IEC 61800-5-2

Edition 2.0 2016-04
REDLINE VERSION

INTERNATIONAL STANDARD

colour
inside

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

IEC 60000:2016-01 RLV(en)

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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 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.

IEC 61800-5-2

Edition 2.0 2016-04
REDLINE VERSION

INTERNATIONAL STANDARD

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 29.200

ISBN 978-2-8322-3353-5

Warning! Make sure that you obtained this publication from an authorized distributor.

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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 second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) rational added in the scope why low demand mode is not covered by this standard

b) definition added for: “*category*” and “*safety function*”

c) “Other sub-functions” sorted into “Monitoring sub-functions” and “Output functions”

d) deleted “proof test” throughout the document because for *PDS(SR)* a proof test is not applicable

e) replaced the term “safety function” by “*safety sub-function*” throughout the document

f) Updated references to IEC 61508 series Ed.2010

g) Added the principle rules of ISO 13849-1 and reference to tables of ISO 13849-2

h) 6.1.6 Text replaced by Table 2

i) 6.1.7 Integrated circuits with on-chip redundancy matched to changed requirement in IEC 61508-2: 2010, Annex E

j) 6.2.8 Design requirements for thermal immunity of a *PDS(SR)*

k) 6.2.9 Design requirements for mechanical immunity of a *PDS(SR)*

l) 6.1.6 *SIL* for multiple *safety sub-functions* within one *PDS(SR)*

m) 6.1.7 Integrated circuits with on-chip redundancy

n) 6.2.1 Basic and well-tried safety principles

o) 6.2.2.1.4 *Diagnostic test* interval when the hardware fault tolerance is greater than zero

p) 6.2.5.2.7 *PDS(SR)* parameterization

q) 9 Test requirements

r) 9.3 Electromagnetic (EM) immunity testing

s) 9.4 Thermal immunity testing

t) 9.5 Mechanical immunity testing

u) Annex A Sequential task table

v) Annex D, D.3.16, Motion and position feedback sensors updated

w) Annex E Electromagnetic immunity (EM) requirement for *PDS(SR)*

x) Annex F Estimation of PFD_{avg} value for low demand with given PFH value

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

FDIS	Report on voting
22G/332/FDIS	22G/335/RVD

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

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

A list of all parts of the IEC 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 stability date indicated on the IEC website 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 PL) 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 *hazard*s where access to the ~~danger zone~~ dangerous area is only possible when rotating parts have ~~attained a safe condition~~ stopped. This part of IEC 61800 gives a methodology to identify the contribution made by a *PDS(SR)* to identified *safety* sub-*function*s 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, which is a product standard, specifies requirements and makes recommendations for the design and development, integration and validation of safety-related power drive systems (*PDS(SR)*) in terms of their functional safety considerations. It applies to adjustable speed electrical power drive systems covered by the other parts of the IEC 61800 series of standards as referred in IEC 61800-2.

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

NOTE 2 Other parts of IEC 61800 cover rating specifications, EMC, electrical safety, etc.

This International Standard is ~~only~~ applicable where functional safety of a *PDS(SR)* is claimed and the *PDS(SR)* is operating mainly in the high demand or continuous mode (see 3.15). ~~For low demand applications, see IEC 61508.~~

While low demand mode operation is possible for a *PDS(SR)*, this standard concentrates on high demand and continuous mode. *Safety sub-functions* implemented for high demand or continuous mode can also be used in low demand mode. Requirements for low demand mode are given in IEC 61508 series. Some guidance for the estimation of average probability of dangerous failure on demand (PFD$_{avg}$) value is provided in Annex F.

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 *subsystem*s of a safety-related system. It is intended to facilitate the realisation of the electrical/ electronic/ programmable electronic (E/E/PE) ~~elements~~ parts of a *PDS(SR)* in relation to the safety performance of *safety sub-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 integrator~~s~~, ~~machinery and plant designers,~~ original equipment manufacturer) 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).

By applying the requirements from this part of the IEC 61800 series, the corresponding requirements of IEC 61508 that are necessary for a *PDS(SR)* are fulfilled.

This part of IEC 61800 does not specify requirements for:

- the *hazard* and risk analysis of a particular application;
- the identification of *safety sub-function*s for that application;
- the initial allocation of *SIL*s to those *safety sub-function*s;
- the driven equipment except for interface arrangements;
- secondary *hazard*s (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)*.
- security aspects (e.g. cyber security or *PDS(SR)* security of access)

NOTE 3 The functional safety requirements of a *PDS(SR)* are dependent on the application, and ~~must~~ can 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 sub-function*s with a *SIL* not greater than *SIL* 3.

Figure 1 shows the installation and the functional ~~elements~~ parts of a *PDS(SR)* that are considered in this part of IEC 61800

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

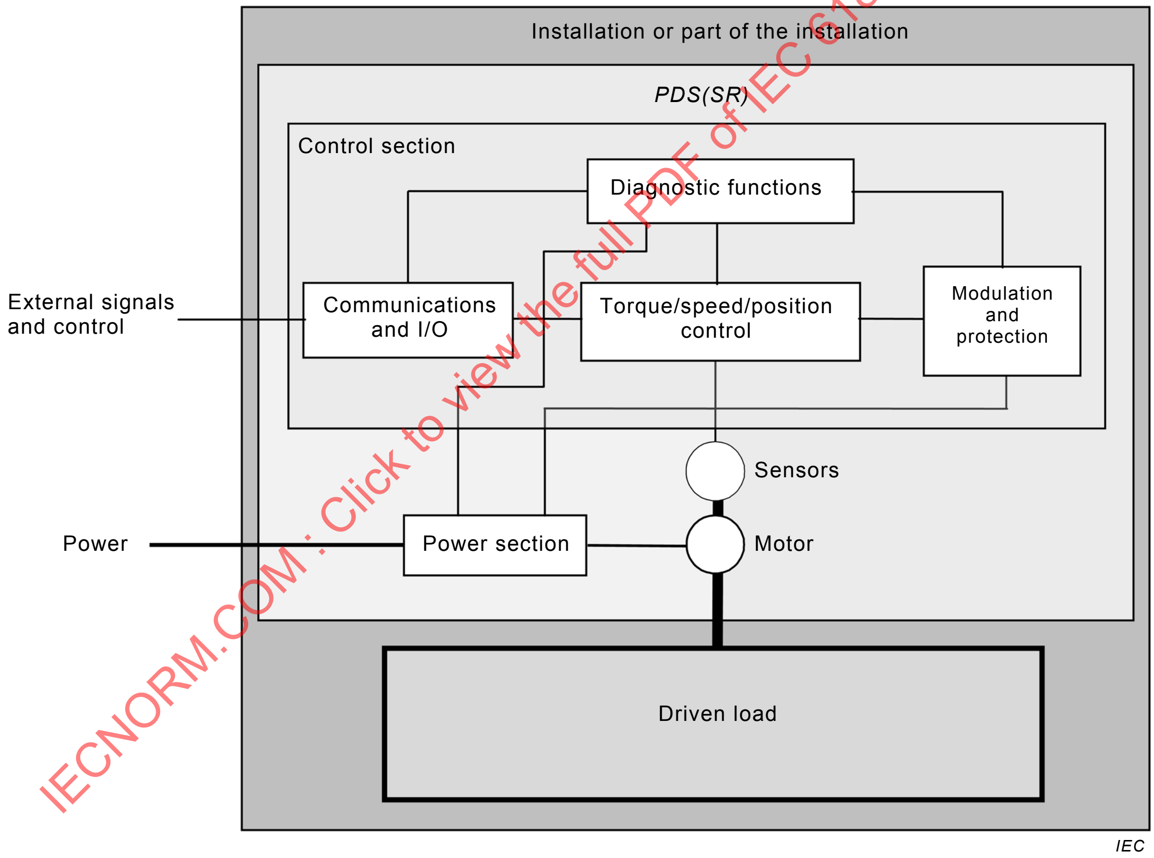

Installation or part of the installation
PDS(SR)
Control section
Diagnostic functions
External signals and control
Communications and I/O
Torque/speed/position control
Modulation and protection
Sensors
Power
Power section
Motor
Driven load
IEC

Figure 1 – Installation and functional ~~elements~~ parts of a *PDS(SR)*

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 61000-2-4:2002, *Electromagnetic compatibility (EMC) – Part 2-4: Environment – Compatibility levels in industrial plants for low-frequency conducted disturbances*

IEC 61000-4-2:2008, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3:2006, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*
IEC 61000-4-3:2006/AMD1:2007
IEC 61000-4-3:2006/AMD2:2010

IEC 61000-4-4:2012, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5:2014, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6:2013, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-29:2000, *Electromagnetic compatibility (EMC) – Part 4-29: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests*

IEC 61000-4-34:2005, *Electromagnetic compatibility (EMC) – Part 4-34: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests for equipment with input current more than 16 A per phase*

IEC 61000-6-7:2014, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61400-21:2008, *Wind turbines – Part 21: Measurement and assessment of power quality characteristics of grid connected wind turbines*

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

IEC 61508-1:~~1998~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:~~2000~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:~~1998~~ 2010, *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~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:~~2000~~ 2010, *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 61800-2:2015, *Adjustable speed electrical power drive systems – Part 2: General requirements – Rating specifications for low voltage adjustable ~~frequency~~ speed a.c. power drive systems*

IEC 61800-3:2004, *Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods*
IEC 61800-3:2004/AMD1:2011

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~~ 2007, *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*~~

ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Terms and definitions

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

~~NOTE 1~~ Table 1 shows an alphabetical list of terms and definitions.

Table 1 – Alphabetical list of terms and definitions

3.1	basic drive module BDM	3.12	hazard	3.23	safety sub-function(s) (of a PDS(SR))
3.2	category	3.13	installation	3.24	safety integrity
3.3	complete drive module CDM	3.14	mission time TM	3.25	safety integrity level SIL
3.4	common cause failure	3.15	mode of operation	3.26	safety-related system
3.5	dangerous failure	3.16	PDS(SR)	3.27	safety requirements specification SRS
3.6	diagnostic coverage DC	3.17	average frequency of a dangerous failure PFH	3.28	SIL capability
3.7	diagnostic test(s)	~~3.13~~	~~Proof test~~	3.29	subsystem
3.8	fail safe	3.18	Performance Level PL	3.30	systematic failure
3.9	fail safe state FS	3.19	safe failure	3.31	systematic safety integrity
3.10	fault reaction function	3.20	safe failure fraction SFF	3.32	validation
3.11	functional safety	3.21	safe state	3.33	verification
		3.22	safety function		

NOTE Throughout this International Standard, references to the following definitions are identified by writing them in *italic* script.

3.1
basic drive module
BDM

electronic power converter and related control, connected between an electric supply and a motor

Note 1 to entry: The *BDM* is capable of transmitting power from the electric supply to the motor and can be capable of transmitting power from the motor to the electric supply.

Note 2 to entry: The *BDM* controls some or all of the following aspects of power transmitted to the motor and motor output: current, frequency, voltage, speed, torque, force.

Note 3 to entry: This note applies to the French language only.

[SOURCE: IEC 61800-3:2004/AMD1:2011, 3.1.1]

3.2
category

classification of the safety-related parts of a *PDS(SR)* in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

[SOURCE: ISO 13849-1, definition 3.1.2, modified] “control system” replaced by “*PDS(SR)”*

3.3
complete drive module
CDM
drive module consisting of, but not limited to, the *BDM* and extensions such as protection devices, transformers and auxiliaries, but excluding the motor and the sensors which are mechanically coupled to the motor shaft

Note 1 to entry: This note applies to the French language only.

[SOURCE: IEC 61800-3:2004/AMD1:2011, 3.1.2]

3.4
common cause failure
failure, which is the result of one or more events, causing ~~coincident~~ concurrent failures of two or more separate channels in a multiple channel system, leading to failure of the *safety sub-function*

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.6.10 modified – "leading to system failure" replaced by "leading to failure of the *safety sub-function*"]

3.5
dangerous failure
~~failure which has the potential to put the *safety-related system* in a hazardous or fail-to-function state~~
failure of a component and/or *subsystem* and/or system that plays a part in implementing the *safety sub-function* that:

a) causes a *safety sub-function* of a *PDS(SR)* to fail such that the equipment or machinery driven by the *PDS(SR)* is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the *safety sub-function* operates correctly

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.6.7, modified – "EUC" replaced by "*PDS(SR)*", "when required" deleted]

3.6
diagnostic coverage
DC
fraction~~al decrease in the probability~~ of dangerous~~ hardware~~ failures~~ resulting from the operation of the~~ detected by automatic *diagnostic tests*

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

Note 2 to entry: *Diagnostic coverage*~~ may~~ can exist for the whole or parts of a *safety-related system*. For example, *diagnostic coverage*~~ may~~ can exist for sensors and/or logic *subsystems* and/or~~ final elements~~ output *subsystem*.

Note 3 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.8.6, modified – "on-line" deleted from "online diagnostic tests"]

3.7
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

3.8
fail safe

design property of an item which prevents its failures from resulting in dangerous faults

[SOURCE: IEC 60500:1998, 821-01-10, modified – "critical" replaced by "dangerous"]

3.9
fail safe state
FS

defined *safe state*, typically resulting from a failure

Note 1 to entry: Fail safe state (*FS*) is used in this standard instead of the defined state (DS) of IEC 61000-6-7.

Note 2 to entry: This note applies to the French language only.

3.10
fault reaction function

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

3.11
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~~ *PDS(SR)* which depends on the correct functioning of the *safety-related parts of the PDS(SR)* and on external risk reduction measures

Note 1 to entry: This standard only considers those aspects in the definition of *functional safety* that depend on the correct functioning of the *PDS(SR)*.

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.~~1~~.12, modified – "EUC and the EUC control system" replaced by "*PDS(SR)*"; "E/E/PE safety-related systems and other" replaced by "*safety-related parts of the PDS(SR)* and on external"]

3.12
hazard

potential source of harm

Note 1 to entry: 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.~~

[SOURCE: ~~ISO/IEC Guide 51:1999, definition 3.5~~ IEC 60050-351:2013, 351-57-01, modified note 1 to entry]

3.13
installation

PDS(SR), equipment ~~or equipments including at least~~ driven by the *PDS(SR)* and ~~the driven~~ possibly other equipment (see Figure 1)

Note 1 to entry: 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~~ "act of installing" will be used in this standard.

3.14
mission time
TM
specified cumulative operating time of the safety-related parts of the *PDS(SR)* during its overall lifetime

Note 1 to entry: This note applies to the French language only.

3.15
mode of operation
way in which a *safety~~-related system~~ sub-function* is intended to be used, with respect to the ~~frequency~~ rate of demands made upon it, which may be either low demand mode, high demand or continuous mode.

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

Note 1 to entry: Low demand mode: where the ~~frequency~~ rate of demands for operation made on a *safety~~-related system~~ sub-function* is no greater than one per year ~~and no greater than twice the proof-test frequency~~.

Note 2 to entry: High demand ~~or~~ and continuous mode: where the ~~frequency~~ rate of demands for operation made on a *safety~~-related system~~ sub-function* is greater than one per year ~~or greater than twice the proof-test frequency~~.

Note 3 to entry: 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~~ mainly considered to operate in the high demand mode 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.~~

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.5.16, modified – "high demand mode" and continuous mode" combined; definition reduced to statements of time]

3.16
PDS(SR)
adjustable speed electrical power drive system ~~suitable for use in~~ providing *safety~~-related applications~~ sub-functions*

3.17
average frequency of a dangerous failure
PFH
~~probability of a dangerous random hardware failure per hour~~
average frequency of a dangerous failure of a *PDS(SR)* to perform the specified *safety sub-function* over a given period of time

Note 1 to entry: in IEC 62061~~:2005~~, the abbreviation *PFH*$_D$ is used.

Note 2 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4:2010; 3.6.19, modified – "E/E/PE safety-related system" replaced by "*PDS(SR)*"]

~~**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]~~

3.18
Performance Level
PL

discrete level used to specify the ability of safety-related parts of control systems to perform a *safety sub-function* under foreseeable conditions

[SOURCE: ISO 13849-1:2006, 3.1.23, modified – "*safety function*" replaced by "*safety sub-function"*]

3.19
safe failure

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

failure of a component and/or *subsystem* and/or system that plays a part in implementing the *safety sub-function* that:

a) results in the spurious operation of the *safety sub-function* to put the *PDS(SR)* (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the *safety sub-function* to put the *PDS(SR)* (or part thereof) into a safe state or maintain a safe state

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.6.8 modified – "element" replaced by "component"; "EUC" replaced by "*PDS(SR)*"]

3.20
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~~

property of a safety related component and *subsystems* that is defined by the ratio of the sum of the average failure rates of safe and dangerous detected failures to the sum of safe and all dangerous failures.

Note 1 to entry: This ratio is represented by the equation: $SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

Note 2 to entry: See Annex C of IEC 61508-2:~~2000~~ 2010.

Note 3 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4:2010; 3.6.15, modified – "element" replaced by "component and *subsystems*"]

3.21
safe state

state of the *PDS(SR)* when safety is achieved

Note 1 to entry: In going from a potentially hazardous condition to the final safe state, the *PDS(SR)* can have to go through a number of intermediate safe states.

[SOURCE: IEC 61508-4:2010; 3.1.13, modified – "EUC" replaced by "*PDS(SR)*"]

3.22
safety function

function to be implemented by a safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the equipment or machinery driven by the PDS(SR), in respect of a specific hazardous event.

[IEC 61508-4:2010; 3.5.1, modified – "E/E/PES" deleted, "EUC" replaced by "the equipment or machinery driven by the *PDS(SR)*"]

3.23
***safety sub-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~~ safety of the *installation* or prevent *hazardous* conditions arising at the *installation*

Note 1 to entry: There are only rare cases where the safety function of the complete application is implemented exclusively within the *PDS(SR)*. In these cases the safety function is still called a *safety sub-function* in this standard. (e.g. always active SLS without external initiation)

3.24
safety integrity
probability of a *PDS(SR)* satisfactorily performing a required *safety sub-function* under all stated conditions within a stated period of time

Note 1 to entry: 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 sub-function*.

Note 2 to entry: The *safety integrity* ~~may not~~ can be ~~the same~~ different for each *safety sub-function* performed by the *PDS(SR)*.

[SOURCE: IEC 61508-4:~~1998~~ 2010; 3.5.4, modified – “E/E/PE safety-related system” replaced by “*PDS(SR)*”]

3.25
safety integrity level
SIL
discrete level (one out of a possible ~~four~~ three) for specifying the *safety integrity* requirements of a *safety sub-function* allocated (in whole or in part) to a *PDS(SR)*

Note 1 to entry: *SIL* ~~4~~ 3 has the highest level of *safety integrity* and *SIL* 1 has the lowest.

Note 2 to entry: *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.

Note 3 to entry: Several methods of writing are used for *SIL*x. Throughout this document *SIL* × is used

Note 4 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4:~~1998~~ 2010; 3.5.8, modified – “corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest” replaced by “for specifying the *safety integrity* requirements of a *safety sub-function* allocated (in whole or in part) to a *PDS(SR)*”]

3.26
safety-related system
designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the ~~EUC~~ equipment or machinery driven by the *PDS(SR)*; 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~~ measures, the necessary safety integrity for the required safety functions

[SOURCE: IEC 61508-4:2010; 3.4.1, modified] “EUC” replaced by “equipment or machinery driven by the *PDS(SR)*”, “E/E/PES” deleted.

3.27
safety requirements specification
SRS
specification containing all the requirements of the *safety sub-functions* ~~that have~~ to be performed by the *PDS(SR)*

Note 1 to entry: This note applies to the French language only.

3.28
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 1 to entry: Each of the designated *safety sub-function*s that a *PDS(SR)* is intended to perform can be associated with a different *SIL capability*.

Note 2 to entry: *SIL* capability includes systematic capability, the fulfillment of the architectural constraints and the hardware failure rate or PFH value.

3.29
subsystem

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

Note 1 to entry: A *PDS(SR)* can itself be a *subsystem*, or be made up from a number of separate *subsystem*s, which when put together to implement the *safety sub-function* under consideration. A *subsystem* can have more than one channel.

Note 2 to entry: Examples of *subsystem*s of a *PDS(SR)* are encoder, power section, control section (see Figure 1).

3.30
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 1 to entry: Examples of causes of *systematic failure*s include human error in:

- the *safety requirements specification*;
- the design, manufacture, ~~installation~~ act of installing, operation of the hardware;
- the design and implementation of the software.

Note 2 to entry: In this standard, failures in a safety-related system are categorized as random hardware failures or systematic failures.

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.6.6]

3.31
systematic safety integrity

part of the *safety integrity* of *safety-related system*s relating to *systematic failure*s in a dangerous mode of failure

Note 1 to entry: *Systematic safety integrity* cannot usually be quantified (as distinct from hardware safety integrity which usually can).

[SOURCE: IEC 61508-4:~~1998~~ 2010; 3.5.6]

3.32
validation

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

Note 1 to entry: *Validation* is the activity of demonstrating that the *PDS(SR)*, before or after ~~installation~~ act of installing, meets in all respects the *safety requirements specification* .

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.8.2, modified Note 1 to entry]

3.33
verification
confirmation by examination and provision of objective evidence that the requirements have been fulfilled

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.8.1, modified – removal of Note 1 to entry]

4 Designated *safety sub-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 sub-function*s in this clause are not considered to form an exhaustive list. Details of implementation for basic *safety sub-functions*, and complex *safety sub-function*s composed of more than one basic *safety sub-function*, have not been provided because of the large number of possibilities. In some cases, further *safety-related system*s external to the *PDS(SR)* (for example a mechanical brake) may be necessary to maintain the ~~safe condition~~ safety when electrical power is removed.

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

Each *safety sub-function* may ~~require~~ include safe inputs and/or outputs ~~signalling~~ in order to accomplish necessary communication with (or activation of) other functions, *subsystem*s 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 sub-function*s perform monitoring tasks only; some perform safety relevant control or other actions. Therefore, a distinction ~~must~~ shall 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 sub-function*; and

- the *fault reaction function* (relevant for all *safety sub-functions*):

  the reaction function when diagnostics detect a fault within the *safety sub-function*.

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

On selecting the appropriate reaction function, it ~~has to~~ shall 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 5.5).

The names of the *safety sub-function*s 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)*.

