 7.4.2.1, 7.7, 7.8, 7.9 |
| 2 | **Spécification des exigences de sécurité s'appliquant au PDS(SR)** | Phase 1 du cycle de vie de sécurité du PDS(SR) (voir 5.2 de la présente norme) |
| | Elaboration d'une spécification des exigences de sécurité (SRS), comprenant les exigences de sécurité fonctionnelle et les exigences d'intégrité de sécurité | Voir 5.4 de la présente norme<br><br>CEI 61508-1:1998, §7.6<br>CEI 61508-2:2000, §7.2, Tableaux B.1, B.6<br>CEI 61508-2:2000, §7.4.4-6, Annexe A<br>CEI 61508-3:1998, §7.2,Tableaux A.1, B.7<br>CEI 61508-3:1998, §7.4.2/4, Tableaux A.3, B.1<br>CEI 61508-7:2000, Tableau C.1<br>Exemples dans la CEI 61508-5,<br>Exemples dans la CEI 61508-6:2000, Annexe A |
| 3 | **Vérification de la spécification des exigences de sécurité relative au PDS(SR)** | |
| | a) Revues de la spécification des exigences de sécurité<br><br>b) Vérification par une personne ou un service indépendant, le cas échéant | a) Voir 8.2 de la présente norme<br><br>b) CEI 61508-2:2000 et CEI 61508-3:1998, §7.9 |

| | Tâches | Références |
|---|---|---|
| **4** | **Concept** | Phase 3 du cycle de vie de sécurité du PDS(SR) (voir 5.2 de la présente norme) |
| | **a) Conception matérielle au niveau architectural, notamment**<br>• Les blocs diagrammes du matériel de sécurité<br>• Interfaces utilisateur et processus<br>• Chemins des signaux de sécurité pertinents<br>• Alimentation<br>• Séparation des canaux indépendants pour atteindre la tolérance aux défauts<br>• Liaisons de communication entre les canaux indépendants pour atteindre la *couverture du diagnostic* | a) Voir l'Article 6 de la présente norme<br>CEI 61508-2:2000, §7.4, Annexe A, Tableaux B.2, B.6<br>Exemples dans la CEI 61508-6:2000, Annexes A et D |
| | **b) Conception logicielle au niveau architectural, notamment:**<br>• Description des fonctions proposées par le logiciel relatif à la sécurité<br>• Interaction avec le matériel<br>• Diagrammes d'états du comportement attendu du logiciel<br>• Interfaces utilisateur et processus<br>• Possibilités de détection de défaut et réactions au défaut<br>• Présentation de la structure logicielle, par exemple, au moyen d'un bloc diagramme<br>• Contrôle et stockage des données relatives à la sécurité<br>• Procédures de la version<br>• Outils utilisés, par exemple, compilateur, vérificateur de code, etc.<br>**c) Recommandation**<br>Pré-estimation de la probabilité de défaillance des fonctions de sécurité liée à des défaillances matérielles aléatoires au niveau des blocs diagrammes fonctionnels | b) CEI 61508-2:2000, §7.2.3.1(h)<br>CEI 61508-3:1998, §7.2.2.8, 7.2.2.10, 7.4.2/3, Tableaux A.2, B.1, B.7, B.9<br>CEI 61508-7:2000, Tableau C.1<br>c) CEI 61508-1:1998, Tableau 2<br>CEI 61508-2:2000, §7.4.3, Tableaux 3, A.1, Annexe C<br>CEI 61508-3:1998, Tableau B.4 (AMDE)<br>Exemples dans la CEI 61508-6:2000, Annexes C et D |
| **5** | **Vérification du concept** | |
| | a) Revues de la conception de système<br>b) Vérification par une personne ou un service indépendant, le cas échéant | a) Voir 8.2 de la présente norme<br>b) CEI 61508-2:2000 et CEI 61508-3:1998, §7.9 |
| **6** | **Planification de la validation** | Phase 2 du cycle de vie de sécurité du PDS(SR) (voir 5.2 de la présente norme) |
| | a) Planification détaillée de la validation du PDS(SR) relatif à la sécurité<br>b) Il convient que le plan de validation soit généré parallèlement à la Phase 9.3 Conception et Développement | a) Voir 8.3 de la présente norme<br>b) CEI 61508-2:2000, §7.3, Tableau B.5<br>CEI 61508-3:1998, §7.3, Tableaux A.7, B.3, B.5 |
| **7** | **Vérification du plan de validation** | |
| | a) Revues du plan de validation<br>b) Vérification par une personne ou un service indépendant, le cas échéant | a) Voir 8.2 de la présente norme<br>b) CEI 61508-2:2000 et CEI 61508-3:1998, §7.9 |