NOTE For detailed examples of the *PDS(SR)* sub-functions specified in this clause see Bibliography (IFA Report 7/2013e)

4.2 *Safety sub-functions*

4.2.1 General

In most cases the *safety functions* of the *PDS(SR)* are a part of the *safety functions* of an application, therefore the *safety functions* of the *PDS(SR)* are named *safety sub-functions* in this document. Figure 2 shows an example of a *safety function* consisting of *safety sub-functions*:

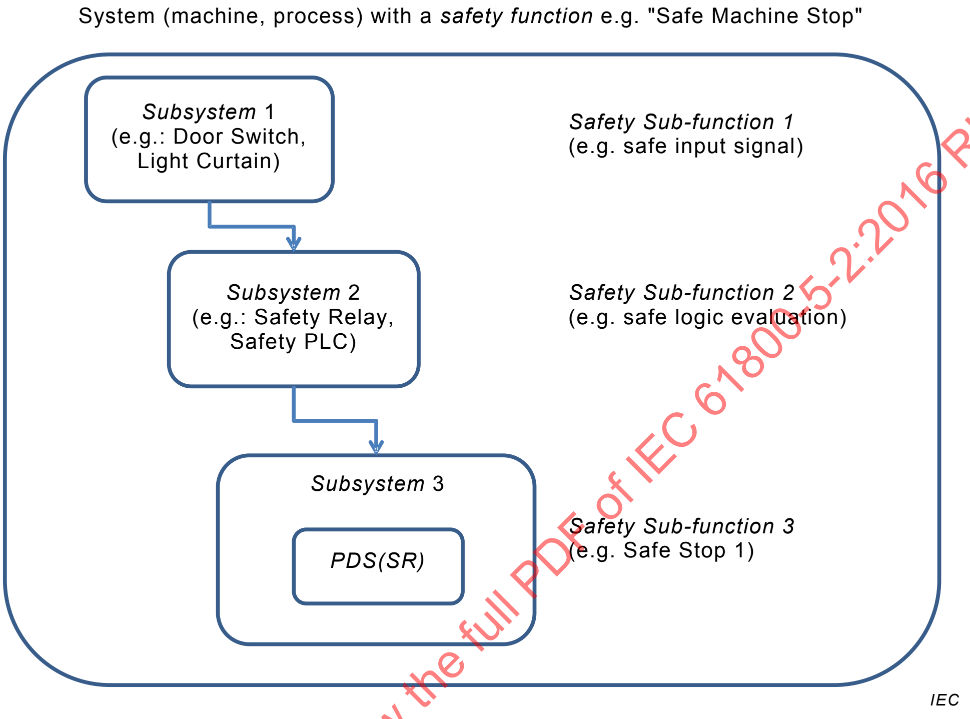

System (machine, process) with a *safety function* e.g. "Safe Machine Stop"
Subsystem 1
(e.g.: Door Switch, Light Curtain)
Safety Sub-function 1
(e.g. safe input signal)
Subsystem 2
(e.g.: Safety Relay, Safety PLC)
Safety Sub-function 2
(e.g. safe logic evaluation)
Subsystem 3
PDS(SR)
Safety Sub-function 3
(e.g. Safe Stop 1)
IEC

Figure 2 – *Safety function* consisting of *safety sub-functions*

NOTE For further information regarding *safety sub-functions* see IFA Report 7/2013e “Safe drive controls with frequency converters” (Bibliography).

4.2.2 Limit values

Where a *safety sub-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~~ can 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 4.2.4.9 ~~should~~ can take into account the maximum allowable over travel distance(s).

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

4.2.3 Stopping functions

4.2.3.1 General

A variety of stopping methods is available for every type of *PDS(SR).*

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 stopping functions.

NOTE When applying safety stopping functions for functions like prevention of unexpected start-up or emergency stop, relevant standards can be considered, e. g. IEC 60204-1, ISO 13850, ISO 12100, ISO 14118.

Any particular requirements for stopping performance ~~should~~ can be specified by the ~~installation designer~~ customers of the *PDS(SR)* manufacturer. The following examples of stopping functions are often used in practice.

4.2.3.2 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).~~

This function prevents force-producing power from being provided to the motor

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

NOTE 1 This *safety sub-function* ~~may~~ can be used where power removal is required to prevent an unexpected start-up according to ISO 14118.

NOTE 2 In circumstances where external influences (for example, falling of suspended loads) are present, additional measures (for example, mechanical brakes) ~~may~~ can be necessary to prevent any *hazard*.

NOTE 3 Electronic means and some contactors are not adequate for protection against electric shock~~, and additional measures for isolation may be necessary~~.

NOTE 4 While the function is active, a limited amount of movement is still possible in the event of a failure in the power section of the *PDS(SR)*

4.2.3.3 Safe stop 1 (SS1)

This function is specified as either

a) Safe Stop 1 deceleration controlled

SS1-d

initiates and controls the motor deceleration rate within ~~set~~ selected limits to stop the motor and ~~initiates~~ performs the STO function (see 4.2.3.2) when the motor speed is below a specified limit; or

b) Safe Stop 1 ramp monitored

SS1-r

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

c) Safe Stop 1 time controlled

SS1-t

initiates the motor deceleration and ~~initiates~~ performs the STO function after an application specific time delay.

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

NOTE The controlled stop of SS1-t can fail undetected, therefore SS1-t cannot be applied if this failure can cause a dangerous situation in the final application.

4.2.3.4 Safe stop 2 (SS2)

This function is specified as either

a) Safe Stop 2 deceleration controlled

SS2-d

initiates and controls the motor deceleration rate within ~~set~~ selected limits to stop the motor and ~~initiates~~ performs the safe operating stop function (see 4.2.4.1) when the motor speed is below a specified limit; or

b) Safe Stop 2 ramp monitored

SS2-r

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

c) Safe Stop 2 time controlled

SS2-t

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

~~NOTE~~ This *safety sub-function* SS2 corresponds to a controlled stop in accordance with stop category 2 of IEC 60204-1.

NOTE The controlled stop of SS2-t can fail undetected, therefore SS2-t cannot be applied if this failure can cause a dangerous situation in the final application.

4.2.4 ~~Other safety~~ Monitoring functions

4.2.4.1 General

In the following function descriptions “prevents” is written when there is a single limit only and “keeps” is written when there is an upper and lower limit. Otherwise there is no difference in intent.

4.2.4.2 Safe operating stop (SOS)

This 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.

4.2.4.3 Safely-limited acceleration (SLA)

This function prevents the motor from exceeding the specified acceleration and/or deceleration limit.

4.2.4.4 Safe acceleration range (SAR)

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

4.2.4.5 Safely-limited speed (SLS)

This function prevents the motor from exceeding the specified speed limit.

4.2.4.6 Safe speed range (SSR)

This function keeps the motor speed within specified limits.

4.2.4.7 Safely-limited torque (SLT)

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

4.2.4.8 Safe torque range (STR)

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

4.2.4.9 Safely-limited position (SLP)

This function prevents the motor shaft (or mover, when a linear motor is used) from exceeding the specified position limit(s).

4.2.4.10 Safely-limited increment (SLI)

This function prevents the motor shaft (or mover, when a linear motor is used) from exceeding the specified limit of position increment.

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

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

4.2.4.11 Safe direction (SDI)

This function prevents the motor shaft from moving more than a defined amount in the unintended direction.

4.2.4.12 Safe motor temperature (SMT)

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

NOTE The SMT *safety sub-function* can be used to protect against over temperature of a motor applied in an explosive atmosphere. Other risks like sparks are not covered by this *safety sub-function*. For further information, see IEC 60079 series of standards. General information for the use of *PDS(SR)* in explosive atmosphere applications is provided in IEC 61800-2:2015.

~~4.2.3.12 Safe brake control (SBC)~~

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

4.2.4.13 Safe cam (SCA)

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

4.2.4.14 Safe speed monitor (SSM)

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

4.2.5 Output functions – Safe brake control (SBC)

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

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.~~

The first objective of this clause is to specify the responsibilities for the management of *functional safety* and the activities to be carried out by those with assigned responsibilities.

The second objective of this clause is to present the *PDS(SR)* development lifecycle and give an overview of its phases.

NOTE ~~This clause is~~ The organizational measures dealt with in this clause provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of *functional safety* of the *PDS(SR)* systems~~ and is~~. Separate and distinct from this are the general health and safety measures necessary for the achievement of safety in the workplace.

5.2 Requirements for the management of *functional safety*

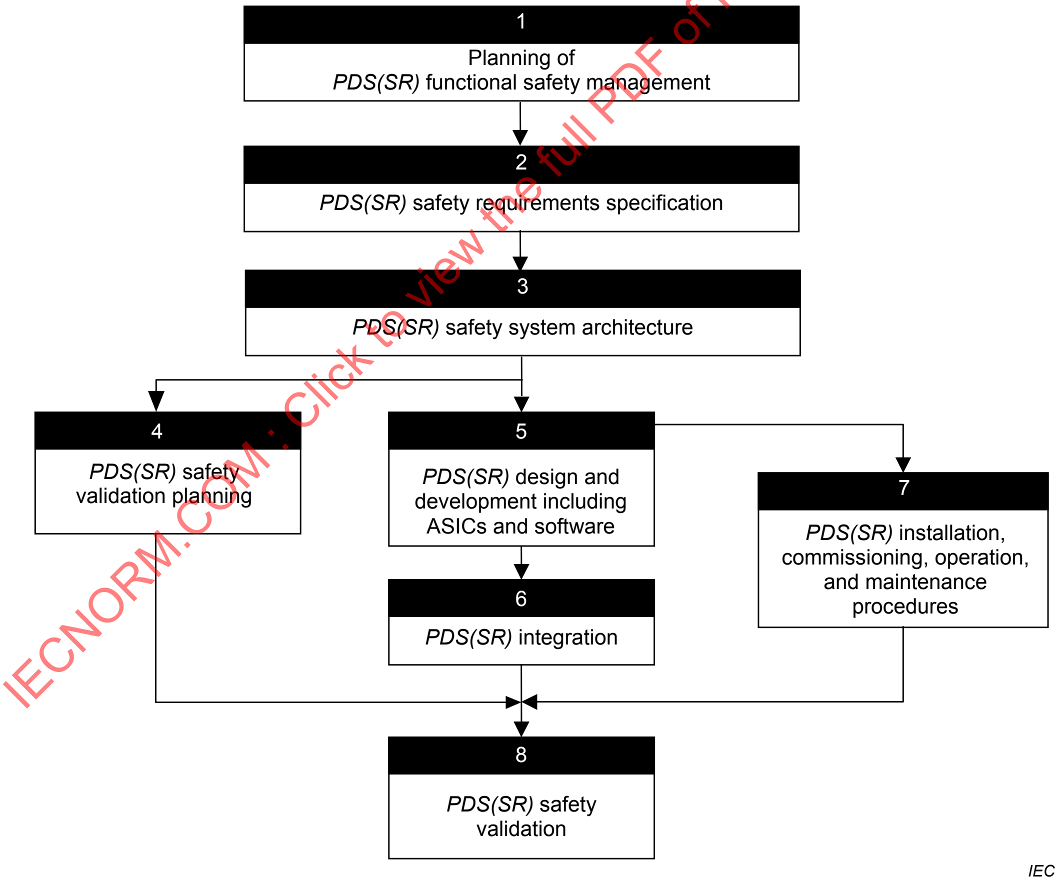
The requirements of Clause 6 of IEC 61508-1:2010 apply.

5.3 *PDS(SR)* development lifecycle

Figure 3 shows the *PDS(SR)* development lifecycle, with cross-references to the relevant sub clauses of this standard, arranged as phase 1 to phase 8.

NOTE This corresponds to the phases, safety requirement specification (phase 9) and realisation (phase 10) of the overall safety lifecycle of IEC 61508-1:2010.

Figure 2 shows this information in the form of a sequential task table.



For phase 1, see 5.4. (phase 9 – see NOTE)	For phase 2, see 5.5. (phase 9 – see NOTE)	For phase 3, see 5.6. (phase 10.1 – see NOTE)	For phase 4, see 5.4 e) (phase 10.2 – see NOTE)
For phase 5, see Clause 6 (phase 10.3 – see NOTE)	For phase 6, see 6.5 (phase 10.4 – see NOTE)	For phase 7, see Clause 7 (phase 10.5 – see NOTE)	For phase 8, see Clause 8 (phase 10.8 – see NOTE)

NOTE Corresponding phase of overall safety lifecycle of IEC 61508-1:2010.

Figure 3 – *PDS(SR)* development lifecycle

5.4 ~~Functional safety~~ Planning of *PDS(SR) functional safety* management

~~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."~~

A plan shall be generated and updated as necessary throughout the entire development of the *PDS(SR)*. It shall define the activities required to satisfy Clauses 5 to 10, and specify persons and their competence, department(s), or organization(s) responsible for completing these activities.

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 5.5), including factors such as:
   - the personnel responsible for generation and maintenance of the *safety requirements specification*;
   - the choice of methods for the avoidance of mistakes during generation of the *safety requirements specification* (see IEC 61508-2:2010, Annex B);
   - the consideration of requirements from guidelines and standards for specific target applications of the *PDS(SR)*;
   - the personnel responsible for *verification* of the *safety requirements specification*;
   - the process for changing the *safety requirements specification* after development has started.

b) Generation of the safety system architecture specification (see 5.6), including factors such as:
   - the personnel responsible for generation and maintenance of the safety system architecture specification;
   - the choice of methods for the avoidance of mistakes during generation of the safety system architecture specification (see IEC 61508-2:2010, Annex B);
   - the consideration of requirements from guidelines and standards for specific target applications of the *PDS(SR)*;
   - the personnel responsible for *verification* of the safety system architecture specification;
   - the process for changing the safety system architecture specification after development has started.

c) Design and development of the *safety sub-function*(s) in the *PDS(SR)*, including (where applicable) factors such as:
   - the personnel responsible for design and development;
   - the selection of product development and project management methodologies (see IEC 61508-7:~~2000~~ 2010, B.1.1);
   - 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)* (e.g. ISO 13849-1 and IEC 62061);
   - the project documentation methodology (see IEC 61508-7:~~2000~~ 2010, B.1.2);
   - the application of structured design techniques (see IEC 61508-7:~~2000~~ 2010, B.3.2);
   - the application of modularization techniques (see IEC 61508-7:2010, B.3.4)
   - the use of ~~simulation or other~~ computer-based design tools (see IEC 61508-7:2010, B.3.5);
   - the design *verification* methodology;

- ~~the integration and functional test techniques, regression testing, and responsible personnel;~~
- the design change management (both hardware and software).

d) A *verification* plan for the *safety sub-function*(s) including factors such as:

- the personnel responsible for *verification*;
- the selection of *verification* strategies, techniques and tools;
- the selection and documentation of *verification* activities;
- the selection and utilization of test equipment;
- the evaluation of *verification* results gained from *verification* equipment and from tests.

e) A *validation* plan for the *safety sub-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 procedures to be applied to validate that each *safety sub-function* of the *PDS(SR)* is correctly implemented, and the pass/fail criteria for accomplishing the tests;
- the procedures to be applied to validate that each *safety sub-function* of the *PDS(SR)* is of the required *safety integrity*, and the pass/fail criteria for accomplishing the tests;
- the required environment in which the testing is to take place including all necessary tools and equipment (also plan which tools and equipment should be calibrated);
- test evaluation procedures (with justifications);
- the test procedures and performance criteria to be applied to validate the specified electromagnetic immunity limits;
- the action to be taken in the event of failure to meet any of 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:

- the personnel responsible for user documentation;
- a list of significant safety-related information which ~~must~~ shall be provided;
- the review process to insure the accuracy of documentation

g) Where assessment is required (see IEC 61508-1:~~1998~~ 2010, Clause 8), a *functional safety* assessment plan ~~comprising the following shall be available~~ providing all information necessary to facilitate an effective assessment and including:

- the scope of the functional safety assessment;
- ~~the personnel responsible for the functional assessment;~~
- the organisations involved;
- the resources required ~~to complete the functional safety assessment activity~~;
- those to perform the *functional safety* assessment;
- the level of independence of ~~the assessment team~~ those performing the *functional safety* assessment;
- the competence of each person involved in the *functional safety* assessment;
- the outputs from the *functional safety* assessment;

- how the *functional safety* assessment relates to, and shall be integrated with, other *functional safety* assessments where appropriate;
- the requirement to perform an impact analysis to determine which parts of the assessment are to be repeated in case of a modification (see also IEC 61508-1:2010, 7.16.2)
- ~~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 means by which the functional safety assessment shall be revalidated after modifications to the PDS(SR).~~

In establishing the scope of each *functional safety* assessment, it will be necessary to specify the documents, and their revision status, that are to be used as inputs for each assessment activity.

NOTE The plan can be made by either those responsible for *functional safety* assessment or those responsible for management of *functional safety*, or can be shared between them.

5.5 Safety requirements specification (*SRS*) for a *PDS(SR)*

5.5.1 General

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

- a *safety* ~~*functionality*~~ *sub-functions* requirements specification (see 5.5.2); and
- a *safety integrity* requirements specification (see 5.5.3).

These shall be ~~written so~~ expressed and structured in such a way that they are:

- clear, precise~~, uniquivocal~~, unambiguous, feasible, verifiable, testable and maintainable;
- written to aid the comprehension by those who are likely to utilise the information at any stage of the *PDS(SR)* safety lifecycle;
- expressed in natural or formal language and/or logic, sequence or cause and effect diagrams that define the necessary *safety sub-functions* with each *safety sub-function* being individually defined.

For the avoidance of mistakes during the compilation of these specifications, appropriate techniques and measures shall be applied (see IEC 61508-2:~~2000~~ 2010, Table B.1).

The requirements for safety-related hardware and software shall be reviewed to ensure that they are adequately specified.

5.5.2 *Safety* ~~*functionality*~~ *sub-functions* requirements specification

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

The *safety* ~~*functionality*~~ *sub-functions* requirements specification shall describe, as appropriate:

a) all *safety sub-functions* to be performed;

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

b) comprehensive detailed requirements sufficient for the design and development of the *PDS(SR)* including all the normative requirements to be fulfilled;

NOTE Requirements like the selected measures of fault avoidance and fault control and the selected measures and techniques for software design and testing etc. can be included in *safety sub-functions* requirement specification.

c) the applicable *mode of operation* regarding *functional safety*;

d) the manner in which the *PDS(SR)* is intended to achieve or maintain a safe state for intended applications;

e) the operating modes of the *PDS(SR)* and its *installation* – for example setting, start-up, maintenance, normal intended operation;

f) all required modes of behaviour of the *PDS(SR)*;

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

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

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

j) 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*);

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

l) 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.

m) 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*);

n) all interfaces, necessary for *functional safety*, between the *PDS(SR)* and any other systems (either directly associated within, or outside, the *installation*).

5.5.3 *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-related functions), ~~both a~~ *SIL capability* (or *SIL*) and ~~a maximum probability~~ an upper limit of ~~dangerous random hardware failure~~ *PFH* value.

NOTE 1 *SIL capability* is relevant if the *PDS(SR)* is to be considered as a component which implements a *safety sub-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 sub-function*. However, it ~~may~~ can also be higher, if the *PDS(SR)* is to be used to implement the *safety sub-function* in a redundant configuration with other components.

NOTE 3 Where a *PDS(SR)* implements a *safety sub-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 sub-function*, and the *safety sub-functions* are used simultaneously, the probability of dangerous random hardware failure of the common hardware ~~should~~ can 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 sub-function* is required for more than one axis, the probability of dangerous random hardware failure of common hardware ~~should~~ can be considered only once when determining the overall probability of dangerous random hardware failure.

b) the required *mission time*;

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

NOTE 6 This information~~ may~~ can 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.

d) any requirement for increased EM immunity (see 6.2.6);

e) limiting and constraint conditions for the realisation of *PDS(SR)* due to the possibility of *common cause failure*s;

f) the quality assurance/quality control measures necessary for management of functional safety (see IEC 61508-1:2010, Clause 6).

5.6 *PDS(SR)* safety system architecture specification

5.6.1 General

5.6.1.1 The objective of the safety system architecture specification is to specify the architectural decomposition of the *PDS(SR)* and the requirements for the resulting *subsystems* and parts of *subsystems* (see Annex A).

NOTE 1 The Safety system architecture specification is normally derived from the *PDS(SR)* safety requirement specification by decomposing the *safety sub-function*s and allocating parts of the *safety sub-function*s to *subsystem*s (for example *safety sub-function* logic, input/output circuitry, power supply, software). The representation of the *PDS(SR)* in form of *subsystems* describes the *PDS(SR)* on an architectural level which allows the specification of the requirements for these *subsystem*s. The requirements can be included in the safety system architecture specification or kept separate and referenced by the safety system architecture specification. The *subsystem*s can be further decomposed to parts to satisfy the design and development requirements.

NOTE 2 A more general approach to this kind of specification is given in IEC 61508-2:2010 as an E/E/PE system design requirement specification.

5.6.1.2 The description of the *subsystems* and parts and the respective requirements shall be expressed and structured in such a way that they are:

- clear, precise, unambiguous, feasible, verifiable, testable and maintainable;
- written to aid the comprehension by those who are likely to utilise the information at any stage of the *PDS(SR)* safety lifecycle;
- traceable to the *PDS(SR) safety requirements specification*.

5.6.2 Requirements for safety system architecture specification

5.6.2.1 The safety system architecture specification shall contain design requirements related to *safety sub-functions* and to *safety integrity*.

5.6.2.2 The safety system architecture specification shall contain details of all hardware and software necessary to implement the required *safety sub-functions*, as specified by the *safety sub-functions requirements specification* of the *PDS(SR)* (see 5.5.2). The architecture shall include, for each *safety sub-function*:

a) requirements for the *subsystem*s and parts as appropriate;

b) requirements for the integration of the *subsystem*s and parts to meet the *PDS(SR)* safety requirement specification;

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

d) accuracy and stability requirements for measurements and controls;

e) safety-related *PDS(SR)* and operator interfaces;

f) interfaces between the *PDS(SR)* and any other systems (either within, or outside, the *installation*);

g) all modes of behaviour of the *PDS(SR)*, in particular, failure behaviour and the required response (for example alarms, automatic shut-down) of the *PDS(SR)*;

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

i) any limiting and constraint conditions for the *PDS(SR)* and its associated subsystems, for example timing constraints or constraints due to the possibility of *common cause failure*s;

j) any specific requirements related to the procedures for starting-up and restarting the *PDS(SR)*.

5.6.2.3 The safety system architecture specification shall contain details, relevant to the design, to achieve the *safety integrity level* for the *safety sub-function*, as specified by the *PDS(SR) safety integrity* requirements specification (see 5.5.3), including:

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

b) all relevant reliability modelling parameters such as the required *diagnostic test* interval of the hardware necessary to achieve the target failure measure;

5.6.2.4 The *PDS(SR)* safety system architecture specification shall be completed in detail as the design progresses and updated as necessary after modification.

5.6.2.5 For the avoidance of mistakes during the development of the specification for the *PDS(SR)* safety system architecture specification, an appropriate group of techniques and measures according to IEC 61508-2:2010, Table B.2 shall be used.