| | Tâches | Références |
|---|---|---|
| **8** | **Conception et développement** | Phase 3 du cycle de vie de sécurité du PDS(SR) (voir 5.2 de la présente norme) |
| | a) Conception matérielle<br>b) Conception logicielle<br>c) Prédiction de fiabilité (calcul de la probabilité de défaillance des fonctions de sécurité liée à des défaillances matérielles aléatoires) incluant:<br>• Type de PDS(SR)<br>• SFF<br>• Bloc diagramme fonctionnel<br>• Modèle de fiabilité<br>• Bases de données du modèle (listes des dispositifs)<br>• Calcul de la PFH<br>• Durée de mission<br>• Intervalle de réparation, intervalle d'essai périodique (le cas échéant) | Voir l'Article 6 de la présente norme<br>a) CEI 61508-2:2000, §7.4, Annexe A, Tableaux B.2, B.3, B.6<br>b) CEI 61508-3:1998, §7.4.5, 7.4.6, Tableau A.4<br>c) CEI 61508-1:1998, Tableau 2<br>CEI 61508-2:2000, §7.4.3, 7.4.7, Tableaux 3, A.1, Annexe C<br>CEI 61508-3:1998, Tableau B.4 (AMDE)<br>Exemples dans la CEI 61508-6:2000, Annexes C et D |
| **9** | **Vérification de la conception** | |
| | a) Revues de la conception système<br>b) Essais fonctionnels par niveau de module<br>c) Vérification par une personne ou un service indépendant, le cas échéant | a) Voir 8.2 de la présente norme<br>c) CEI 61508-2:2000, §7.9<br>CEI 61508-3:1998, §7.4.7, 7.4.8, 7.5, 7.9, Tableaux A.5, A.9 |
| **10** | **Intégration du PDS(SR)** | Phase 4 du cycle de vie de sécurité du PDS(SR) (voir 5.2 de la présente norme) |
| | Intégration du PDS(SR) relatif à la sécurité et essais | Voir 6.5 de la présente norme |
| **11** | **Vérification de l'intégration** | |
| | Revue des résultats des essais d'intégration logicielle/matérielle et documentation | Voir 8.2 de la présente norme<br>CEI 61508-2:2000, §7.5, 7.9, Tableaux B.3, B.6<br>CEI 61508-3:1998, §7.4.3.2(f), 7.4.5.5, 7.4.6.2, 7.4.7, 7.5, 7.9, Tableaux A.5, A.6, A.9 |
| **12** | **Installation, mise en service, fonctionnement (documentation utilisateur)** | Phase 5 du cycle de vie de sécurité du PDS(SR) (voir 5.2 de la présente norme) |
| | Elaboration de la documentation utilisateur contenant les détails relatifs à l'installation, la mise en service, le fonctionnement et la maintenance du PDS(SR). | Voir l'Article 7 de la présente norme<br>CEI 61508-2:2000, §7.6, Tableau.B.4 |
| **13** | **Vérification de la documentation utilisateur** | |
| | a) Revues de la documentation utilisateur contenant les détails relatifs à l'installation, la mise en service, le fonctionnement et la maintenance du PDS(SR).<br>b) Vérification par une personne ou un service indépendant, le cas échéant | a) Voir 8.2 de la présente norme<br>b) CEI 61508-2:2000 et CEI 61508-3:1998, §7.9 |