5.6.2.6 The implications imposed on the architecture by the *PDS(SR)* safety system architecture specification shall be considered.

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

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 *hazard*ous 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~~ cannot 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 parts of the IEC 61800 series, listed in the normative references.

6.1.3 Realisation

The *PDS(SR)* shall be realised in accordance with its *safety requirements specification* (see 5.5).

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 6.2.3), and

  – the requirements for the ~~probability of dangerous random hardware failures per hour~~ *PFH* value (see 6.2.2 or 6.2.3);

b) the requirements for *systematic safety integrity* comprising:

- the requirements for the avoidance of failures (see 6.2.5.1), and the requirements for the control of systematic faults (see 6.2.5.2), or
- evidence that components used are 'proven-in-use'. In this case the components shall fulfil the relevant requirements of IEC 61508-2:2010

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

NOTE If PL and category are to be claimed refer to ISO 13849-1:2006, 6.2 additionally.

6.1.5 Safety and non-*safety sub-functions*

Where a PDS(SR) is to perform both safety and non-*safety sub-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)~~ adequate design measures ensure that the failures of non-*safety sub-functions* cannot adversely affect *safety sub-functions*.

See IEC 61508-3:2010, Annex F, for techniques for achieving non-interference between software parts on a single computer.

~~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~~ for multiple *safety sub-functions* within one *PDS(SR)*

The *safety integrity level* of one *safety sub-function* can be different from the others, and the requirements for design of each *safety sub-function* are defined as follows.

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

As an example see Table 2:

Table 2 – Example for determining the *SIL* from hardware and software independence

***PDS(SR)* implementing two *safety sub-functions* (Y and Z) with different *SIL* requirements: Function Z: *SIL* H[a] / function Y: *SIL* L[a]**				
Design type	**Evidence of sufficient independence between *safety sub-functions* Y and Z**		**Final *SIL* requirement for *safety sub-function***	
	for hardware	**for software**	**Z**	**Y**
Hardware (HW) **and** software (SW) design	Yes	Yes	*SIL* H	*SIL* L
	No	Yes	SW: *SIL* H HW: *SIL* H	SW: *SIL* L HW: *SIL* H [b]
		No	*SIL* H	*SIL* H
	Yes	No	SW: *SIL* H HW: *SIL* H	SW: *SIL* H [b] HW: *SIL* L
Hardware **only** design	Yes	not applicable	*SIL* H	*SIL* L
	No		*SIL* H	*SIL* H [b]

[a] with *SIL* H higher than *SIL* L

[b] HW and/or SW separation is not sufficient

~~NOTE~~ Sufficient independence ~~may~~ shall be established by showing that the probability of a dependent failure between the parts implementing *safety sub-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 sub-functions* involved.

6.1.7 Integrated circuits with on-chip redundancy

Digital ICs which implement on-chip redundancy with the goal of increasing fault tolerance in a *PDS(SR)* shall satisfy all of the special requirements for ICs with on-chip redundancy according to IEC 61508-2:2010, Annex E, in case of duplicated circuitry. Alternatively a justification shall be given that the same level of independence between different channels is achieved by applying a different set of measures.

6.1.8 Software requirements

If software is used to implement a *safety sub-function* of the *PDS(SR)* with a specific *SIL* or *SIL capability* (see 5.5.3), then this software shall be implemented in accordance with the requirements defined by IEC 61508-3:2010 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~~ capability (for example failure mode and effects analysis, fault tree analysis).

6.2 *PDS(SR)* design requirements

6.2.1 Basic and well-tried safety principles

Basic and well-tried safety principles shall be considered where applicable when a category is claimed for the *PDS(SR)*.

- For electrical and electro-mechanical *PDS(SR)*, these principles correspond to ISO 13849-2:2012, Table D.1 and Table D.2
- For mechanical parts (e.g. encoders), these principles correspond to ISO 13849-2:2012, Table A.1 and Table A.2

6.2.2 Requirements for the estimation of the probability of dangerous random hardware failures per hour (*PFH*)

6.2.2.1 General requirements

6.2.2.1.1 *PFH* for each *safety sub-function*

The *PFH* of each *safety sub-function* (or group of simultaneously ~~used~~ activated *safety sub-functions*) to be performed by the *PDS(SR)*, estimated according to 6.2.2.1.2 and Annex B, shall be equal to or less than the target failure measure (see Table 3) as specified in the *safety integrity* requirements specification (see 5.5.3).

The *PFH* value as defined by the *SIL* refers to a complete *safety sub-function*. If a *PDS(SR)* is intended to perform only a part of a *safety sub-function* within a safety related control system then the *PFH* of the ~~drive~~ *PDS(SR)* 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 sub-function* (see IEC 61508-1:~~1998~~ 2010, Table 3), unless there is a requirement in the *PDS(SR) safety integrity* requirements specification (see 5.5.3) for the *safety sub-function* to meet a specific target failure measure, rather than a specific *SIL*.

Table 3 – *Safety integrity levels*: target failure measures for a *PDS(SR) safety sub-function*

Safety integrity level SIL	*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 sub-function* (or group of simultaneously ~~used~~ activated *safety sub-functions*) of the *PDS(SR)* shall be estimated separately.

NOTE 1 Different *safety sub-functions* ~~may~~ can have common components and/or unique components, resulting in different *PFH* for each *safety sub-function* (or group of simultaneously used *safety sub-functions*).

NOTE 2 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);
- parts count (see IEC 61709:2011);
- procedure description (see IEC 61508-6:2010);

– simplified procedure for estimating PL (see ISO 13849-1:2006, 4.5.4).

See also IEC 60300-3-1.

NOTE 3 The mean time to restoration (see IEC 60050 ~~191-13-08~~ 192-07-23) 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 4 Failures due to common cause effects and data communication processes ~~may~~ can 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 IEC 61508-6:2000, Annex D).

~~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.~~

NOTE 5 If PL is to be claimed refer to ISO 13849-1:2006, Table 3, additionally.

6.2.2.1.2 Estimation of *PFH*

The *PFH* of each *safety sub-function* (or group of simultaneously ~~used~~ activated *safety sub-functions*) to be performed by the *PDS(SR)*, due to random hardware failures shall be estimated using IEC 61508-2:~~2000~~ 2010, Annex A, taking into account:

a) the architecture of the *PDS(SR)* as it relates to each *safety sub-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 failure*s (see IEC 61508-6:~~2000~~ 2010, Annex D);

e) the *diagnostic coverage* (DC) of the *diagnostic tests* (determined according to IEC 61508-2:~~2000~~ 2010, Annex A and Annex C) and the associated *diagnostic test* interval,

~~NOTE 1~~ and 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.~~

f) the repair times for detected failures;

NOTE 1 The repair time will constitute one part of the mean time to restoration (see ~~IEV 191-13-08~~ IEC 60050-192:2015, 192-07-23), 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~~ 2010 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~~ equipment or machinery driven by the *PDS(SR)* 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.

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

NOTE 2 For information about estimation of the $\mathrm{PFD}_{\mathrm{avg}}$ value from the *PFH* value for low demand applications, see Annex F.

6.2.2.1.3 Failure rate data

Component failure rate data shall be obtained from:

– a recognised source; or

– estimate~~s~~ based upon those Type A components that are considered to be “proven in use” (see IEC 61508-2:~~2000~~ 2010, 7.4.10).

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

~~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~~ can be used.

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

NOTE 2 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~~ can 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 3 The fault lists given in Annex D can be used to assist in determination of failure modes.

Any failure rate data used shall have a confidence level of at least ~~60~~ 70 %.

6.2.2.1.4 *Diagnostic test* interval when the hardware fault tolerance is greater than zero

The *diagnostic test* interval of any *subsystem* of the *PDS(SR)* shall be ~~such as to enable the PDS(SR)~~ appropriate to meet ~~the requirement for~~ the required *PFH* (see 6.2.2.1.1).

~~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).~~

NOTE 1 For information regarding mathematical impact of diagnostic test interval see Clause B.4

NOTE 2 For redundant parts of a *PDS(SR)* which cannot be tested without disrupting the application in which the *PDS(SR)* is used (machine or plant) and where no justifiable technical solution can be implemented, the following maximum diagnostic test intervals can be considered as acceptable:

- one test per year for *SIL* 2, PL d / category 3;
- one test per three months for *SIL* 3, PL e / category 3;
- one test per day for *SIL* 3, PL e / category 4.

PL and category according to ISO 13849-1.

6.2.2.1.5 Diagnostic test interval when the hardware fault tolerance is zero

The *diagnostic test* interval of any *subsystem* of a *PDS(SR)* having a hardware fault tolerance of zero, on which a *safety sub-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~~ process safety time.

6.2.3 Architectural constraints

6.2.3.1 Limitations of *SIL*

In the context of hardware *safety integrity*, the highest *safety integrity level* that can be claimed for a *safety sub-function* is limited by the hardware fault tolerance and *safe failure* fraction of the *subsystems* of a *PDS(SR)* that carry out that *safety sub-function*. A hardware fault tolerance of *N* means that *N*+1 faults could cause a loss of the *safety sub-function*. Table 4 and Table 5 specify the highest *safety integrity level* that can be claimed for a *safety sub-function* which uses a *subsystem*, taking into account the hardware fault tolerance and *safe failure* fraction of that *subsystem* (see IEC 61508-2:~~2000~~ 2010, Annex C). The requirements of Table 4 or Table 5, whichever is appropriate, shall be applied to each *subsystem* carrying out a *safety sub-function* and hence every part of the *PDS(SR)*; 6.2.3.2.2 and 6.2.3.2.3 specify which one of Table 4 or Table 5 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 Clause D.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~~ can 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~~ can 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.~~

NOTE 3 This clause is based on route 1_H of IEC 61508-2:2010, 7.4.4; for the requirements related to route 2_H see IEC 61508-2:2010, 7.4.4.3.

6.2.3.2 Type A and Type B *subsystems*

6.2.3.2.1 General

(See also IEC 61508-2:2010; 7.4.4.1.2 and 7.4.4.1.3)

6.2.3.2.2 Type A

A *subsystem* can be regarded as type A if, for the components required to achieve the *safety sub-function*, the following criteria are satisfied:

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 failures* are met.

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

6.2.3.2.3 Type B

A *subsystem* shall be regarded as type B if, for the components required to achieve the *safety sub-function*, one or more of the criteria of 6.2.3.2.2 ~~is~~ are 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~~ shall be regarded as type B rather than type A.

NOTE 1 For example, the control section consisting of microcontrollers etc. is considered as a type B *subsystem*.

NOTE 2 Clause D.3 lists faults and fault exclusions that ~~may~~ can be considered.

6.2.3.3 Architectural constraints

The architectural constraints of either Table 4 or Table 5 shall apply: Table 4 applies for every type A *subsystem* forming part of the *PDS(SR)*; Table 5 applies for every type B *subsystem* forming part of the *PDS(SR)*.

NOTE For information about type A and type B refer to IEC 61508-2:2010, 7.4.4.1.2 and 7.4.4.1.3

Table 4 –~~ Hardware safety integrity: architectural constraints on type A safety-related *subsystems*~~
Maximum allowable safety integrity level for a *safety sub-function* carried out by a type A safety-related *subsystem*

***Safe failure* fraction** [a]	**Hardware fault tolerance *N* (see 6.2.3.1)**		
	0	**1**	**2**
< 60 %	*SIL* 1	*SIL* 2	*SIL* 3
60 % to < 90 %	*SIL* 2	*SIL* 3	*SIL* 3~~[b]~~
90 % to < 99 %	*SIL* 3	*SIL* 3~~[b]~~	*SIL* 3~~[b]~~
≥ 99 %	*SIL* 3	*SIL* 3~~[b]~~	*SIL* 3~~[b]~~

[a] See 6.2.4 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 5 ~~– Hardware safety integrity: architectural constraints on type B safety-related *subsystems*~~
Maximum allowable safety integrity level for a *safety sub-function* carried out by a type B safety-related *subsystem*

***Safe failure* fraction** [a]	**Hardware fault tolerance *N* (see 6.2.3.1)**		
	0	**1**	**2**
< 60 %	Not ~~allowed~~ permitted	*SIL* 1	*SIL* 2
60 % to < 90 %	*SIL* 1	*SIL* 2	*SIL* 3
90 % to < 99%	*SIL* 2	*SIL* 3	*SIL* 3~~[b]~~
≥ 99 %	*SIL* 3~~[b]~~	*SIL* 3~~[b]~~	*SIL* 3~~[b]~~

[a] See 6.2.4 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.~~

Exception:

For a *subsystem* with a hardware fault tolerance of zero and where fault exclusions have been applied to faults of electrical or electronic parts that could lead to a *dangerous failure*, then the maximum *SIL* that can be claimed due to architectural constraints of that *subsystem* is limited to:

- *SIL* 3, if tables D.1, D.3, D.5, D.6, D.7 and D.8 apply
- *SIL* 2 in all other cases.

NOTE If category is to be claimed refer to ISO 13849-1:2006, 6.2 additionally.

6.2.4 Estimation of *safe failure fraction (SFF)*

6.2.4.1 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).

For calculation of *SFF* see IEC 61508-2:2010, Annex A and Annex C

For *PDS(SR)* the route 1_H is preferred. Route 2_H shall be restricted for *PDS(SR)* to Type A *subsystems*.

NOTE This clause is based on route 1_H of IEC 61508-2:2010, 7.4.4.2; for the requirements related to route 2_H see IEC 61508-2:2010, 7.4.4.3.

Basis of data is given in 6.2.2.1.3.

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

~~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.~~

~~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.~~

6.2.5 Requirements for *systematic safety integrity* of a *PDS(SR)* and *PDS(SR) subsystems*

6.2.5.1 Requirements for the avoidance of failures

6.2.5.1.1 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)* according to IEC 61508-2:2010, Table B.2.

Tests, as planned according to 6.2.5.1.4, shall be performed. See also Clause 9.

NOTE For claiming a PL refer to ISO 13849-1:2006, Annex G.

6.2.5.1.2 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*.

6.2.5.1.3 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 *subsystem*s 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.

6.2.5.1.4 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 7.2).

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.

6.2.5.1.5 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.

6.2.5.2 Requirements for the control of systematic faults

6.2.5.2.1 General

NOTE For claiming a PL refer to ISO 13849-1:2006, Annex G.

6.2.5.2.2 Design features

For controlling systematic faults, the design shall ~~possess~~ provide features that make the *PDS(SR)* and its *subsystem*s 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~~ according IEC 61800-2:2015, Table 6 as applicable for the environment specified for the *PDS(SR)*;

c) electromagnetic disturbances, see 6.2.6;

d) mistakes made by the operator of the *PDS(SR)* (see IEC 61508-2:~~2000~~ 2010, Clause A.3 and Table A.17);

e) residual design faults in the software (see IEC 61508-3:~~1998~~ 2010, 7.4.3 and associated table);

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

When application specific integrated circuits (ASICs) are used to implement *safety sub-functions* in a *PDS(SR)*, an appropriate group of techniques and measures that are essential to prevent the introduction of faults during the design and development shall be used. The informative Annex F of IEC 61508-2:2010, provides an example of techniques and measures. The related ASIC development lifecycle is shown in IEC 61508-2:2010, Figure 3.

6.2.5.2.3 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)*.

6.2.5.2.4 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.

6.2.5.2.5 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 IEC 61508-7:~~2000~~ 2010, B.4.8.

6.2.5.2.6 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 sub-function*s of the *PDS(SR)*) via plausibility checks.

NOTE See IEC 61508-7:~~2000~~ 2010, B.4.6 and B.4.9.

6.2.5.2.7 *PDS(SR)* parameterization

Almost all *PDS(SR)* need configuration parameters which determine the behaviour of *safety sub-function*s. The software-based parameterization shall be considered as a safety-related aspect of the *PDS(SR)* design to be described in the software *safety requirements specification*.

Parameterization during act of installing and maintenance shall be carried out using a dedicated parameterization tool provided by the supplier of the *PDS(SR)*. This tool shall have its own identification (name, version, etc.) and shall prevent unauthorized modification, for example, by use of a password. There are no *functional safety* requirements to be fulfilled by this parameterization tool.

A special procedure shall be used for setting the safety-related parameters. This procedure shall include confirmation of input parameters to the *PDS(SR)* by

- retrieval, display and check by operator of the modified parameters and
- a *verification* of the correctness of the parameters in the *PDS(SR)* by
  - a configuration test (see 7.2) or
  - other suitable means defined by the *PDS(SR)* manufacturer

as well as subsequent documented confirmation of the safety-related parameters, e.g. by a suitably skilled person and by means of an automatic check by a parameterization tool.

NOTE 1 For reference, see IEC 61508-3:2010, 7.4.4.

NOTE 2 This is of particular importance where parameterization is carried out using a device not specifically intended for the purpose (e.g. personal computer or equivalent).

NOTE 3 For more details on software-based parameterization see ISO 13849-1:2006, 4.6.4 and/or IEC 62061:2012, 6.11.2.

6.2.5.2.8 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.~~

6.2.6 Design requirements for electromagnetic (EM) immunity of a *PDS(SR)*

The *PDS(SR)* shall be designed to have the appropriate EM immunity for operating within the specified or anticipated electromagnetic environment (first environment or second environment) as classified in IEC 61800-3.

The EM immunity test requirements are described in 9.2 and Annex E.

6.2.7 Design requirements for thermal immunity of a *PDS(SR)*

The *PDS(SR)* shall be designed to have the appropriate thermal immunity for operating within the specified or anticipated thermal environment as classified in IEC 61800-2.

The thermal immunity test requirements are described in 9.4.

6.2.8 Design requirements for mechanical immunity of a *PDS(SR)*

The *PDS(SR)* shall be designed to have the appropriate mechanical immunity for operating within the specified or anticipated mechanical environment as classified in IEC 61800-5-1 and IEC 61800-2.

The mechanical immunity test requirements are described in 9.5.

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 sub-function* is detected, a *fault reaction function* shall be initiated in order to prevent a *hazard*. Diagnostics and *fault reaction function*s 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 sub-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 sub-function* within a *PDS(SR)* 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 sub-function* due to random failures (see 6.2.1.1.2). This does not cover all data communication within a *PDS(SR)*. For example data communication within one printed wiring board is not covered by this requirement.

For details see IEC 61508-2:2010, 7.4.11.

NOTE Additional information regarding safety communication channels can be found in IEC 61784-3.

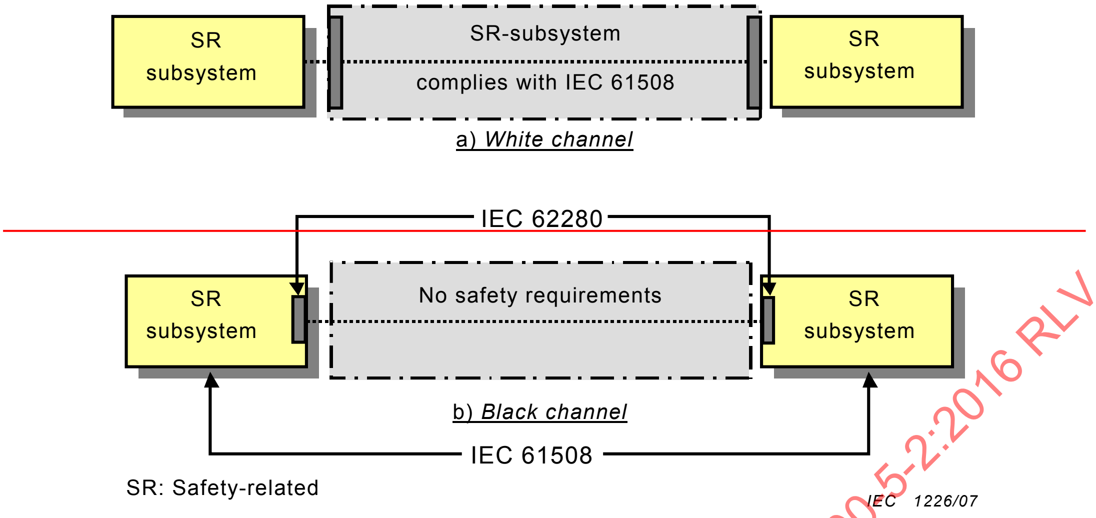
~~NOTE The term masquerade means that the true contents of a message are not correctly identified. For example, a message from a non-safety component is incorrectly identified as a message from a safety component.~~

~~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 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 61508-3:2010. 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 IEC 61508-7:~~2000~~ 2010, B.5.2) ~~may~~ can suffice. Static analysis (see IEC 61508-7:~~2000~~ 2010, B.6.4), dynamic analysis (see IEC 61508-7:~~2000~~ 2010, B.6.5) or failure analysis (see IEC 61508-7:~~2000~~ 2010, B.6.6) ~~may~~ can 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 sub-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 General

PDS(SR) manufacturers shall provide information for the users in a safety manual. General requirements of the safety manual are referred to IEC 61508-2:2010, Annex D, and IEC 61508-3:2010, Annex D. This clause describes additional requirements for a *PDS(SR)*.

NOTE For claiming a PL refer to ISO 13849-1:2006, Clause 11.

7.2 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 *safety sub-function* and interface which is available for use in the implementation of *safety sub-functions*. This shall comprise:

   - a detailed description of the *safety sub-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 sub-function* is intended to be active or disabled;
   - the priority of those ~~functions~~ *safety sub-function* that are simultaneously active and can conflict with each other.

b) The *safety integrity* information for each *safety sub-function*, including:

   - the *SIL* or *SIL* capability; (includes systematic capability, see IEC61508-2);
   - the PFH value for each *safety sub-function*;
   - resulting PFH-value for a group of simultaneously activated *safety sub-functions*;
   - PL and category according to ISO 13849-1 when applicable.

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, IEC 61800-2, IEC 61800-3, IEC 61800-4 and IEC 61800-5-1). This shall take into account storage, transport, ~~installation~~ act of installing, commissioning, testing, operation and maintenance.

   NOTE As an example for an EMC related information for use: "Warning: handheld radio transmitters held closer than 20 cm to *PDS(SR)* can disturb the *safety sub-functions* of the *PDS(SR)*" or similar (see E.2, footnote p)

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 (e.g. limited number of operations of a relay);
- any limits on the application of the *PDS(SR)* which should be observed in order to avoid *systematic failure*s;
- ~~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.~~
- any information valid hardware and software versions and the combinations permitted for the *safety sub-functions;* the fact that *safety sub-function*s cannot prevent any failure of non-*safety sub-function*s of the *PDS(SR).*

  NOTE 1 For example, the failure of deceleration initiated by SS1-t is not prevented.

  NOTE 2 For example, while function STO is active, a limited amount of movement is still possible in the event of failure in the power section of the *PDS(SR).*

e) The~~ installation~~ act of installing and commissioning guidance (see IEC 61800-5-1:~~2003~~ 2007, Clause 6), including setting and parameterisation.

f) The requirements for configuration test of *safety sub-functions*, in cases where the integrity of the means of configuration of a *safety sub-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 sub-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 sub-functions* that will be used in the application of the *PDS(SR)*;
- the results of each test of these *safety sub-function*s, 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 sub-function*s 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;
- the routine actions which need to be carried out to maintain the *functional safety* of the application of the *PDS(SR)*, including the compatibility of hardware and software versions and safety parameters such as *PFH* and *SIL*

NOTE The *PDS(SR)* operation and maintenance procedures ~~should~~ can 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~~ *PDS(SR)* development lifecycle (see 5.3).

NOTE If PL is to be claimed refer to ISO 13849-1 and/or ISO 13849-2.

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.~~

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

The requirements of IEC 61508-2:2010, 7.9.2 apply.

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.~~

The objective of the requirements of this subclause is to validate that the *PDS(SR)* meets in all respects the requirements for safety in terms of the required *safety sub-function*s and *safety integrity*.

The requirements of IEC 61508-2:2010, 7.7.2 apply.

8.4 Documentation

Appropriate documentation concerning *PDS(SR) verification* and *validation* shall be produced, according to the appropriate requirements of 8.2 and 8.3 ~~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 sub-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 sub-function*;

b) the functional testing of each diagnostic~~s~~ function for each *safety sub-function*; (fault insertion testing);

c) the environmental testing of each *safety sub-function* for immunity to each of the following environmental stresses:

   1) electromagnetic (EM)

   2) thermal

   3) mechanical (shock & vibration)

d) the acceptance criteria.

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

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

NOTE When it is difficult to perform *safety sub-function* tests on the complete *PDS(SR)* because of e.g. size, parts of the *PDS(SR)* that are considered to be safety-relevant can be tested individually.

9.2 Functional testing

Functional testing of each *safety sub-function*, including related diagnostics (fault insertion testing), shall be performed.

9.3 Electromagnetic (EM) immunity testing

9.3.1 General

The performance criterion that shall be applied when performing EM immunity tests on the *PDS(SR)* is specified in 9.3.3. This criterion does not apply to the normal (non-safety related) functions of the equipment.

NOTE Functional electromagnetic compatibility (EMC) of the *PDS(SR)* is achieved when it complies with the requirements of IEC 61800-3.

9.3.2 Intended EM environment

Where the EM environment is not known or not declared by the *PDS(SR)* manufacturer or the intended environment is the second environment, the *PDS(SR)* shall be verified to the immunity requirements given in the second environment columns of Tables E.1, E.2 and E.3.

When the environment of the intended use of the *PDS(SR)* is the first environment, the *PDS(SR)* shall be verified to the immunity requirements given in the first environment columns of Tables E.1 and E.3.

The performance criterion of 9.3.3 shall be applied.

The specified mitigation measures shall be in place during the tests to verify their effectiveness.

9.3.3 Performance criterion (fail safe state – FS)

The following performance criterion shall be satisfied while the *PDS(SR)* exercises all safety-related hardware parts during the tests. The behaviour of non-safety related functions of the *PDS(SR)* are not considered, unless non-safety related components are used as indicators of the *safety sub-functions* and have been verified to be operating properly.

Additionally no hazards shall be introduced by the *PDS(SR)* when the EM immunity tests are applied.

Safety sub-functions of the *PDS(SR)*:

- do not deviate outside their specified limits for *functional safety* (equal to criterion A of IEC 61800-3), 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 (fail safe state) of the *PDS(SR)* is maintained or achieved within the specified maximum fault reaction time.

Permanent degradation of the *safety sub-function* or destruction of components is permitted provided a defined safe state shall be 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.

9.4 Thermal immunity testing

9.4.1 General

Thermal immunity testing of each *safety sub-function*, including related diagnostics, shall be performed.

9.4.2 Functional thermal test

The test shall be performed according to the temperature rise test of IEC 61800-5-1:2007 to determine that each *safety sub-function* of the *PDS(SR)* works properly under the rated temperature operating conditions.

9.4.3 Component thermal test

For all components of each *safety sub-function*, the component manufacturer's specified maximum operating temperature shall not be exceeded during the test.

NOTE 1 Testing whether all safety-related components are operated in the specified temperature range when the *PDS(SR)* is applied to its specified minimum and maximum ambient temperatures can be performed at a lower temperature than the rated maximum ambient air temperature of the *PDS(SR)*. The maximum temperatures attained during testing can be corrected to the maximum rated ambient temperature for the *PDS(SR)* by adding the difference between the ambient temperature during the test and the maximum rated ambient temperature for the *PDS(SR)*.

NOTE 2 IEC 61800-5-1 provides information regarding thermal test methods.

9.5 Mechanical immunity testing

9.5.1 General

Shock and vibration immunity testing of each *safety sub-function*, including related diagnostics, shall be performed.

9.5.2 Vibration test

Testing shall be performed according to the test conditions of the vibration test of IEC 61800-5-1:2007, except that the *PDS(SR)* shall be powered and each *safety sub-function* shall be verified while operating.

9.5.3 Shock test

Testing shall be performed according to the test conditions of the shock test of IEC 61800-2:2015, except that the *PDS(SR)* shall be powered and each *safety sub-function* shall be verified while operating.

9.5.4 Performance criterion for mechanical immunity tests (fail safe state – FS)

Safety sub-functions of the *PDS(SR)*:

- 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 mechanical disturbance in such a way that a defined safe state (fail safe state) of the *PDS(SR)* is maintained or achieved within the specified maximum fault reaction time.

9.6 Test documentation

During *PDS(SR)* testing for *safety sub-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~~ model 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~~ pass/fail status of the test. If the test has failed, the mode of failure shall be documented.

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

10.2.1 General

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.

10.2.2 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~~ modification;

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

NOTE For the selection of appropriate techniques to implement the requirements for software modifications, see IEC 61508-3:2010, Table A.8.

10.2.3 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~~ performed.

10.2.4 Authorization

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

10.2.5 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~~ modifications;

d) the test cases for components including re*validation* data;

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

f) the deviation from previous operations and conditions;

g) the necessary ~~changes~~ modifications 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 in Table A.1 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~~ architecture" 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~~ can 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.~~

Table A.1 – Design and development procedure for *PDS(SR)*

	Tasks	References
1	**General requirements**	
	All relevant documents should be under the control of an appropriate document control scheme ~~Description of project management~~ ~~Certification~~ Software quality management system **Safety Concept:** a) Hardware design on an architectural level, including – Block diagrams of safety related hardware – User and process interfaces – Safety relevant signal paths – Power supply – Separation of independent channels to achieve fault tolerance – Communication links between independent channels to achieve diagnostic coverage b) Software design on an architectural level, including: – description of the functions provided by the safety related software – interaction with hardware – state machine diagrams of the intended behaviour of the software – user and process interfaces – fault detection possibilities and fault reactions – overview of software structure, for example with block diagram – control and storage of safety related data – version procedures – used tools, for example compiler, code checker, etc.	IEC 61508-1:~~1998~~ 2010, Clause 5 ~~IEC 61508-2:2000, §7.3, 7.7, 7.8, 7.9~~ IEC 61508-3:~~1998~~ 2010, Clause 6 ~~7.3, 7.4.2.1, 7.7, 7.8, 7.9~~ Phase 3 of *PDS(SR)* safety lifecycle (see 4.2 of this standard) a) See Clause 5 of this standard IEC 61508-2:2000, 7.4, Annex A, Tables B.2, B.6 Examples in IEC 61508-6:2000, Annexes A and D b) IEC 61508-2:2000, 7.2.3.1(h) IEC 61508-3:2010, 7.2.2.8, 7.2.2.10, 7.4.2, 7.4.3, Tables A.2, B.1, B.7, B.9 IEC 61508-7:2000, Table C.1

	Tasks	References
2	**Planning of *PDS(SR) functional safety* management**	Phase 1 of *PDS (SR)* safety lifecycle (see 5.3 and 5.4 of this standard)
	Generation of a plan which defines the activities required to satisfy Clauses 5 to 10 of this standard and identifies persons, department(s), or organization(s) responsible for completing these activities. "Plan shall be updated as necessary throughout the entire development of the *PDS(SR)*"	See 5.4 of this standard IEC 61508-1:2010, 6.2 IEC 61508-3:2010, 6.2
3	**Specification of *PDS(SR)* safety requirements**	Phase 2 of PDS(SR) safety lifecycle (see 5.3 and 5.5 of this standard)
	Development of a safety requirements specification (SRS) including *safety sub-functions* requirements and *safety integrity requirements*	See 5.4 of this standard IEC 61508-1:~~1998~~ 2010, 7.5, 7.10 IEC 61508-2:~~2000~~ 2010, 7.2, Tables B.1, B.6 IEC 61508-2:~~2000~~ 2010, 7.4.6 to 7.4.8, Annex A IEC 61508-3:~~1998~~ 2010, 7.2, Tables A.1, B.7 IEC 61508-3:~~1998~~ 2010, 7.4.2 to 7.4.4, Tables A.3, B.1 IEC 61508-7:~~2000~~ 2010, Table C.1 IEC 61508-6:2010, Annex A Examples in IEC 61508-5:2010, ~~Examples in IEC 61508-6:2000, Annex A~~
4	**Verification of *PDS(SR)* safety requirements specification**	
	a) Reviews of the *safety requirements specification* b) Check by an independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:~~2000~~ 2010 and IEC 61508-3:~~1998~~ 2010, 7.9
5	**~~Concept~~ Safety system architecture specification for a *PDS(SR)***	Phase 3 of *PDS(SR)* safety lifecycle (see 5.3 and 5.6 of this standard)
	a) ~~Hardware design on an architectural level, including~~ Details of hardware and software necessary to implement *safety sub-functions* specified by the *SRS*. For each *safety sub-function*, the architecture should also include: • ~~Block diagrams of safety related hardware~~ • ~~User and process interfaces~~ • ~~Safety relevant signal paths~~ • ~~Power supply~~ • ~~Separation of independent channels to achieve fault tolerance~~ • ~~Communication links between independent channels to achieve *diagnostic coverage*~~ • requirements for *subsystems* and parts of *subsystems* as appropriate; • requirements for the integration of the *subsystems* and parts to satisfy the *SRS;* • throughput performance that enables response time requirements to be met; • accuracy and stability requirements for measurements and controls; • safety-related operator interfaces; • other items specified in 5.6.2.2.	a) See 5.6 of this standard IEC 61508-2:~~2000~~ 2010, 7.4, Annex A~~, Tables B.2, B.6~~ IEC 61508-3:2010, 7.4.2, 7.4.3 Examples in IEC 61508-6:~~2000~~ 2010, Annexes A and D

	Tasks	References
	b) **~~Software design on an architectural level, including~~** **Details of how the design will achieve the *safety integrity level* and required target failure measure for the *safety sub-function* including:** - ~~description of the functions provided by the safety related software~~ - ~~interaction with hardware~~ - ~~state machine diagrams of the intended behaviour of the software~~ - ~~user and process interfaces~~ - ~~fault detection possibilities and fault reactions~~ - ~~overview of software structure, for example with block diagram~~ - ~~control and storage of safety related data~~ - ~~version procedures~~ - ~~used tools, for example compiler, code checker, etc.~~ - architecture of each *subsystem* required to meet architectural constraints on hardware *safety integrity;* - relevant reliability modelling parameters such as required *diagnostic test* interval of all hardware components necessary to achieve the target failure measure; - actions taken in the event of a detected *dangerous failure;* - how the safety-related hardware will achieve immunity to all required environmental conditions, including EM, over the entire safety lifecycle; - QA/QC measures necessary for safety management.	b) IEC 61508-2:~~2000~~ 2010, 7.4, Tables 2, 3, Annexes A, C IEC 61508-3:~~1998~~ 2010, 7.2.2.8, 7.2.2.10, 7.4.2,7.4.3 Tables A.2, B.1, B.7, B.9 IEC 61508-6:2010, Clause A.2 IEC 61508-7:~~2000~~ 2010, Table C.1
	c) **Recommendation** Pre-estimation of the probability of failure of *safety sub-functions* due to random hardware failures on a level of functional block diagrams	c) IEC 61508-1:~~1998~~ 2010, Table 2 IEC 61508-2:~~2000~~ 2010, 7.4.4, Tables 3, A.1, Annex C IEC 61508-3:~~1998~~ 2010, Clause 8, Table A.10, B.4 (FMEA) Examples in IEC 61508-6:~~2000~~ 2010, Annexes C and D
6	**Verification of ~~concept~~ safety system architecture specification**	
	a) Reviews of system ~~design~~ architecture b) Check by independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:~~2000~~ 2010 and IEC 61508-3:~~1998~~ 2010, 7.9
7	**Validation planning**	Phase 4 of *PDS(SR)* safety lifecycle (see 5.4 d of this standard)
	a) Detailed planning of the validation of safety related *PDS(SR)*. b) The validation plan should be generated in parallel to Phase 9.3 Design and Development.	a) See 8.3 of this standard b) IEC 61508-2:~~2000~~ 2010, 7.3, Table B.5 IEC 61508-3:~~1998~~ 2010, 7.3, Tables A.7, B.3, B.5
8	**Verification of validation plan**	
	a) Reviews of the *validation* plan b) Check by independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:~~2000~~ 2010 and IEC 61508-3:~~1998~~ 2010, 7.9

	Tasks	References
9	**Design and development**	Phase 5 of PDS(SR) safety lifecycle (see 5.3 of this standard)
	a) Hardware design b) Software design c) Reliability Prediction (calculation of the probability of failure of *safety sub-functions* due to random hardware failures) including: • type of *PDS(SR)* • SFF • functional block diagram • reliability model • data basis of the model (device lists) • *PFH~~ calculation~~ estimation* • *mission time* • repair interval~~, proof test interval (if relevant)~~	See Clause 6 of this standard a) IEC 61508-2:~~2000~~ 2010, 7.4, Annex A, Table B.2, B.3, B.6 b) IEC 61508-3:~~1998~~ 2010, 7.4.5, 7.4.6, Table A.4 c) IEC 61508-1:~~1998~~ 2010, Table 2 IEC 61508-2:~~2000~~ 2010, 7.4.3, 7.4.9, Table 3, A.1, Annex C IEC 61508-3:~~1998~~ 2010, Table B.4 (FMEA) Examples in IEC 61508-6:~~2000~~ 2010, Annexes C and D
10	**Verification of the design**	
	a) Reviews of the system design b) Functional tests on module level c) Check by an independent person or department where required	a) See 8.2 of this standard c) IEC 61508-2:~~2000~~ 2010, 7.9 IEC 61508-3:~~1998~~ 2010, 7.4.7, 7.4.8, 7.5, 7.9, Tables A.5, A.9
11	***PDS(SR)* integration**	Phase 6 of *PDS(SR)* safety lifecycle (see 5.3 of this standard)
	Integration and test of the safety related *PDS(SR)*.	See 6.5 of this standard IEC 61508-2:2010, 7.5 IEC 61508-3:2010, 7.4.8, 7.5
12	**Verification of integration**	
	Review of HW/SW integration test results and documentation	See 8.2 of this standard IEC 61508-2:~~2000~~ 2010, 7.5, 7.9, Tables B.3, B.6 IEC 61508-3:~~1998~~ 2010, 7.4.3.2(f), 7.4.5.5, 7.4.6.1, 7.4.7, 7.4.8, 7.5, 7.9, Tables A.5, A.6, A.9
13	**~~Installation~~ Act of installing, commissioning and operation (user documentation)**	Phase 7 of *PDS(SR)* safety lifecycle (see 5.3 of this standard)
	Develop user documentation describing the *PDS(SR)* ~~installation~~ act of installing, commissioning, operation and maintenance.	See Clause 7 of this standard IEC 61508-2:~~2000~~ 2010, 7.6, Table B.4
14	**Verification of user documentation**	
	a) Reviews of user documentation describing the *PDS(SR)*~~ installation~~ act of installing, commissioning, operation and maintenance. b) Check by an independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:~~2000~~ 2010,7.9~~ and IEC 61508-3:1998~~

	Tasks	References
15	**Validation of *PDS(SR)***	Phase 8 of PDS(SR) safety lifecycle (see 5.3 of this standard)
	a) Provide all necessary information needed for *PDS(SR)* validation b) Complete software and appropriate documentation c) *Validation* tests and procedures according to the *validation* plan d) Documentation of the results of the *validation* tests e) Prepare appropriate documentation for third party *validation* where necessary	a) See 8.3 of this standard c) IEC 61508-2:~~2000~~ 2010, 7.3, 7.7, Tables B.5, B.6 IEC 61508-3:~~1998~~ 2010, 7.7, 7.9, Table A.7
16	***PDS(SR)* modification procedure**	
	a) Modification request and analysis b) Appropriate documentation of all modified parts of the *PDS(SR)* c) Re-*verification* of modified parts d) Update of reliability prediction if modification has impact on fault tolerance, probability of dangerous faults, *diagnostic coverage* or *common cause failure* e) Re-validation of at least modified parts of the *PDS(SR)* f) Software modification	a) See Clause 10 of this standard b) IEC 61508-1:~~1998~~ 2010, 7.16 IEC 61508-2:~~2000~~ 2010, 7.5.2.5, 7.8 Example in IEC 61508-1:~~1998~~ 2010, Figure 9 f) IEC 61508-3:~~1998~~ 2010, 7.1.2.9, 7.5.2.6, 7.6.2, 7.8.2, Table A.8

Annex B
(informative)

Example for ~~determination~~ estimation of *PFH*

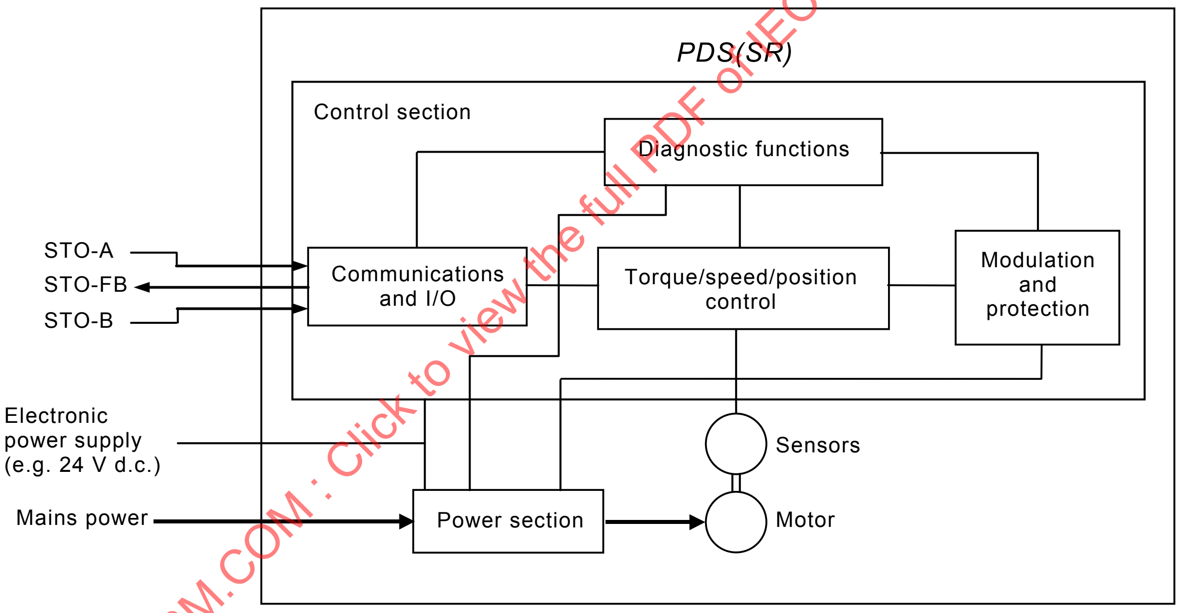
B.1 General

This clause describes the ~~determination~~ estimation of the *PFH* of an example *PDS(SR)* with the *safety sub-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 sub-function* STO, which is triggered by two redundant digital inputs ~~interfaces~~ and gives a single feedback signal through a digital output ~~interface~~ (see Figure B.1).



~~NOTE~~ **Key**

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*.

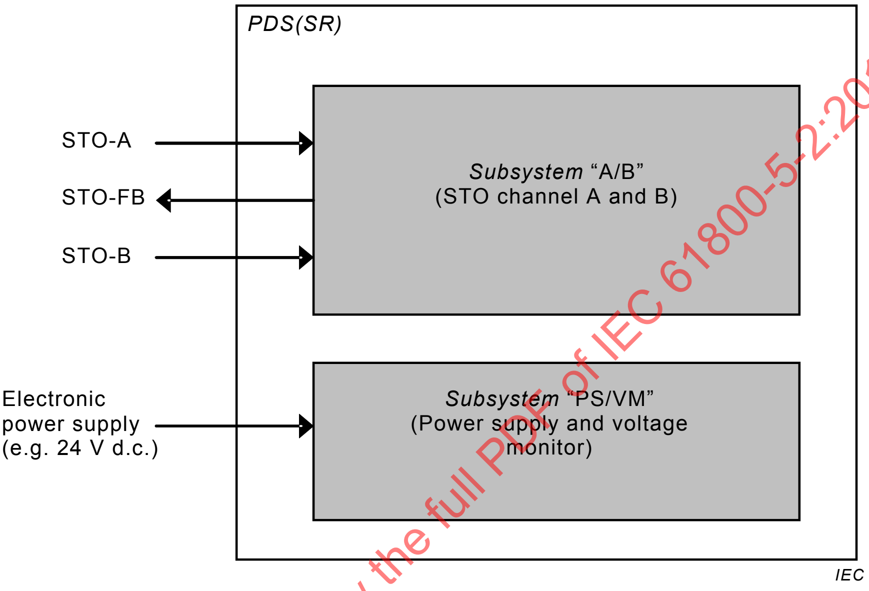
Within the *PDS(SR)*, the *safety sub-function* STO is implemented together with the ~~standard~~ non-safety-related functionality of the *PDS(SR)* using only a few *safety sub-function* exclusive components.

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 sub-function* STO of this example *PDS(SR)* is calculated as follows:

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

where $PFH_{\mathrm{A/B}}$ and $PFH_{\mathrm{PS/VM}}$ are the *PFH* values of *subsystem* A/B and *subsystem* PS/VM respectively.



Key

STO-A	STO trigger input channel A
STO-B	STO trigger input channel B
STO-FB	STO feedback output

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

B.2.2 *Subsystem* A/B

The *safety sub-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 sub-function*:

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

The architectural constraints of a type B *subsystem* (see 6.2.3.3) show that, for *SIL* 2 and hardware fault tolerance 1, the *safe failure fraction (SFF)* ~~must~~ shall 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 sub-function*:

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

The architectural constraints of a type B *subsystem* (see 6.2.3.3) 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

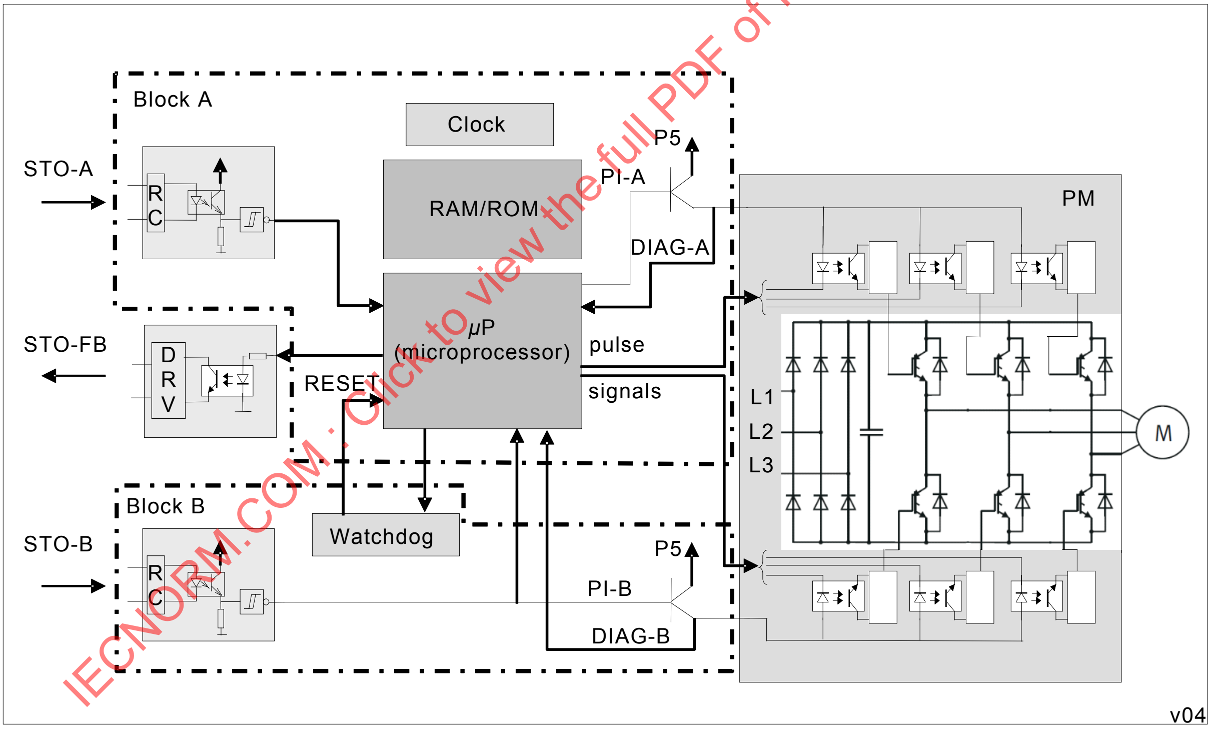
B.3.1 *Subsystem* "A/B" (main *subsystem*)

B.3.1.1 Function block division

Within the *PDS(SR)*, the *subsystem* A/B is part of the implementation of the *safety sub-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 sub-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~~ each channel is merged in one function block (Block A and B).

Component failures within the power module itself do not cause a loss of the *safety sub-function*. Therefore, the power module is not to be included in any subsystem contributing to the *PFH* value.



~~NOTE 1~~ **Key**

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

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

~~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~~ can 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 sub-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, IEC 61508-6:~~2000~~ 2010, Annex C, 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 failures* ~~has to~~ can be defined using the tables in IEC 61508-2:2010. This proportioning defines the failure rates λ_{DD} (dangerous ~~detectable~~ detected) and λ_{DU} (dangerous ~~undetectable~~ undetected) of the component.

The total failure rates of the function block (λ_S, λ_{DD}, λ_{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 IEC 61508-6:~~2000~~ 2010, Annex C, 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 failure*s and a 50 % portion of *dangerous failure*s. The portion of detected failures is determined by using the tables of IEC 61508-2.

NOTE Use of this simplified method is more efficient than a detailed analysis but can result in failure rates λ_S, λ_{DD} and λ_{DU} less favorable (i.e. more conservative) than if a detailed analysis is conducted

This method will also lead to the failure rates λ_S, λ_{DD} and λ_{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 61508-2:2010.

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

Method (IEC 61508-2:2010)	**DC level claim**	***Diagnostic test* implementation**
Table A.3 Failure detection by on-line 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:	λ_A	(total failure rate)		450 FIT
	λ_{AS}	(proportion of *safe failures*)	0,5*450 FIT	225 FIT
	λ_{AD}	(proportion of *dangerous failures*)	0,5*450 FIT	225 FIT
	λ_{ADD}	$DC_A*\lambda_{AD}$	0,9*225 FIT	202,5 FIT
	λ_{ADU}	$(1-DC_A)*\lambda_{AD}$	(1-0,9)*225 FIT	22,5 FIT
Block B:	λ_B	(total failure rate)		70 FIT
	λ_{BS}	(proportion of *safe failures*)	0,5*70 FIT	35 FIT
	λ_{BD}	(proportion of *dangerous failures*)	0,5*70 FIT	35 FIT
	λ_{BDD}	$DC_B*\lambda_{BD}$	0,9*35 FIT	31,5 FIT
	λ_{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 IEC 61508-2:~~2000~~ 2010, Clause C.1, item h, is:

$$\begin{aligned} SFF_{A/B} &= [(\lambda_{AS}+\lambda_{BS}) + (DC_A * \lambda_{AD}) + (DC_B * \lambda_{BD})] / [(\lambda_{AS}+\lambda_{BS}) + (\lambda_{AD}+\lambda_{BD})] \\ &= [(225 + 35) + (0,9 * 225) + (0,9 * 35)]\ \text{FIT} / [(225 + 35) + (225 + 35)T]\ \text{FIT} \\ &= 494\ \text{FIT} / 520\ \text{FIT}; \end{aligned}$$

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

NOTE The calculation of $SFF_{A/B}$ is shown to demonstrate the principal. Due to the determined test intervals in Table B.1, $SFF_{A/Bresulting}$ can be applied (see Clause B.4).

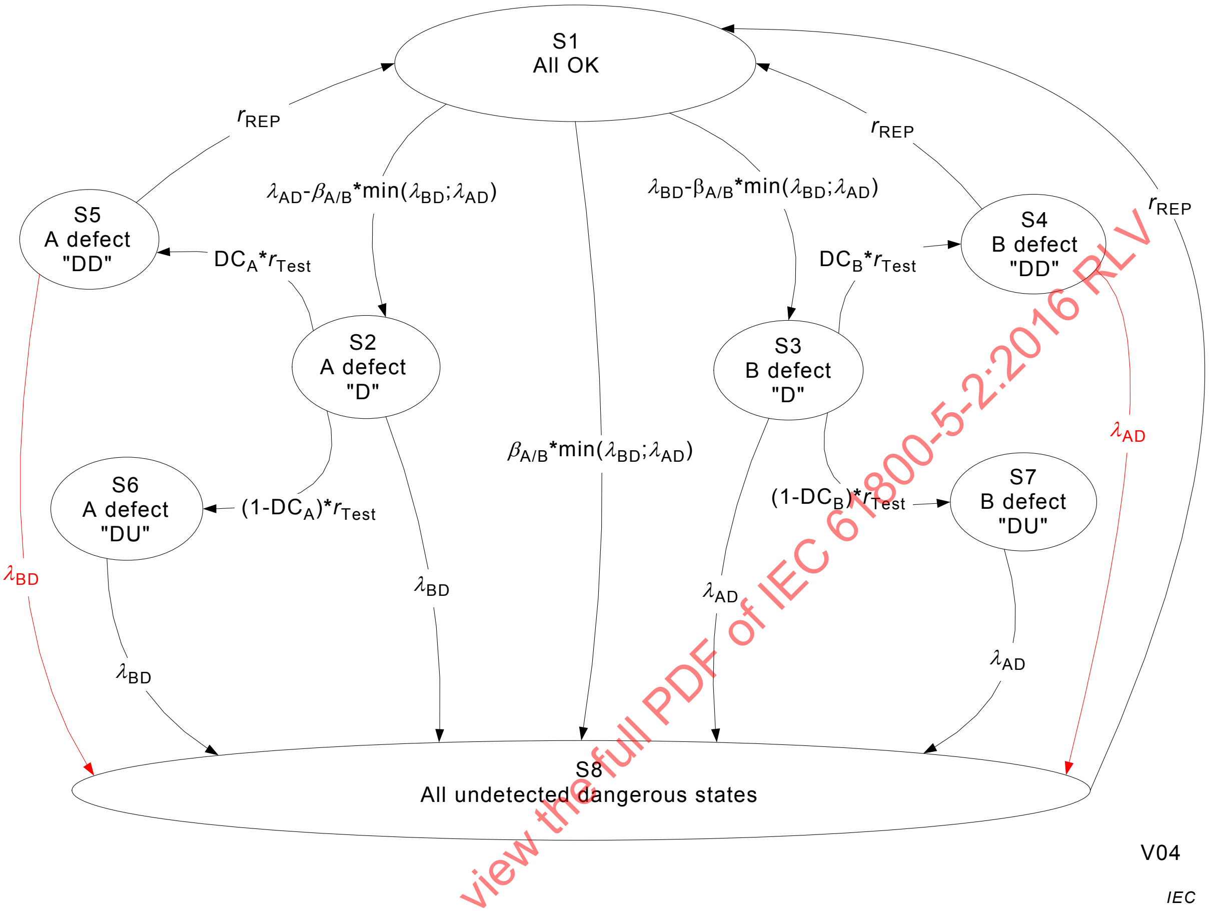
B.3.1.4 *Common cause failure* factor $\beta_{A/B}$

The *common cause failure* factor $\beta_{A/B}$ is estimated by using IEC 61508-6:~~2000~~ 2010, Table D.4.

$\beta_{A/B}$ = 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.



Key:

S1, S2, S3, S4, S5, S6, S8: states of the Markov model

"D": defect

"DD": defect detected

"DU" defect undetected

other terms are explained in the clause above

NOTE 1 The above Markov model Figure B.4 ~~should~~ can 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(λ_{BD};λ_{AD}) means λ_{BD} or λ_{AD}, whichever is smaller. Due to the fact that the common cause failure rate, while increasing the beta factor, can reach only the λ value of the channel with the smaller value the minimum function for calculating the common cause failure rate is justified.

NOTE 4 The Model assumes continuous mode of operation, i.e. permanent presence of the demand to perform the *safety sub-function*. Therefore, any entering to state S8 causes a contribution to *PFH* and no additional transitions are needed to represent the occurrence of a demand. Thus the model covers the entire range of possible demand rates. On the other hand, in the present case of a redundant architecture the assumption of continuous demand does not lead to a significant increase of PFH as compared to high demand.

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

The model does not take into 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 The rate of simultaneous failure of both blocks can never be greater than the lower of 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 sub-function* is no ~~more~~ longer available and ~~no~~ the test is not 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 sub-function*.

B.3.1.6 *PFH* value calculation

λ values, DC and β 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 [$p_{\text{i}}(t)$] of each state [S*i*] of the Markov model ~~has to~~ can 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~~ can be done up to the *mission time* T_{M}.

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

$$PFH_{A/B} = \frac{1}{T_M} \int_0^{T_M} \{\beta_{A/B} \cdot \min(\lambda_{AD}, \lambda_{BD}) \cdot p_1(t) + \lambda_{AD}\,[p_3(t) + p_4(t) + p_7(t)] + \lambda_{BD}\,[p_2(t) + p_5(t) + p_6(t)]\} dt$$

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

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

$\beta_{\mathrm{A/B}}$	r_{Rep}	r_{Test}	T_{M} years	$PFH_{\mathrm{A/B}}$
2 %	1/8 h	1/8 h	10	~~$6.84 \ 10^{-10}$ /h~~ $7{,}67 \times 10^{-10}$ /h
2 %	1/8 h	**1/24 h**	10	~~6.84×10^{-10} /h~~ $7{,}68 \times 10^{-10}$ /h
2 %	1/8 h	**1/168 h**	10	~~6.86×10^{-10} /h~~ $7{,}70 \times 10^{-10}$ /h
2 %	1/8 h	**1/672 h**	10	~~6.91×10^{-10} /h~~ $7{,}76 \times 10^{-10}$ /h
2 %	1/8 h	**1/8760 h**	10	~~7.72×10^{-10} /h~~ $8{,}76 \times 10^{-10}$ /h
2 %	**1/8760 h**	1/8 h	10	~~6.83×10^{-10} /h~~ $8{,}76 \times 10^{-10}$ /h
2 %	1/8 h	1/8 h	**20**	~~7.38×10^{-10} /h~~ $8{,}34 \times 10^{-10}$ /h
2 %	1/8 h	**1/672 h**	20	~~7.46×10^{-10} /h~~ $8{,}43 \times 10^{-10}$ /h
3 %	1/8 h	1/8 h	20	~~1.05×10^{-9} /h~~ $1{,}18 \times 10^{-9}$ /h
5 %	1/8 h	1/8 h	20	~~1.68×10^{-9} /h~~ $1{,}88 \times 10^{-9}$ /h

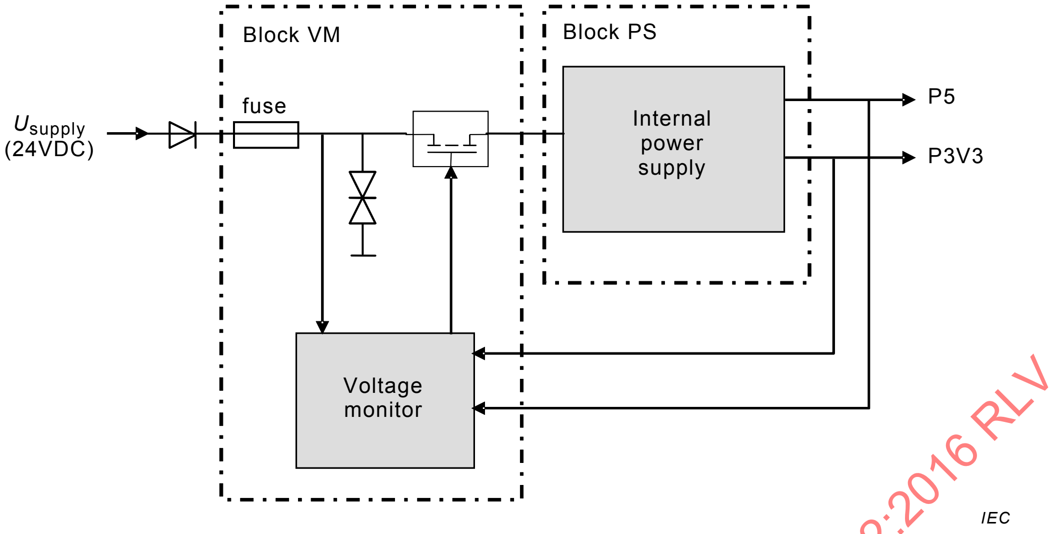
~~NOTE~~ Values in bold characters give the modified value regarding the previous line.

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. Nevertheless, not all of the parameter values may be realistic. Regarding the achievable overall accuracy of a PFH calculation, the PFH value of a complete safety device should be specified using a mantissa with one decimal place only. Table B.2 provides two decimal places only in order to demonstrate even low effects of particular parameter variations.

B.3.2 *Subsystem* "PS/VM"

B.3.2.1 Function block division

For the *safety sub-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~~ **Key**

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 failures* of printed board circuits is then also 50 %.

The *diagnostic coverage* (DC) can be estimated by using the tables of IEC 61508-2:~~2000~~ 2010, Annex A.

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

The *safe failure* fraction of *subsystem* PS/VM is calculated according to IEC 61508-2:~~2000~~ 2010, Clause C.1, item g (see Note):

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

$$= [125 + (125 * 0{,}99)] \text{ FIT} / 250 \text{ FIT}$$

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

NOTE The monitor block does not contribute to the *SFF* but only to the *PFH*.

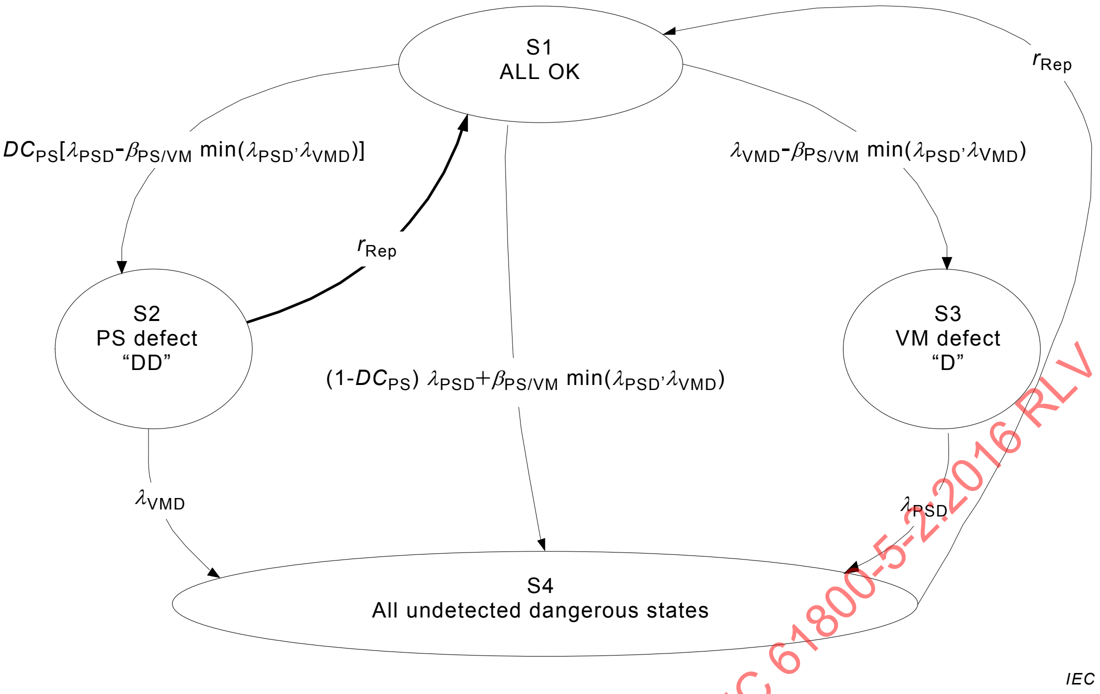
B.3.2.4 *Common cause failure* factor $\beta_{\mathbf{PS/VM}}$

The *common cause failure* factor $\beta_{\mathrm{PS/VM}}$ is estimated by using of IEC 61508-6:~~2000~~ 2010, Table D.4.

$\beta_{\mathrm{PS/VM}}$ = 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.


S1
ALL OK
r_{Rep}
$DC_{PS}[\lambda_{PSD}-\beta_{PS/VM}\ \min(\lambda_{PSD},\lambda_{VMD})]$
$\lambda_{VMD}-\beta_{PS/VM}\ \min(\lambda_{PSD},\lambda_{VMD})$
r_{Rep}
S2
PS defect
“DD”
S3
VM defect
“D”
$(1-DC_{PS})\ \lambda_{PSD}+\beta_{PS/VM}\ \min(\lambda_{PSD},\lambda_{VMD})$
λ_{VMD}
λ_{PSD}
S4
All undetected dangerous states
IEC

Key:

S1, S2, S3, S4: states of the Markov model

"D":	defect
"DD":	defect detected
"DU"	defect undetected

Other terms are explained in Subclause B.3.2

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.

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

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 3).

NOTE 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 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 sub-function* is no more available

State S4 represents the dangerous situation where the *safety sub-function* is no ~~more~~ longer available and ~~no~~ the test is not effective any longer. Since continuous *mode of operation* is assumed for the *PDS(SR)*, state S4` represents the "*hazard*ous event" resulting from a dangerously failed *PDS(SR)* confronted with demand of the *safety sub-function*.

B.3.2.6 *PFH* value calculation

λ values, DC and β 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~~ can 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~~ can be done up to the *mission time* T_{M}.

$$\text{PFH}_{\text{PS/VM}} = \frac{1}{T_{\text{M}}}\int_{0}^{T_{\text{M}}}\left[\left((1-\text{DC}_{\text{PS}})\cdot\lambda_{\text{PSD}} + \beta_{\text{PS/VM}}\cdot\min(\lambda_{\text{PSD}},\lambda_{\text{VMD}})\right)\cdot p_1(t) + \lambda_{\text{VMD}}\cdot p_2(t) + \lambda_{\text{PSD}}\cdot p_3(t)\right]dt$$

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

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

$\beta_{\text{PS/VM}}$	r_{Rep}	T_{M} years	$PFH_{\text{PS/VM}}$
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 sub-function* STO of *PDS(SR)*

Example *PFH* values with r_{Rep} = 1/8 h, r_{Test} = 1/8 h and varied parameter T_{M}:

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

$PFH_{\text{STO/}PDS(SR)}$ (T_{M} = 10 years) = (~~6,84~~ 7,67 × 10^{-10}/h + 4,39 × 10^{-9}/h) = ~~5,074~~ 5,16 × 10^{-9}/h;

$PFH_{\text{STO/}PDS(SR)}$ (T_{M} = 20 years) = (~~7,38~~ 8,34 × 10^{-10}/h + 5,03 × 10^{-9}/h) = ~~5,768~~ 5,86 × 10^{-9}/h.

B.4 Reduction of DC and SFF depending on test interval

Increasing the test interval will lead to a lower resulting *diagnostic coverage* ($\text{DC}_{\text{resulting}}$) and lower resulting *safe failure fraction*.

In the following the deduction of DC and SFF including the dependence on the diagnostic test interval is given:

Refer to IEC 61508-6: 2010, B.3.3.2.1, Formula for t(CE)

t(CE) = (1-DC)(T1/2 + MRT) + DC * MTTR; (1)

with T1 = TM;

MRT = 0; and (no repair during operation time of PDS)

MTTR = DI/2; (average time until fault detection, no repair time)

follows:

t(CE) = (1-DC)TM/2 + DC*DI/2; (2)

For reference to normative requirements a ‘resulting DC‘ will be calculated which depends on the diagnostic interval DI

Assuming:

t(CE) = (1-DC‘)TM/2;

then:

(1-DC’)TM/2 = (1-DC)TM/2 + DC*DI/2;

resolving for DC’ leads to

DC‘ (= $\text{DC}_{\text{resulting}}$) depending on DC and DI

DC’ = $\mathbf{DC}_{\text{resulting}}$ = DC(1-DI/TM);

SFF‘ (= $\text{SFF}_{\text{resulting}}$) according IEC 61508:

$\text{SFF}_{\text{resulting}} = \boldsymbol{SFF'} = \frac{\lambda s}{\lambda} + \left(1 - \frac{\lambda s}{\lambda}\right) DC';$

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 62380:2004, 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 16); can be obtained from: Siemens AG, CT*~~*SR*~~ *TIM IR SI,*~~*Otto-Hahn-Ring 6, D-81739*~~ *D-80200 Munich*.
- Reliability Prediction of Electronic Equipment, MIL-HDBK-217~~E~~F, *Notice 2:1995, Department of Defense, Washington DC,*~~*1982*~~ *20301.*
- Reliability Prediction Procedure for Electronic Equipment, Telcordia SR-332, *Issue*~~*01*~~ *03,* ~~*May 2001*~~ *Jan 2011 (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~~ China 299B Electronic Reliability Prediction
- AT&T reliability manual – *Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors,l, 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.*~~ *is the new Reliability Analysis Center (RAC) software tool that ties together several tools into a comprehensive system reliability prediction methodology. The PRISM concept accounts for the myriad of factors that can influence system reliability, combining all those factors into an integrated system reliability assessment resource. PRISM was developed to overcome inherent limitations in MIL-HDBK-217 that is no longer being actively maintained*

or updated by the Department of Defense (DoD) The PRISM software is available from the address below, RELIASS; Cams Hall, Cams Hill; FAREHAM; Hampshire, PO16 8AB;United Kingdom

- Analog Devices Component MTTF data – *www.analog.com under "about ADI"*
- FIDES – *Reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA, new version from 2009 (http://fides-reliability.org)*.

C.2 Helpful standards concerning component failure

IEC 60300-3-2:2004, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-5:2001, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60319:1999, *Presentation and specification of reliability data for electronic components*

IEC 60706-3:2006, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60721-1:2002, *Classification of environmental conditions – Part 1: Environmental parameters and their severities*

IEC 61709:2011, *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 D.3.1 up to D.3.16 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~~ can 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~~ can be helpful for evaluation:

Test Method for Measuring Whisker Growth on Tin and Tin Alloy Surface Finishes, JESD22A121~~-01~~A, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834,http://www.jedec.org/standards-documents/results/JESD22A121

Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes, JESD201A, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, http://www.jedec.org/standards-documents/results/JESD201

Tin whiskers on printed circuit boards – Consequences for safety components in machine construction, IFA Institut für Arbeitsschutz, Alte Heerstrasse 111, 53757 Sankt Augustin, http://www.dguv.de/ifa/Praxishilfen/Zinnwhisker-auf-Leiterplatten/index-2.jsp

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~~ can be regarded.

NOTE 4 Whiskers on tracks of printed circuit boards have not been reported yet. Tracks usually consist of copper without tin coating. Pads ~~may~~ can 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.1 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:~~ ~~– permanently connected (fixed) and protected against external damage, for example by cable ducting, armouring; or~~ ~~– separate multicore cables, or~~ ~~– within an electrical enclosure (see remark 1)), or~~ ~~– 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)).~~	

D.3.1 Conductors/cables

The requirements of ISO 13849-2: 2012,Table D.4, apply.

D.3.2 Printed wiring boards/assemblies

The requirements of Table D.1 apply.

Table D.1 – 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. 2) The creepage distances and clearances are dimensioned to at least IEC~~ 60664-1~~ 61800-5-1 with pollution degree 2/~~ installation category~~ OVC III; if both tracks are PELV/SELV – powered~~ by a SELV/PELV supply~~, pollution degree 2/~~ installation category~~ OVC II apply with a minimum clearance of 0,1 mm. 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. NOTE 1 Alternative methods to ensure protection against conductive contamination are: • enclosure of safety relevant circuitry of at least IP54 according to IEC 60529, • cabinet for safety relevant *BDM/CDM* of at least IP54 according to IEC 60529, • environmentally controlled location for the *BDM/CDM* which does not contain conductive contamination. NOTE 2 Experience has shown that a solder mask is satisfactory as a protective layer. NOTE 3 A~~ further~~ protective layer covering according to IEC 60664-3 can reduce the creepage distances and clearances dimensions. Compliance with NEMA 250, Type 12 enclosure requirements is considered to be sufficient to demonstrate compliance with IP54 requirements.
Open-circuit of any track	None	–
NOTE 1 Printed wiring board (PWB) is another term for printed circuit board (PCB). NOTE 2 Over voltage category (OVC) is defined in IEC 61800-5-1.		

D.3.3 Terminal block

The requirements of Table D.2 apply.

Table D.2 – 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. 2) Guaranteed by design, for example shaping shrink down plastic tubing over connection point.
Open-circuit of individual terminals	None	–

D.3.4 Multi-pin connector

The requirements of Table D.3 apply.

Table D.3 – 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). Remark 2) also applies if the connector is mounted on a PWB.	1) By using ferrules or other suitable means for multi-stranded wires, regarding Creepage distances and clearances and all gaps ~~should be dimensioned to at least IEC 60664-1 -1:1992 with nstallation category III~~ refer to IEC 61800-5-1:2007, 4.3.6. 2) The assembled board ~~should be~~ is mounted in an enclosure ~~of at least IP 54 (see EN 60529)~~ giving protection against conductive contamination and the printed side(s) ~~of the assembled board is covered~~ are coated with an ageing-resistant varnish or protective layer covering all conductor paths ~~in accordance with IEC 60664-3.~~ NOTE 1 Alternative methods to ensure protection against conductive contamination are: • Enclosure of safety relevant circuitry of at least IP54 according to IEC 60529 • Cabinet for safety relevant *BDM/CDM* of at least IP54 according to IEC 60529 • Environmentally controlled location for the *BDM/CDM* which does not contain conductive contamination NOTE 2 Experience has shown that a solder mask is satisfactory as a protective layer. NOTE 3 A protective layer covering according to IEC 60664-3 can reduce the creepage distances and clearances dimensions. Compliance with NEMA 250, Type 12 enclosure requirements is considered to be sufficient to demonstrate compliance with IP54 requirements.
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	–

D.3.5 Electromechanical devices

The requirements of Table D.4 apply.

Table D.4 – 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~~ IEC 61800-5-1:2007, 4.3.6. 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.~~ ~~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.~~ ~~Short-circuits in coils and windings need to be avoided by taking appropriate steps, for example:~~ ~~▪ impregnating the coils so as to fill all the cavities between individual coils and the body of the coil and the core; and~~ ~~▪ using winding conductors well within their insulation and high temperature ratings.~~ ~~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~~ ~~$0,5L_N < L < L_N$ + tolerance~~ ~~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.~~ ~~2) Resistors in surface-mount technology must be a thin film metal type in package types MELF, miniMELF or µMELF.~~
~~Random change of value~~ ~~$0,5R_N < R < 2R_N$~~ ~~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~~ ~~$0,5R_N < R < 2R_N$~~ ~~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~~ ~~0,5 R_p < R < 2 R_p~~ ~~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~~ ~~0,5 C_N < C < C_N + tolerance~~ ~~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 δ~~	~~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.~~ ~~2) Measures are taken to ensure that an internal failure of the optocoupler cannot result in excessive temperature of its insulating material.~~

D.3.6 Transformers

The requirements of ISO 13849-2:2012, Table D.12 apply.

D.3.7 Inductances

The requirements of ISO 13849-2:2012, Table D.13 apply.

D.3.8 Resistors

The requirements of ISO 13849-2:2012, Table D.14 apply.

D.3.9 Resistor Networks

The requirements of ISO 13849-2:2012, Table D.15 apply .

D.3.10 Potentiometers

The requirements of ISO 13849-2:2012, Table D.16 apply.

D.3.11 Capacitors

The requirements of ISO 13849-2:2012, Table D.17 apply.

D.3.12 Discrete semiconductors

(For example diodes, Zener diodes, transistors, triacs, GTO thyristors, IGBTs, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs]) .

The requirements of ISO 13849-2:2012, Table D.18 apply.

D.3.13 Signal Isolation components

The requirements of Table D.5 apply.

Table D.5 – Signal Isolation components

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 across the isolation barrier	Short-circuit across the isolation barrier can be excluded if remarks 1) and 2) are fulfilled.	1) The Signal Isolation component is built in accordance with OVC III according to IEC 61800-5-1. If a SELV/PELV power supply is used, pollution degree 2/ OVC II applies. NOTE All requirements of IEC 61800-5-1:2007, 4.3.6 apply. 2) Measures are taken to ensure that an internal failure of the Signal Isolation component cannot result in excessive temperature of its insulating material.

D.3.14 Non-programmable integrated circuits

The requirements of Table D.6 apply.

Table D.6 – Non-programmable integrated circuits

Fault considered	Fault exclusions	Remarks
Open-circuit of each individual connection	None	Refer to IEC 61508-2:2010, Annex E
Short-circuit between any two connections	Possible exclusion – see remark.	
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.		

D.3.15 Programmable and/or complex integrated circuits

The requirements of Table D.7 apply.

Table D.7 – Programmable and/or complex integrated circuits

Fault considered	Fault exclusions	Remarks
Faults in all or part of the function	None	Refer to IEC 61508-2:2010, Annex E
Open-circuit of each individual connection	None	
Short-circuit between any two connections	~~None~~ Possible exclusion – see remark.	
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 sub-function*.		

D.3.16 Motion and position feedback sensors

The requirements of Table D.8 apply.

Table D.8 – Motion and position feedback sensors

Fault considered	Fault exclusion	Remarks
General		
Short-circuit between any two conductors of the connecting cable	The requirements of ~~Table D.1~~ D.3.1 applies	
Open-circuit of any conductor of the connecting cable	None	
~~Input or output stuck at 0 or 1,~~ Stuck-at Ground, $U_B/2$, U_B on single or on several inputs/outputs at the same time	None	U_B is the power supply of the sensor. Sensor inputs are applied e. g. for parameter settings. The behavior of the individual sensor in case of a fault has to be considered.
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:~~ ~~– sensor housing from motor chassis~~ ~~– sensor shaft from motor shaft~~	~~Preparing FMEA and prove long-term integrity of mechanical fixings~~	~~Output signal equals standstill~~ ~~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.~~

Fault considered	Fault exclusion	Remarks
Loss or loosening of attachment during standstill or during motion: - sensor housing from motor chassis - sensor shaft from motor shaft - mounting of the read head	Preparing FMEA and prove ~~long-term integrity of mechanical fixings~~ – permanent fastness for form-locked connections – fastness for force-locked connections	~~Possible effects:~~ ~~- static offset of sensor shaft~~ ~~- dynamic slip of sensor shaft~~ ~~- wrong output signal/zero speed signal~~ ~~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.~~ The maximum permissible loading of the sensor is known or limited on the sensor's data sheet. a) For form-locked connections: 1) Design for permanent fastness in accordance with generally acknowledged technical experience with a high safety factor – Verification is performed by calculation and with a suitable test. – Example for steel components: Overdimensioning with a safety factor $S \geq 2$ against fatigue fracture. or 2) Overdimensioning with a safety factor $S \geq 5$ against fatigue fracture – Verification is performed by calculation. b) For force-locked connections: 1) Overdimensioning with a safety factor $S \geq 4$ against slipping – Detailed measures for application and maintaining the preloading force are to be defined in the user documentation (e.g. defined pairs of materials, surfaces and torque-controlled tightening methods). – Verification is performed by calculation and with a suitable test. or 2) Overdimensioning with a safety factor $S \geq 10$ against slipping – Measures for application and maintaining the preloading force are to be defined in the user documentation – Verification is performed by calculation.
Loosening of solid measure [a] (e.g. optical encoder disc)	None	Output indicates wrong position
No light from diode	None	Not applicable on encoders not using any light emitting diodes, e.g. resolvers

Fault considered	Fault exclusion	Remarks
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~~ sine-/cosine output signal(s) into square wave: each half period sine wave replaced by square wave with same amplitude.	None	For example, no Sin/Cos – type signal, signal offset It is impossible to consider all possible signal shapes caused by component faults. Instead, square wave is assumed representative.
Exchange of Sin and Cos output signal	Fault exclusion ~~allowed~~ is permitted if there are no electronic components applied to select an output signal from several sources	
Change of DC part of sine-/cosine output signal(s) within power supply voltage.	None	
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
Additionally for encoder with incremental and absolute signals		
~~Concurrently~~ Simultaneous wrong position signal change from both 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: - repeating - loss - insertion - wrong order - wrong data - delay - masquerade	None	Equals fault model for communication busses which are addressed by the IEC 61784 series.
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 - No conversion start for A/D converter - Wrong timing of Sample & Hold	None	
A/D converter generates wrong values	None	For example due to over modulation caused by too high reference voltage or electromagnetic influence

Fault considered	Fault exclusion	Remarks
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 and resolvers. If other sensors (for example inductive sensors) are used, corresponding faults apply.		

Annex E
(normative)

Electromagnetic (EM) immunity requirement for *PDS(SR)*

E.1 General

To show compliance with the design requirements for a *PDS(SR)* regarding electromagnetic (EM) immunity described in 6.2.6, the immunity requirements provided in the following tables E.1, E.2 and E.3 shall apply with performance criteria of 9.3.3.

According to IEC Guide 107 the requirements of this Annex E are based on IEC 61000-6-7:2014.

Due to the differences of port/interface definitions between IEC 61000-6-7 and IEC 61800-3, the EM immunity requirements for *PDS(SR)* are given in Tables E.1, E.2 and E.3.

It is permitted to verify immunity of safety sub-functions for all phenomena in Tables E.1 and E.2 using calculation or simulation, as well as by testing.

E.2 Immunity requirements – low frequency disturbances

These requirements apply to the following power ports:

- all power ports which provide power for *safety sub-function*s in low voltage *PDS(SR)*, and
- all auxiliary low voltage power ports which provide power for *safety sub-function*s in *PDS(SR)* of rated voltage above 1 000 V (only second environment).

Table E.1 – Minimum immunity requirements for voltage deviations, dips and short interruptions

Phenomenon		First environment		Second environment	
	Reference document	Level		Level	
Voltage deviations (> 60 s)	IEC 61000-2-4 Class 2	±10 % [a]		+10 % / –15 % [a]	
Voltage dips [c]	IEC 61000-4-11 [d] or IEC 61000-4-34 [d]	Volts remaining	Cycles	Volts remaining	Cycles
		0 %	1	0 %	1
		40 %	25/30 [b]	40 %	10/12 [b]
		70 %	25/30 [b]	70 %	25/30 [b]
		–	–	80 %	250/300 [b]
Voltage dips for auxiliary DC power ports below 60 V [e]	IEC 61000-4-29	40 %	0,5	40 %	0,5
		70 %	0,5	70 %	0,5
Short interruptions	IEC 61000-4-11 [d] or IEC 61000-4-34 [d]	Volts remaining	Cycles	Volts remaining	Cycles
		–	–	0 %	10/12 [b]
		0 %	25/30 [b]	0 %	25/30 [b]
		0 %	250/ 300 [b]	0 %	250/300 [b]

[a] "Voltage deviation" is a supply voltage variation from the nominal supply voltage. Testing of voltage deviations for three phase PDS requires increasing or reducing the voltage of all three phases simultaneously.

[b] "x/y cycles" means "x cycles for 50 Hz test" and "y cycles for 60 Hz test"

[c] Power ports with current rating ≥75 A, the method of the voltage drop test according to IEC 61400-21:2008, 7.5 can be used.

[d] IEC 61000-4-11 applies to equipment rated less than or equal to 16 A and IEC 61000-4-34 to equipment rated above 16 A.

[e] This test addresses external DC power supplies which provide power to the safety sub-function(s)

NOTE No conducted common mode tests are required due to the higher emission of conducted common mode voltage by a *PDS(SR)* compared to the test levels of IEC 61000-6-7.

Table E.2 – *PDS(SR)* minimum immunity requirements for voltage deviations, dips and short interruptions on main power ports with a rated voltage above 1 000 V

Phenomenon	Reference document	Level	
Voltage deviations exceeding 1 min	IEC 61000-2-4 Class 3	+10 % / –15 %	
Voltage deviations not exceeding 1 min	IEC 61000-2-4 Class 3	+10 % / –15 %	
Voltage dips	IEC 61000-4-34 [b]	Volts remaining	Cycles
		0 %	1
		40 %	10/12 [c]
		70 %	25/30 [c]
		80 %	250/300 [c]
Voltage dips for auxiliary DC power ports below 60 V [e]	IEC 61000-4-29	40 %	0,5
		70 %	0,5
Short interruptions	IEC 61000-4-34 [b]	Volts remaining	Cycles
		0 %	10/12 [b]
		0 %	25/30 [b]
		0 %	250/300 [c]

[a] "Voltage deviation" is a supply voltage variation from the nominal supply voltage. Testing of voltage deviations for three phase PDSs requires increasing or reducing the voltage of all three phases simultaneously.

When considering voltage deviations, any voltage steps shall not exceed ±12 % of nominal voltage and the time between steps shall not be less than 2 s.

When the voltage is below nominal, the maximum output power ratings – speed and/or torque – can be reduced, because they are voltage dependent.

[b] Typical depths and durations of voltage dips are given in IEC 61000-2-8.

[c] "x/y cycles" means "x cycles for 50 Hz test" and "y cycles for 60 Hz test".

[d] Opening of fuses is permitted for line-commutated converters operating in inverting mode.

[e] This test addresses external DC power supplies which provide power to the safety sub-function(s).

E.3 Immunity requirements – high frequency disturbances

Table E.3 – Immunity requirements – high frequency disturbances

1	2	3	4	5
Port/interface	**Phenomenon**	**Basic standard for test method**	**Level for first environment**	**Level for second environment**
Enclosure port	ESD [m n] air discharge (AD) [o] contact discharge (CD)	IEC 61000-4-2 [q]	4 kV CD or 8 kV AD if CD impossible	6 kV CD or 8 kV AD if CD impossible 8kV CD or 15 kV AD [m]
	Radio-frequency electromagnetic field, amplitude modulated [p]	IEC 61000-4-3*	80 MHz to 1 000 MHz 10 V/m 80 % AM (1 kHz)	80 MHz to 1 000 MHz 20 V/m [i g] 80 % AM (1 kHz)
	Radio-frequency electromagnetic field, amplitude modulated [p]	IEC 61000-4-3*	1,4 GHz to 2,0 GHz 3 V/m 80 % AM (1 kHz)	1,4 GHz to 2,0 GHz 10 V/m [i g] 80 % AM (1 kHz)
	Radio-frequency electromagnetic field, amplitude modulated [p]	IEC 61000-4-3*	2,0 GHz to 2,7 GHz 1 V/m 80 % AM (1 kHz)	2,0 GHz to 6 GHz 3 V/m [i g] 80 % AM (1 kHz)
Power ports (except auxiliary DC power ports below 60 V)	Fast transient-burst	IEC 61000-4-4 [h]	2 kV/5 kHz [a]	4 kV/5kHz [a]
	Surge [b] 1,2/50 µs, 8/20 µs	IEC 61000-4-5 [r]	1 kV [c] 2 kV [d]	2 kV [c] 4 kV [d]
	Conducted radio-frequency common mode [e]	IEC 61000-4-6*	0,15 MHz to 80 MHz 10 V 80 % AM (1 kHz)	0,15 MHz to 80 MHz [k] 20 V [g] 80 % AM (1 kHz)
Power interfaces	Fast transient-burst [e]	IEC 61000-4-4 [h]	2 kV/5 kHz Capacitive clamp	4 kV/5 kHz Capacitive clamp
Signal interfaces	Fast transient-burst [e]	IEC 61000-4-4 [h]	1 kV/5 kHz Capacitive clamp	2 kV/5 kHz Capacitive clamp
	Conducted radio-frequency common mode [e]	IEC 61000-4-6*	0,15 MHz to 80 MHz 10 V 80 % AM (1 kHz)	0,15 MHz to 80 MHz [k] 20 V [g] 80 % AM (1 kHz)
Ports for process measurement control lines Auxiliary DC power ports below 60 V	Fast transient-burst [e]	IEC 61000-4-4 [h]	2 kV/5 kHz Capacitive clamp	**4** kV/5 kHz Capacitive clamp
	Surge [f] 1,2/50 µs, 8/20 µs	IEC 61000-4-5 [r]	1 kV [d f]	2 kV [d f]
	Conducted radio-frequency common mode [e]	IEC 61000-4-6*	0,15 MHz to 80 MHz 10 V 80 % AM (1 kHz)	0,15 MHz to 80 MHz [k] 20 V [g] 80 % AM (1 kHz)

* See also IEC 61800-3:2012, 5.3.4.

NOTE The required immunity for *functional safety* purposes can be achieved through the use of external protection devices.

[a] Power ports with current rating <100 A: direct coupling using the coupling and decoupling network. Power ports with current rating ≥100 A: direct coupling or capacitive clamp without decoupling network. If the capacitive clamp is used, the test level shall be 4 kV/ 5 kHz or 100 kHz.

[b] Applicable only to power ports with current consumption <63 A during light load test conditions as specified in 5.1.3. of IEC 61800-3:2012. The rated impulse voltage of the basic insulation shall not be exceeded (see IEC 60664-1).

[c] Coupling line-to-line.

[d] Coupling line-to-earth.

[e] Applicable only to ports or interfaces with cables whose total length according to the manufacturer's functional specification can exceed 3 m.

[f] Applicable only to ports with cables whose total length according to the manufacturer's functional specification can exceed 30 m. In the case of a shielded cable, a direct coupling to the shield is applied. This immunity requirement does not apply to fieldbus or other signal interfaces where the use of surge protection devices is not practical for technical reasons. The test is not required where normal functioning cannot be achieved because of the impact of the coupling/decoupling network on the equipment under test (EUT).

[g] The test level specified is the r.m.s. value of the unmodulated carrier.

[h] For an *PDS(SR)* intended to be used in *safety integrity level SIL* 3 applications (according to IEC 61508), the duration of the test at the highest specified level shall be increased by a factor of 5 compared to the duration as given in the basic standard.

[i] These increased values shall be applied in the frequency ranges as given in Table E.4 used for mobile transmitters in general.

[k] These increased values shall be applied in the frequency ranges as given in Table E.5 used for mobile transmitters in general.

[m] The higher test levels apply in case the discharge is done onto cabinet enclosures.

[n] Levels shall be applied in accordance with the environmental conditions described in IEC 61000-4-2 on parts which can be accessible by persons other than trained personnel in accordance with defined procedures for the control of ESD but not to equipment where access is limited to service personnel only.

[o] For air discharge test not only the given level has to be tested, but all the levels up to the given one.

[p] If hand held radio transmitters could be used closer than 20 cm a warning shall be given in the safety manual that the *PDS (SR)* could be disturbed.

[q] For a *PDS(SR)* intended to be used in *safety integrity level SIL* 3 applications, the number of discharges shall be increased by the factor of 3.

[r] For a *PDS(SR)* intended to be used in *safety integrity level SIL* 3 applications, the number of surge pulses shall be increased by the factor of 3.

Table E.4 – General frequency ranges for mobile transmitters and ISM for radiated tests

Centre frequency MHz	**Frequency range** MHz	**Purpose**
84,000	83,996 to 84,004	ISM (UK only)
	137 to 174	Mobile and SRD
151,850	151,820 to 151,880	MURS
154,585	154,570 to 154,600	MURS
168,000	167,992 to 168,008	ISM UK only
219,500	219 to 220	AMATEUR
	380 to 400	TETRA
	420 to 470	AMATEUR
433,920	433,05 to 434,79	ISM (Region 1 only)
	450 to 470	4G/LTE-A
	698 to 894	3G/UMTS3.9G/LTE
	746 to 845	TETRA
	825 to 845	TETRA
	830 to 840	3G/FOMA
	860 to 915	3.9G/LTE
873,000	870 to 876	TETRA
	860 to 960	RFID
	886 to 906	ISM UK only
	880 to 915	GSM 3G/FOMA 3G/HSPA
918,000	915 to 921	NADC
	902 to 928	ISM (Region 2 only)
	925 to 960	GSM 3G/HSPA
	1 240 to 1 300	AMATEUR
	1 428 to 1 496	3G/UMTS 3G/HSPA 3.9G/LTE
	1476 to 1511 1525 to 1559 1627 to 1661 1710 to 1785	3.9G/LTE
	1 710 to 1 785	GSM 3G/UMTS 3G/FOMA 3G/HSPA
	1 805 to 1 880	GSM 3G/UMTS 3G/FOMA 3G/HSPA 3.9G/LTE
	1 900 to 2 025	3G/UMTS 3G/FOMA 3.9G/LTE
	2 110 to 2 200	3G/UMTS 3G/FOMA 3.9G/LTE
	2 300 to 2 450	AMATEUR
	2 400 to 2 500	ISM
	2300 to 2400	3.9G/LTE 4G/LTE-A
	2 500 to 2 690	3.9G/LTE
	3 300 to 3 500	AMATEUR
	3 400 to 3 600	4G/LTE-A
	5 150 to 5 350	HIPERLAN
	5 470 to 5 725	HIPERLAN
	5 650 to 5 925	AMATEUR
	5 725 to 5 875	ISM
	5 795 to 5 815	RTTT

Table E.5 – General frequency ranges for mobile transmitters and ISM for conducted tests

Centre frequency MHz	**Frequency range** MHz	**Purpose**
3,39	3,370 to 3,410	ISM Netherlands only
6,780	6,765 to 6,795	ISM
13,560	13,553 to 13,567	ISM
27,120	26,957 to 27,283	ISM/CB/SRD
40,680	40,66 to 40,70	ISM/SRD
For those frequency bands where a centre frequency is indicated the test shall be performed at the centre frequency only.		

Annex F
(informative)

Estimation of PFD$_{avg}$ value for low demand with given PFH value

F.1 General

While low demand mode operation is possible for a *PDS(SR)*,this standard concentrates on to high demand and continuous mode, no requirements are given for low demand mode. *Safety sub-functions* implemented for high demand or continuous mode can be used in low demand mode. For this case a simplified conservative method to estimate the PFD$_{avg}$ value from the PFH value is given in this annex.

NOTE 1 For the limits of the PFD$_{avg}$ value regarding *SIL* see IEC 61508-1.

NOTE 2 For the design of a *PDS(SR)* especially for low demand mode see IEC 61508 series.

F.2 Estimation of PFD$_{avg}$ value for low demand with given PFH value

For an electrical power drive system with a specified *safety sub-function* quantified by a related *PFH* value for high demand or continuous *mode of operation*, an estimated value for the PFD*avg* in a low demand application can be derived from the *PFH* under certain circumstances. Provided that

1) the *safety sub-function* to be used in the low demand application is exactly the same as specified for high demand or continuous *mode of operation*, e.g. safe torque off (STO), and the system states regarded as safe states in the context of the high demand or continuous mode *safety sub-function* are also safe states in the context of the low demand application (e.g. de-energized output),
2) compulsory actuations of the *safety sub-function* needed for testing, if any, are executed in accordance with the requirements of the manufacturer,

an estimated value for the PFD$_{avg}$ may be derived from the *PFH* value for high demand using the following equation:

$$PFD_{avg} = \frac{1}{2} PFH \cdot T_M$$

where T_M is the specified *mission time* of the *PDS(SR)* expressed in hours.

NOTE 1 The indicated PFD$_{avg}$ equation tends to deliver conservative results.

NOTE 2 Considering a particular *PDS(SR)*, PFD$_{avg}$ often consumes a higher proportion of the PFD$_{avg}$ limit of a certain *SIL* than its *PFH* will consume with respect to the *PFH* limit of the same *SIL*. It can occur that the *PFH* value complies with a certain *SIL* while the PFD$_{avg}$ value derived from the above given formula does not. For the limits of the PFD$_{avg}$ value regarding *SIL,* see IEC 61508-2:2010.

NOTE 3 For *PFH* value estimation see 6.2.2.1.2.

NOTE 4 For description of PFD$_{avg}$ see IEC 61508-4:2010; 3.6.18.

Bibliography

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

IEC 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 60664-1:~~1992~~ 2007, *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~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

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~~ application programming 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 61558-1:2005/AMD1:2009

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

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*

IEC 62425, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

~~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*

EN 50495:2010, *Safety devices required for the safe functioning of equipment with respect to explosion risks*

IFA Report 7/2013e *"Safe drive controls with frequency converters"*
http://www.dguv.de/ifa/Publikationen/Reports-Download/Reports-2013/IFA-Report-7-2013/index-2.jsp

____

IEC 61800-5-2

Edition 2.0 2016-04

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

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 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 second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) rational added in the scope why low demand mode is not covered by this standard
b) definition added for: "*category*" and "*safety function*"
c) "Other sub-functions" sorted into "Monitoring sub-functions" and "Output functions"
d) deleted "proof test" throughout the document because for *PDS(SR)* a proof test is not applicable

e) replaced the term “safety function” by “*safety sub-function*” throughout the document

f) Updated references to IEC 61508 series Ed.2010

g) Added the principle rules of ISO 13849-1 and reference to tables of ISO 13849-2

h) 6.1.6 Text replaced by Table 2

i) 6.1.7 Integrated circuits with on-chip redundancy matched to changed requirement in IEC 61508-2: 2010, Annex E

j) 6.2.8 Design requirements for thermal immunity of a *PDS(SR)*

k) 6.2.9 Design requirements for mechanical immunity of a *PDS(SR)*

l) 6.1.6 *SIL* for multiple *safety sub-functions* within one *PDS(SR)*

m) 6.1.7 Integrated circuits with on-chip redundancy

n) 6.2.1 Basic and well-tried safety principles

o) 6.2.2.1.4 *Diagnostic test* interval when the hardware fault tolerance is greater than zero

p) 6.2.5.2.7 *PDS(SR)* parameterization

q) 9 Test requirements

r) 9.3 Electromagnetic (EM) immunity testing

s) 9.4 Thermal immunity testing

t) 9.5 Mechanical immunity testing

u) Annex A Sequential task table

v) Annex D, D.3.16, Motion and position feedback sensors updated

w) Annex E Electromagnetic immunity (EM) requirement for *PDS(SR)*

x) Annex F Estimation of PFD_{avg} value for low demand with given PFH value

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

FDIS	Report on voting
22G/332/FDIS	22G/335/RVD

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

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

A list of all parts of the IEC 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 stability date indicated on the IEC website 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 performance level PL) 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 as machine safety standards dealing with detailed safety requirements for a particular machine or group of machines.

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 *hazard*s where access to the dangerous area is only possible when rotating parts have stopped. This part of IEC 61800 gives a methodology to identify the contribution made by a *PDS(SR)* to identified *safety sub-function*s 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

This part of IEC 61800, which is a product standard, specifies requirements and makes recommendations for the design and development, integration and validation of safety related power drive systems (*PDS(SR))* in terms of their functional safety considerations. It applies to adjustable speed electrical power drive systems covered by the other parts of the IEC 61800 series of standards as referred in IEC 61800-2.

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

NOTE 2 Other parts of IEC 61800 cover rating specifications, EMC, electrical safety, etc.

This International Standard is applicable where functional safety of a *PDS(SR)* is claimed and the *PDS(SR)* is operating mainly in the high demand or continuous mode (see 3.15)

While low demand mode operation is possible for a *PDS(SR)*, this standard concentrates on high demand and continuous mode. *Safety sub-function*s implemented for high demand or continuous mode can also be used in low demand mode. Requirements for low demand mode are given in IEC 61508 series. Some guidance for the estimation of average probability of dangerous failure on demand (PFD$_{avg}$) value is provided in Annex F.

This part of IEC 61800 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 *subsystem*s of a safety-related system. It is intended to facilitate the realisation of the electrical/ electronic/ programmable electronic (E/E/PE) parts of a *PDS(SR)* in relation to the safety performance of *safety sub-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 (system integrator, original equipment manufacturer) 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).

By applying the requirements from this part of the IEC 61800 series, the corresponding requirements of IEC 61508 that are necessary for a *PDS(SR)* are fulfilled.

This part of IEC 61800 does not specify requirements for:

- the *hazard* and risk analysis of a particular application;
- the identification of *safety sub-function*s for that application;
- the initial allocation of *SIL*s to those *safety sub-function*s;
- the driven equipment except for interface arrangements;
- secondary *hazard*s (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)*.

- security aspects (e.g. cyber security or *PDS(SR)* security of access)

NOTE 3 The functional safety requirements of a *PDS(SR)* are dependent on the application, and can be considered as a part of the overall risk assessment of the *installation*. Where the supplier of the *PDS(SR)* is not 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)*.

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

Figure 1 shows the installation and the functional parts of a *PDS(SR)* that are considered in this part of IEC 61800 and shows a logical representation of a *PDS(SR)* rather than its physical description.

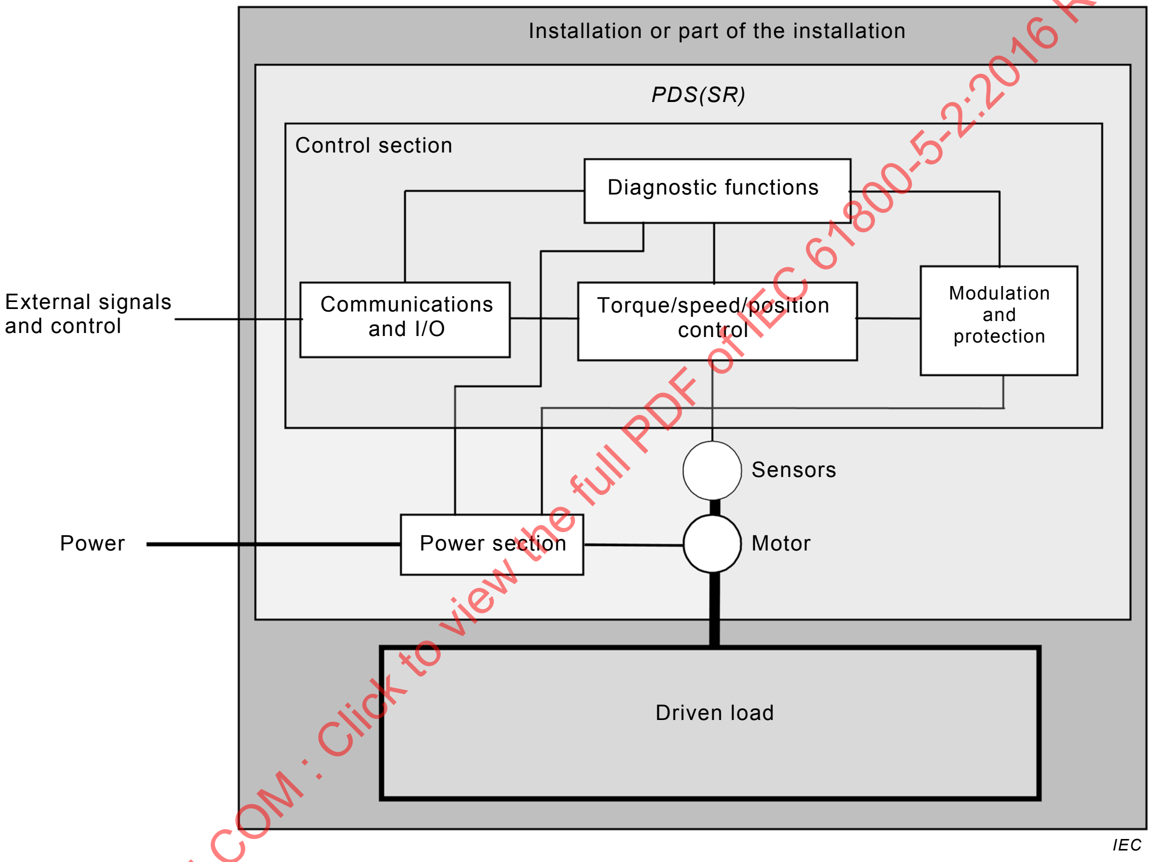

Installation or part of the installation
PDS(SR)
Control section
Diagnostic functions
External signals and control
Communications and I/O
Torque/speed/position control
Modulation and protection
Sensors
Power
Power section
Motor
Driven load
IEC

Figure 1 – Installation and functional parts of a *PDS(SR)*

2 Normative references

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

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

IEC 61000-2-4:2002, *Electromagnetic compatibility (EMC) – Part 2-4: Environment – Compatibility levels in industrial plants for low-frequency conducted disturbances*

IEC 61000-4-2:2008, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3:2006, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*
IEC 61000-4-3:2006/AMD1:2007
IEC 61000-4-3:2006/AMD2:2010

IEC 61000-4-4:2012, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5:2014, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6:2013, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-29:2000, *Electromagnetic compatibility (EMC) – Part 4-29: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests*

IEC 61000-4-34:2005, *Electromagnetic compatibility (EMC) – Part 4-34: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests for equipment with input current more than 16 A per phase*

IEC 61000-6-7:2014, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61400-21:2008, *Wind turbines – Part 21: Measurement and assessment of power quality characteristics of grid connected wind turbines*

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

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

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

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:2010, *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 61800-2:2015, *Adjustable speed electrical power drive systems – Part 2: General requirements – Rating specifications for low voltage adjustable speed a.c. power drive systems*

IEC 61800-3:2004, *Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods*
IEC 61800-3:2004/AMD1:2011

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 61800-5-1:2007, *Adjustable speed electrical power drive systems – Part 5-1: Safety requirements – Electrical, thermal and energy*

ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. Table 1 shows an alphabetical list of terms and definitions

Table 1 – Alphabetical list of terms and definitions

3.1	basic drive module BDM	3.12	hazard	3.23	safety sub-function(s) (of a PDS(SR))
3.2	category	3.13	installation	3.24	safety integrity
3.3	complete drive module CDM	3.14	mission time TM	3.25	safety integrity level SIL
3.4	common cause failure	3.15	mode of operation	3.26	safety-related system
3.5	dangerous failure	3.16	PDS(SR)	3.27	safety requirements specification SRS
3.6	diagnostic coverage DC	3.17	average frequency of a dangerous failure PFH	3.28	SIL capability
3.7	diagnostic test(s)	3.18	Performance Level PL	3.29	subsystem
3.8	fail safe	3.19	safe failure	3.30	systematic failure
3.9	fail safe state FS	3.20	safe failure fraction SFF	3.31	systematic safety integrity
3.10	fault reaction function	3.21	safe state	3.32	validation
3.11	functional safety	3.22	safety function	3.33	verification

NOTE Throughout this International Standard, references to the following definitions are identified by writing them in *italic* script.

3.1
basic drive module
BDM
electronic power converter and related control, connected between an electric supply and a motor

Note 1 to entry: The *BDM* is capable of transmitting power from the electric supply to the motor and can be capable of transmitting power from the motor to the electric supply.

Note 2 to entry: The *BDM* controls some or all of the following aspects of power transmitted to the motor and motor output: current, frequency, voltage, speed, torque, force.

Note 3 to entry: This note applies to the French language only.

[SOURCE: IEC 61800-3:2004/AMD1:2011, 3.1.1]

3.2
category
classification of the safety-related parts of a *PDS(SR)* in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

[SOURCE: ISO 13849-1, definition 3.1.2, modified] "control system" replaced by "*PDS(SR)"*

3.3
complete drive module
CDM
drive module consisting of, but not limited to, the *BDM* and extensions such as protection devices, transformers and auxiliaries, but excluding the motor and the sensors which are mechanically coupled to the motor shaft

Note 1 to entry: This note applies to the French language only.

[SOURCE: IEC 61800-3:2004/AMD1:2011, 3.1.2]

3.4
common cause failure
failure, which is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to failure of the *safety sub-function*

[SOURCE: IEC 61508-4:2010, 3.6.10 modified – "leading to system failure" replaced by "leading to failure of the *safety sub-function*"]

3.5
dangerous failure
failure of a component and/or *subsystem* and/or system that plays a part in implementing the *safety sub-function* that:

a) causes a *safety sub-function* of a *PDS(SR)* to fail such that the equipment or machinery driven by the *PDS(SR)* is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the *safety sub-function* operates correctly

[SOURCE: IEC 61508-4:2010, 3.6.7, modified – "EUC" replaced by "*PDS(SR)*", "when required" deleted]

3.6
diagnostic coverage
DC
fraction of dangerous failures detected by automatic *diagnostic tests*

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

Note 2 to entry: *Diagnostic coverage* can exist for the whole or parts of a *safety-related system*. For example, *diagnostic coverage* can exist for sensors and/or logic *subsystems* and/or output *subsystem*.

Note 3 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4: 2010; 3.8.6, modified – "on-line" deleted from "online diagnostic tests"]

3.7
diagnostic test
test intended to detect faults or failures and produce a specified output when a fault or failure is detected

3.8
fail safe
design property of an item which prevents its failures from resulting in dangerous faults

[SOURCE: IEC 60500:1998, 821-01-10, modified – “critical” replaced by “dangerous”]

3.9
fail safe state
FS
defined *safe state*, typically resulting from a failure

Note 1 to entry: Fail safe state (*FS*) is used in this standard instead of the defined state (DS) of IEC 61000-6-7.

Note 2 to entry: This note applies to the French language only.

3.10
fault reaction function
function that is initiated when a fault or failure within the *PDS(SR)*, which could cause a loss of the *safety sub-function*, is detected, and which is intended to maintain the safety of the *installation* or prevent *hazardous* conditions arising at the *installation*

3.11
functional safety
part of the overall safety relating to the *PDS(SR)* which depends on the correct functioning of the *safety-related parts of the PDS(SR)* and on external risk reduction measures

Note 1 to entry: This standard only considers those aspects in the definition of *functional safety* that depend on the correct functioning of the *PDS(SR)*.

[SOURCE: IEC 61508-4:2010; 3.1.12, modified – “EUC and the EUC control system” replaced by “*PDS(SR)*”; “E/E/PE safety-related systems and other” replaced by “*safety-related parts of the PDS(SR)* and on external”]

3.12
hazard
potential source of harm

Note 1 to entry: 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).

[SOURCE: IEC 60050-351:2013, 351-57-01, modified note 1 to entry]

3.13
installation
PDS(SR), equipment driven by the *PDS(SR)* and possibly other equipment (see Figure 1)

Note 1 to entry: The word “*installation*” is also used in this international standard to denote the process of installing a *PDS(SR)*. In these cases, the word “act of installing” will be used in this standard.

3.14
mission time
TM
specified cumulative operating time of the safety-related parts of the *PDS(SR)* during its overall lifetime

Note 1 to entry: This note applies to the French language only.

3.15
mode of operation

way in which a *safety sub-function* is intended to be used, with respect to the rate of demands made upon it, which may be either low demand mode, high demand or continuous mode.

Note 1 to entry: Low demand mode: where the rate of demands for operation made on a *safety sub-function* is no greater than one per year.

Note 2 to entry: High demand and continuous mode: where the rate of demands for operation made on a *safety sub-function* is greater than one per year.

Note 3 to entry: 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 mainly considered to operate in the high demand mode or continuous mode.

[SOURCE: IEC 61508-4:2010; 3.5.16, modified – “high demand mode” and continuous mode” combined; definition reduced to statements of time]

3.16
PDS(SR)

adjustable speed electrical power drive system providing *safety sub-function*s

3.17
average frequency of a dangerous failure
PFH

average frequency of a dangerous failure of a *PDS(SR)* to perform the specified *safety sub-function* over a given period of time

Note 1 to entry: In IEC 62061 the abbreviation *PFH_D* is used.

Note 2 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4:2010; 3.6.19, modified – “E/E/PE safety-related system” replaced by “*PDS(SR)”*]

3.18
Performance Level
PL

discrete level used to specify the ability of safety-related parts of control systems to perform a *safety sub-function* under foreseeable conditions

[SOURCE: ISO 13849-1:2006, 3.1.23, modified – “*safety function*” replaced by “*safety sub-function”*]

3.19
safe failure

failure of a component and/or *subsystem* and/or system that plays a part in implementing the *safety sub-function* that:

a) results in the spurious operation of the *safety sub-function* to put the *PDS(SR)* (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the *safety sub-function* to put the *PDS(SR)* (or part thereof) into a safe state or maintain a safe state

[SOURCE: IEC 61508-4:2010; 3.6.8 modified – “element” replaced by “component”; “EUC” replaced by “*PDS(SR)*”]

3.20
safe failure fraction
SFF
property of a safety related component and *subsystems* that is defined by the ratio of the sum of the average failure rates of safe and dangerous detected failures to the sum of safe and all dangerous failures.

Note 1 to entry: This ratio is represented by the equation: $SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

Note 2 to entry: See Annex C of IEC 61508-2:2010.

Note 3 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4:2010; 3.6.15, modified – “element” replaced by “component and *subsystems*”]

3.21
safe state
state of the *PDS(SR)* when safety is achieved

Note 1 to entry: In going from a potentially hazardous condition to the final safe state, the *PDS(SR)* can have to go through a number of intermediate safe states.

[SOURCE: IEC 61508-4:2010; 3.1.13, modified – “EUC” replaced by “*PDS(SR)*”]

3.22
safety function
function to be implemented by a safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the equipment or machinery driven by the PDS(SR), in respect of a specific hazardous event.

[IEC 61508-4:2010; 3.5.1, modified – “E/E/PES” deleted, “EUC” replaced by “the equipment or machinery driven by the *PDS(SR)*”]

3.23
***safety sub-function*, <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 safety of the *installation* or prevent *hazardous* conditions arising at the *installation*

Note 1 to entry: There are only rare cases where the safety function of the complete application is implemented exclusively within the *PDS(SR)*. In these cases the safety function is still called a *safety sub-function* in this standard. (e.g. always active SLS without external initiation)

3.24
safety integrity
probability of a *PDS(SR)* satisfactorily performing a required *safety sub-function* under all stated conditions within a stated period of time

Note 1 to entry: 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 sub-function*.

Note 2 to entry: The *safety integrity* can be different for each *safety sub-function* performed by the *PDS(SR)*.

[SOURCE: IEC 61508-4:2010; 3.5.4, modified – “E/E/PE safety-related system” replaced by “*PDS(SR)*”]

3.25
safety integrity level
SIL
discrete level (one out of a possible three) for specifying the *safety integrity* requirements of a *safety sub-function* allocated (in whole or in part) to a *PDS(SR)*

Note 1 to entry: *SIL* 3 has the highest level of *safety integrity* and *SIL* 1 has the lowest.

Note 2 to entry: *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.

Note 3 to entry: Several methods of writing are used for *SIL*x. Throughout this document *SIL* × is used

Note 4 to entry: This note applies to the French language only.

[SOURCE: IEC 61508-4:2010; 3.5.8, modified – "corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest" replaced by "for specifying the *safety integrity* requirements of a *safety sub-function* allocated (in whole or in part) to a *PDS(SR)*"]

3.26
safety-related system
designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the equipment or machinery driven by the *PDS(SR)*; and
- is intended to achieve, on its own or with other risk reduction measures, the necessary safety integrity for the required safety functions

[SOURCE: IEC 61508-4:2010; 3.4.1, modified] "EUC" replaced by "equipment or machinery driven by the *PDS(SR)",* "E/E/PES" deleted.

3.27
safety requirements specification
SRS
specification containing all the requirements of the *safety sub-function*s to be performed by the *PDS(SR)*

Note 1 to entry: This note applies to the French language only.

3.28
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 1 to entry: Each of the designated *safety sub-function*s that a *PDS(SR)* is intended to perform can be associated with a different *SIL capability*.

Note 2 to entry: *SIL* capability includes systematic capability, the fulfillment of the architectural constraints and the hardware failure rate or PFH value.

3.29
subsystem
part of the top-level architectural design of a *safety-related system*, failure of which results in failure of a *safety-related function*

Note 1 to entry: A *PDS(SR)* can itself be a *subsystem*, or be made up from a number of separate *subsystem*s, which when put together to implement the *safety sub-function* under consideration. A *subsystem* can have more than one channel.

Note 2 to entry: Examples of *subsystem*s of a *PDS(SR)* are encoder, power section, control section (see Figure 1).

3.30
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 1 to entry: Examples of causes of *systematic failure*s include human error in:

- the *safety requirements specification*;
- the design, manufacture, act of installing, operation of the hardware;
- the design and implementation of the software.

Note 2 to entry: In this standard, failures in a safety-related system are categorized as random hardware failures or systematic failures.

[SOURCE: IEC 61508-4:2010, 3.6.6]

3.31
systematic safety integrity
part of the *safety integrity* of *safety-related system*s relating to *systematic failures* in a dangerous mode of failure

Note 1 to entry: *Systematic safety integrity* cannot usually be quantified (as distinct from hardware safety integrity which usually can).

[SOURCE: IEC 61508-4:2010; 3.5.6]

3.32
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: *Validation* is the activity of demonstrating that the *PDS(SR)*, before or after act of installing , meets in all respects the *safety requirements specification* .

[SOURCE: IEC 61508-4:2010, 3.8.2, modified Note 1 to entry]

3.33
verification
confirmation by examination and provision of objective evidence that the requirements have been fulfilled

[SOURCE: IEC 61508-4:2010, 3.8.1, modified – removal of Note 1 to entry]

4 Designated *safety sub-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 sub-function*s in this clause are not considered to form an exhaustive list. Details of implementation for basic *safety sub-function*s, and complex *safety sub-function*s composed of more than one basic *safety sub-function*, have not been provided because of the large number of possibilities. In some cases, further *safety-related system*s external to the *PDS(SR)* (for example a mechanical brake) may be necessary to maintain the safety when electrical power is removed.

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

Each *safety sub-function* may include safe inputs and/or outputs in order to accomplish necessary communication with (or activation of) other functions, *subsystem*s or systems (which may or may not be safety-related).

Some of the *safety sub-function*s perform monitoring tasks only; some perform safety relevant control or other actions. Therefore, a distinction shall 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 sub-function*; and

– the *fault reaction function* (relevant for all *safety sub-functions*):

  the reaction function when diagnostics detect a fault within the *safety sub-function*.

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

On selecting the appropriate reaction function, it shall 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 5.5).

The names of the *safety sub-function*s 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)*.

NOTE For detailed examples of the *PDS(SR)* sub-functions specified in this clause see Bibliography (IFA Report 7/2013e)

4.2 *Safety sub-functions*

4.2.1 General

In most cases the *safety functions* of the *PDS(SR)* are a part of the *safety functions* of an application, therefore the *safety functions* of the *PDS(SR)* are named *safety sub-functions* in this document. Figure 2 shows an example of a *safety function* consisting of *safety sub-functions*:

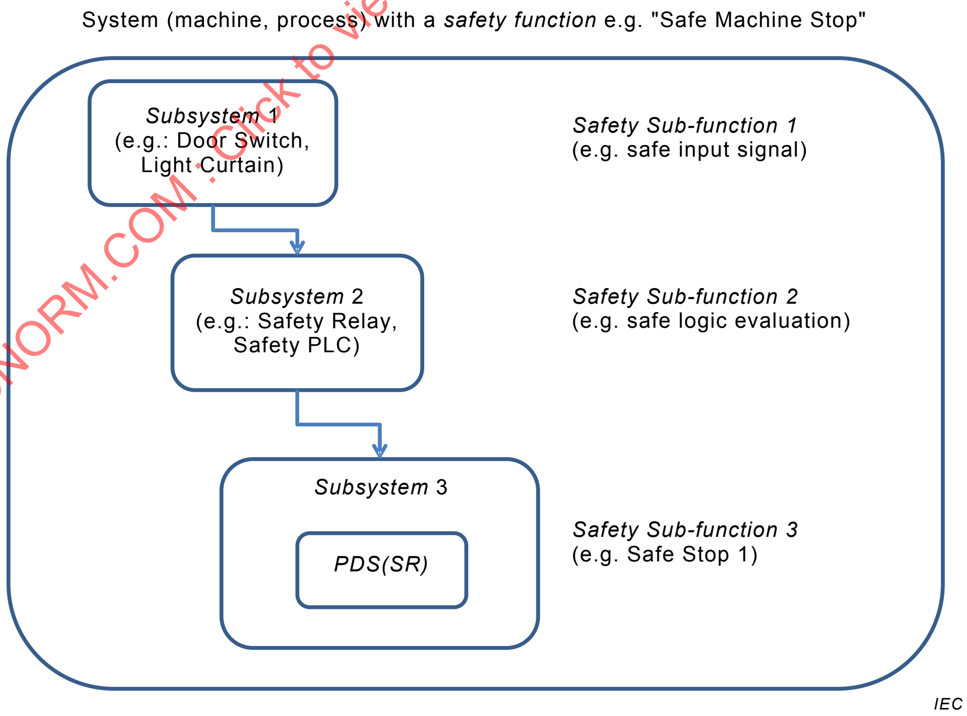

System (machine, process) with a *safety function* e.g. "Safe Machine Stop"
Subsystem 1
(e.g.: Door Switch, Light Curtain)
Safety Sub-function 1
(e.g. safe input signal)
Subsystem 2
(e.g.: Safety Relay, Safety PLC)
Safety Sub-function 2
(e.g. safe logic evaluation)
Subsystem 3
PDS(SR)
Safety Sub-function 3
(e.g. Safe Stop 1)
IEC

Figure 2 – *Safety function* consisting of *safety sub-functions*

NOTE For further information regarding *safety sub-functions* see IFA Report 7/2013e “Safe drive controls with frequency converters” (Bibliography).

4.2.2 Limit values

Where a *safety sub-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 can 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 4.2.4.9 can take into account the maximum allowable over travel distance(s).

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

4.2.3 Stopping functions

4.2.3.1 General

A variety of stopping methods is available for every type of *PDS(SR).*

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 stopping functions.

NOTE When applying safety stopping functions for functions like prevention of unexpected start-up or emergency stop, relevant standards can be considered, e. g. IEC 60204-1, ISO 13850, ISO 12100, ISO 14118.

Any particular requirements for stopping performance can be specified by the customers of the *PDS(SR)* manufacturer. The following examples of stopping functions are often used in practice.

4.2.3.2 Safe torque off (STO)

This function prevents force-producing power from being provided to the motor

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

NOTE 1 This *safety sub-function* can be used where power removal is required to prevent an unexpected start-up according to ISO 14118.

NOTE 2 In circumstances where external influences (for example, falling of suspended loads) are present, additional measures (for example, mechanical brakes) can be necessary to prevent any *hazard*.

NOTE 3 Electronic means and some contactors are not adequate for protection against electric shock.

NOTE 4 While the function is active, a limited amount of movement is still possible in the event of a failure in the power section of the *PDS(SR)*

4.2.3.3 Safe stop 1 (SS1)

This function is specified as either

a) Safe Stop 1 deceleration controlled

   SS1-d

   initiates and controls the motor deceleration rate within selected limits to stop the motor and performs the STO function (see 4.2.3.2) when the motor speed is below a specified limit; or

b) Safe Stop 1 ramp monitored

   SS1-r

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

c) Safe Stop 1 time controlled

SS1-t

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

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

NOTE The controlled stop of SS1-t can fail undetected, therefore SS1-t cannot be applied if this failure can cause a dangerous situation in the final application.

4.2.3.4 Safe stop 2 (SS2)

This function is specified as either

a) Safe Stop 2 deceleration controlled

SS2-d

initiates and controls the motor deceleration rate within selected limits to stop the motor and performs the safe operating stop function (see 4.2.4.1) when the motor speed is below a specified limit; or

b) Safe Stop 2 ramp monitored

SS2-r

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

c) Safe Stop 2 time controlled

SS2-t

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

This *safety sub-function* SS2 corresponds to a controlled stop in accordance with stop category 2 of IEC 60204-1.

NOTE The controlled stop of SS2-t can fail undetected, therefore SS2-t cannot be applied if this failure can cause a dangerous situation in the final application.

4.2.4 Monitoring functions

4.2.4.1 General

In the following function descriptions “prevents” is written when there is a single limit only and “keeps” is written when there is an upper and lower limit. Otherwise there is no difference in intent.

4.2.4.2 Safe operating stop (SOS)

This 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.

4.2.4.3 Safely-limited acceleration (SLA)

This function prevents the motor from exceeding the specified acceleration and/or deceleration limit.

4.2.4.4 Safe acceleration range (SAR)

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

4.2.4.5 Safely-limited speed (SLS)

This function prevents the motor from exceeding the specified speed limit.

4.2.4.6 Safe speed range (SSR)

This function keeps the motor speed within specified limits.

4.2.4.7 Safely-limited torque (SLT)

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

4.2.4.8 Safe torque range (STR)

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

4.2.4.9 Safely-limited position (SLP)

This function prevents the motor shaft (or mover, when a linear motor is used) from exceeding the specified position limit(s).

4.2.4.10 Safely-limited increment (SLI)

This function prevents the motor shaft (or mover, when a linear motor is used) from exceeding the specified limit of position increment.

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

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

4.2.4.11 Safe direction (SDI)

This function prevents the motor shaft from moving more than a defined amount in the unintended direction.

4.2.4.12 Safe motor temperature (SMT)

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

NOTE The SMT *safety sub-function* can be used to protect against over temperature of a motor applied in an explosive atmosphere. Other risks like sparks are not covered by this *safety sub-function*. For further information, see IEC 60079 series of standards. General information for the use of *PDS(SR)* in explosive atmosphere applications is provided in IEC 61800-2:2015.

4.2.4.13 Safe cam (SCA)

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

4.2.4.14 Safe speed monitor (SSM)

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

4.2.5 Output functions – Safe brake control (SBC)

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

5 Management of *functional safety*

5.1 Objective

The first objective of this clause is to specify the responsibilities for the management of *functional safety* and the activities to be carried out by those with assigned responsibilities.

The second objective of this clause is to present the *PDS(SR)* development lifecycle and give an overview of its phases.

NOTE The organizational measures dealt with in this clause provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of *functional safety* of the *PDS(SR)* systems. Separate and distinct from this are the general health and safety measures necessary for the achievement of safety in the workplace.

5.2 Requirements for the management of *functional safety*

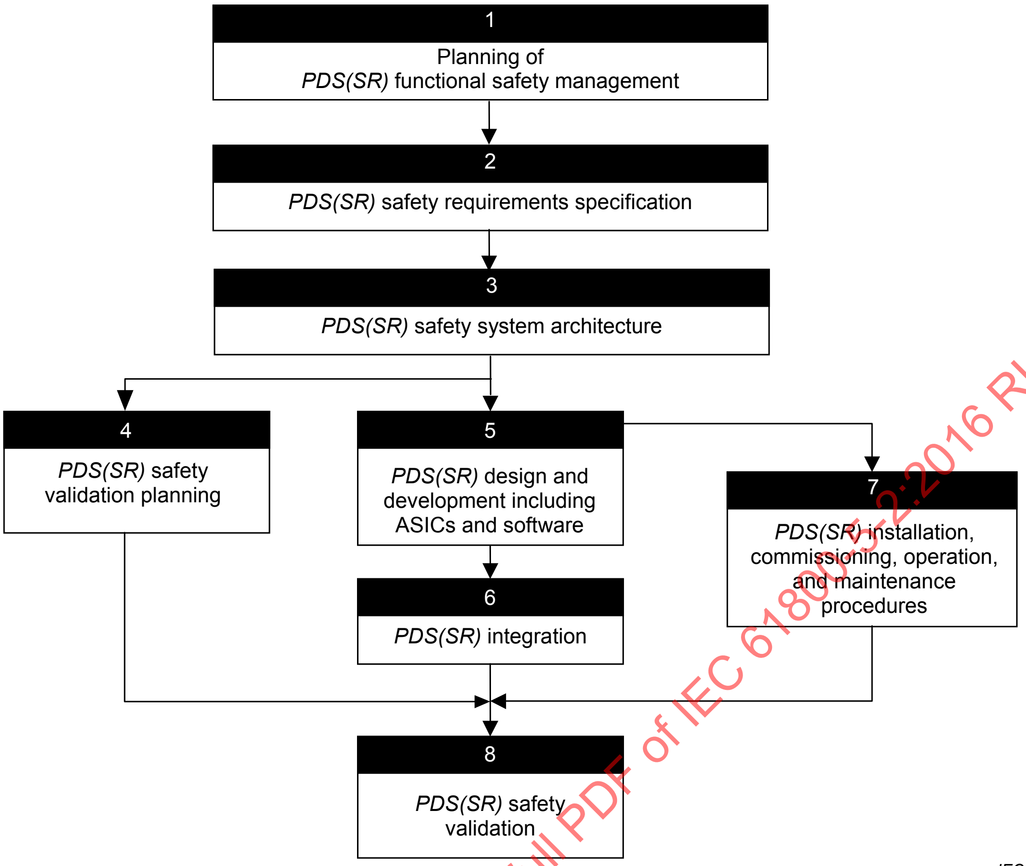
The requirements of Clause 6 of IEC 61508-1:2010 apply.

5.3 *PDS(SR)* development lifecycle

Figure 3 shows the *PDS(SR)* development lifecycle, with cross-references to the relevant sub clauses of this standard, arranged as phase 1 to phase 8.

NOTE This corresponds to the phases, safety requirement specification (phase 9) and realisation (phase 10) of the overall safety lifecycle of IEC 61508-1:2010.

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


1
Planning of PDS(SR) functional safety management
2
PDS(SR) safety requirements specification
3
PDS(SR) safety system architecture
4
PDS(SR) safety validation planning
5
PDS(SR) design and development including ASICs and software
6
PDS(SR) integration
7
PDS(SR) installation, commissioning, operation, and maintenance procedures
8
PDS(SR) safety validation
IEC

For phase 1, see 5.4. (phase 9 – see NOTE)	For phase 2, see 5.5. (phase 9 – see NOTE)	For phase 3, see 5.6. (phase 10.1 – see NOTE)	For phase 4, see 5.4 e) (phase 10.2 – see NOTE)
For phase 5, see Clause 6 (phase 10.3 – see NOTE)	For phase 6, see 6.5 (phase 10.4 – see NOTE)	For phase 7, see Clause 7 (phase 10.5 – see NOTE)	For phase 8, see Clause 8 (phase 10.8 – see NOTE)

NOTE Corresponding phase of overall safety lifecycle of IEC 61508-1:2010.

Figure 3 – *PDS(SR)* development lifecycle

5.4 Planning of *PDS(SR) functional safety* management

A plan shall be generated and updated as necessary throughout the entire development of the *PDS(SR)*. It shall define the activities required to satisfy Clauses 5 to 10, and specify persons and their competence, department(s), or organization(s) responsible for completing these activities.

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

a) Generation of the *safety requirements specification* (see 5.5), including factors such as:

- the personnel responsible for generation and maintenance of the *safety requirements specification*;
- the choice of methods for the avoidance of mistakes during generation of the *safety requirements specification* (see IEC 61508-2:2010, Annex B);
- the consideration of requirements from guidelines and standards for specific target applications of the *PDS(SR)*;
- the personnel responsible for *verification* of the *safety requirements specification*;
- the process for changing the *safety requirements specification* after development has started.

b) Generation of the safety system architecture specification (see 5.6), including factors such as:
   - the personnel responsible for generation and maintenance of the safety system architecture specification;
   - the choice of methods for the avoidance of mistakes during generation of the safety system architecture specification (see IEC 61508-2:2010, Annex B);
   - the consideration of requirements from guidelines and standards for specific target applications of the *PDS(SR)*;
   - the personnel responsible for *verification* of the safety system architecture specification;
   - the process for changing the safety system architecture specification after development has started.

c) Design and development of the *safety sub-function*(s) in the *PDS(SR)*, including (where applicable) factors such as:
   - the personnel responsible for design and development;
   - the selection of product development and project management methodologies (see IEC 61508-7:2010, B.1.1);
   - 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)* (e.g. ISO 13849-1 and IEC 62061);
   - the project documentation methodology (see IEC 61508-7:2010, B.1.2);
   - the application of structured design techniques (see IEC 61508-7:2010, B.3.2);
   - the application of modularization techniques (see IEC 61508-7:2010, B.3.4)
   - the use of computer-based design tools (see IEC 61508-7:2010, B.3.5);
   - the design *verification* methodology;
   - the design change management (both hardware and software).

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

e) A *validation* plan for the *safety sub-function*(s) comprising the following:
   - the personnel responsible for *validation* testing;
   - the identification of the relevant modes of operation of the *PDS(SR)*;
   - the procedures to be applied to validate that each *safety sub-function* of the *PDS(SR)* is correctly implemented, and the pass/fail criteria for accomplishing the tests;
   - the procedures to be applied to validate that each *safety sub-function* of the *PDS(SR)* is of the required *safety integrity*, and the pass/fail criteria for accomplishing the tests;
   - the required environment in which the testing is to take place including all necessary tools and equipment (also plan which tools and equipment should be calibrated);
   - test evaluation procedures (with justifications);
   - the test procedures and performance criteria to be applied to validate the specified electromagnetic immunity limits;
   - the action to be taken in the event of failure to meet any of the acceptance criteria.

f) Planning for safety-related user documentation including:
   - the personnel responsible for user documentation;

- a list of significant safety-related information which shall be provided;
- the review process to insure the accuracy of documentation

g) Where assessment is required (see IEC 61508-1:2010, Clause 8), a *functional safety* assessment plan providing all information necessary to facilitate an effective assessment and including:

- the scope of the *functional safety* assessment;
- the organisations involved;
- the resources required;
- those to perform the *functional safety* assessment;
- the level of independence of those performing the *functional safety* assessment;
- the competence of each person involved in the *functional safety* assessment;
- the outputs from the *functional safety* assessment;
- how the *functional safety* assessment relates to, and shall be integrated with, other *functional safety* assessments where appropriate;
- the requirement to perform an impact analysis to determine which parts of the assessment are to be repeated in case of a modification (see also IEC 61508-1:2010, 7.16.2)

In establishing the scope of each *functional safety* assessment, it will be necessary to specify the documents, and their revision status, that are to be used as inputs for each assessment activity.

NOTE The plan can be made by either those responsible for *functional safety* assessment or those responsible for management of *functional safety*, or can be shared between them.

5.5 Safety requirements specification (*SRS*) for a *PDS(SR)*

5.5.1 General

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

- a *safety sub-functions* requirements specification (see 5.5.2); and
- a *safety integrity* requirements specification (see 5.5.3).

These shall be expressed and structured in such a way that they are:

- clear, precise, unambiguous, feasible, verifiable, testable and maintainable;
- written to aid the comprehension by those who are likely to utilise the information at any stage of the *PDS(SR)* safety lifecycle;
- expressed in natural or formal language and/or logic, sequence or cause and effect diagrams that define the necessary *safety sub-function*s with each *safety sub-function* being individually defined.

For the avoidance of mistakes during the compilation of these specifications, appropriate techniques and measures shall be applied (see IEC 61508-2:2010, Table B.1).

The requirements for safety-related hardware and software shall be reviewed to ensure that they are adequately specified.

5.5.2 *Safety sub-functions* requirements specification

The *safety sub-function*s requirements specification shall provide comprehensive detailed requirements sufficient for the design and development of the *PDS(SR)*.

The *safety sub-function*s requirements specification shall describe, as appropriate:

a) all *safety sub-function*s to be performed;

b) comprehensive detailed requirements sufficient for the design and development of the *PDS(SR)* including all the normative requirements to be fulfilled;

NOTE Requirements like the selected measures of fault avoidance and fault control and the selected measures and techniques for software design and testing etc. can be included in *safety sub-function*s requirement specification.

c) the applicable *mode of operation* regarding *functional safety*;

d) the manner in which the *PDS(SR)* is intended to achieve or maintain a safe state for intended applications;

e) the operating modes of the *PDS(SR)* and its *installation* – for example setting, start-up, maintenance, normal intended operation;

f) all required modes of behaviour of