| | Tâches | Références |
|---|---|---|
| **14** | **Validation du PDS(SR)** | Phase 6 du cycle de vie de sécurité du PDS(SR) (voir 5.2 de la présente norme) |
| | a) Mention de tous les détails nécessaires à la validation du PDS(SR)<br>b) Documentation logicielle complète et documentation requise<br>c) Essais et procédures de validation conformes au plan de validation<br>d) Documentation des résultats des essais de validation<br>e) Le cas échéant, préparation de la documentation requise en vue de la validation par une tierce partie | a) Voir 8.3 de la présente norme<br>c) CEI 61508-2:2000, §7,7, Tableaux B.5, B.6<br>CEI 61508-3:1998, §7.5.2.7, 7.7, 7.9, Tableau A.7 |
| **15** | **Procédure de modification du PDS(SR)** | |
| | a) Demande de modification et analyse<br>b) Documentation adaptée de toutes les parties du PDS(SR) ayant été modifiées<br>c) Re-vérification des parties ayant été modifiées<br>d) Mise à jour de la prédiction de fiabilité si la modification a un impact sur la tolérance aux défauts, la probabilité de défaillance dangereuse, la *couverture du diagnostic* ou la *défaillance de cause commune*<br>e) Re-validation au moins des parties du PDS(SR) ayant été modifiées<br>f) Modification logicielle | a) Voir l'Article 10 de la présente norme<br>b) CEI 61508-1:1998, §7.16<br>CEI 61508-2:2000, §7.5.2.5, 7.8<br>Exemple dans la CEI 61508-1:1998, Figure 9<br>f) CEI 61508-3:1998, § 7.1.2.8, 7.5.2.6, 7.6.2, 7.8.2, Tableau A.8 |

# Annexe B
(informative)

# Exemple de détermination de la *PFH*

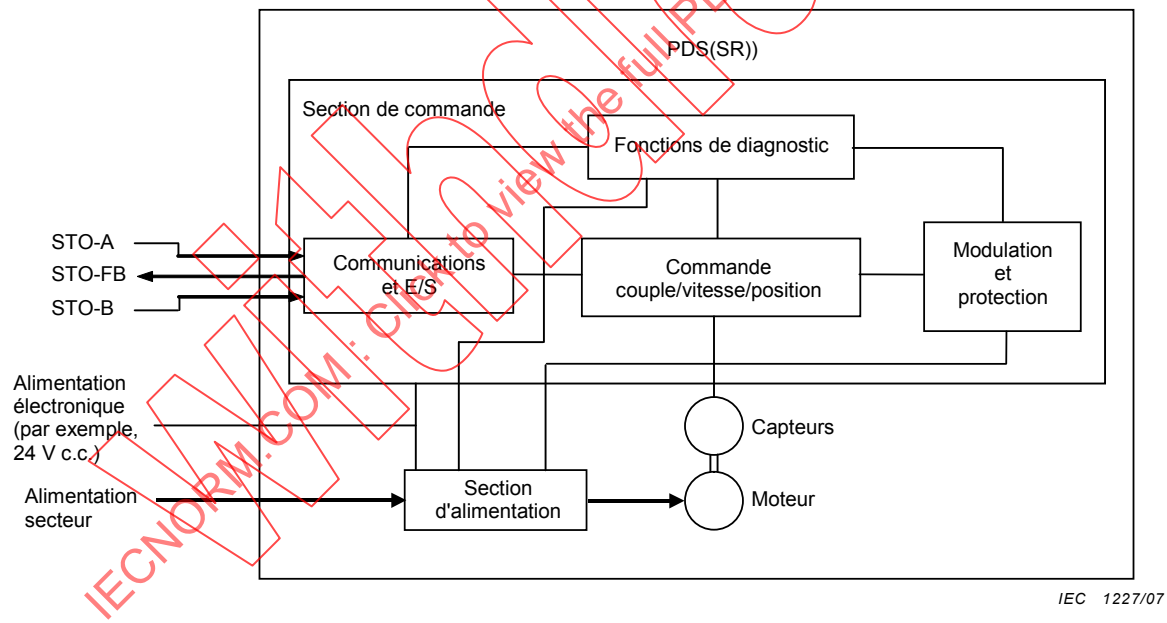
## B.1 Généralités

Le présent article contient un exemple de quantification de la probabilité *PFH* pour un PDS(SR) proposant la fonction de sécurité Suppression Sûre du Couple (STO). Toutes les exigences requises s'appliquant au PDS(SR) et à ses parties structurelles internes sont spécifiées, afin de donner un exemple le plus détaillé possible de mode de quantification de la proportion PFH.

## B.2 Exemple de structure d'un PDS(SR)

### B.2.1 Généralités

Le PDS(SR) décrit dans le présent article comporte la fonction de sécurité STO; cette fonction est activée par deux interfaces d'entrée numériques redondantes et produit un signal de réaction unique par le biais d'une interface de sortie numérique (voir la Figure B.1).




NOTE STO-A: canal d'entrée A d'activation de la fonction STO; STO-B: canal d'entrée B d'activation de la fonction STO; STO-FB: sortie de réaction de la fonction STO.

**Figure B.1 – Exemple de PDS(SR)**

Les exigences s'appliquant à l'exemple sont les suivantes:

– SIL 2;

– mode de fonctionnement continu.

A l'intérieur du PDS(SR), la fonction de sécurité STO est installée conjointement avec la fonctionnalité standard du PDS(SR), à l'aide d'un nombre réduit de composants exclusifs à la fonction de sécurité.

Du fait de la présence d'un bloc d'alimentation interne monocanal, le PDS(SR) est divisé en deux sous-systèmes indépendants: le sous-système bicanal A/B et le sous-système PS/VM (alimentation/contrôleur de tension) (voir la Figure B.2).

La valeur de la PFH de la fonction de sécurité STO pour cet exemple de PDS(SR) se calcule de la manière suivante:

$PFH_{PDS(SR)} = PFH_{A/B} + PFH_{PS/VM}$

où $PFH_{A/B}$ et $PFH_{PS/VM}$ sont respectivement les valeurs de la PFH des sous-systèmes A/B et PS/VM.

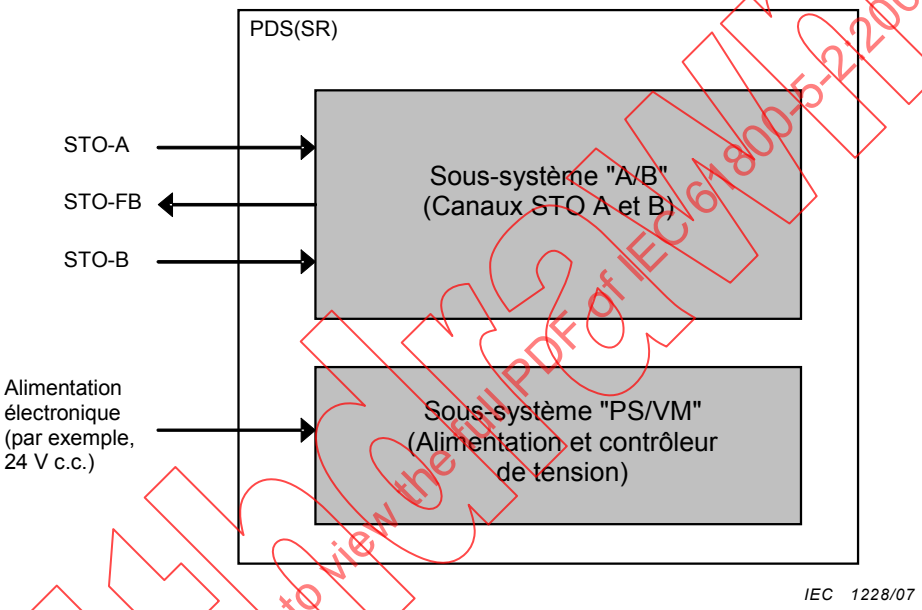



**Figure B.2 – Sous-systèmes du PDS(SR)**

### B.2.2 Sous-système A/B

La fonction de sécurité STO est installée avec deux canaux, de manière à atteindre une tolérance aux défauts du matériel égale à 1. Elle est modélisée par le sous-système «A/B», pour lequel il est procédé à un calcul informatique de la valeur de la PFH indépendante. La réalisation du sous-système donne les propriétés système suivantes, en ce qui concerne la fonction de sécurité:

– type B (matériel complexe);
– tolérance aux défauts du matériel égale à 1 (installation bicanal).

Les contraintes architecturales d'un sous-système de type B (voir 6.2.2.3) montrent que, pour le SIL 2 et une tolérance aux défauts du matériel égale à 1, la proportion de défaillances en sécurité (SFF) doit être d'au moins 60 %.

### B.2.3 Sous-système PS/VM

Dans la mesure où le bloc d'alimentation interne (PS) est monocanal, un contrôleur de tension (VM) est installé. Le bloc d'alimentation interne et le contrôleur de tension sont modélisés sous la forme d'un sous-système séparé «PS/VM» pour lequel il est procédé à un calcul informatique de la valeur de la PFH indépendante. La réalisation du sous-système donne les propriétés système suivantes, en ce qui concerne la fonction de sécurité: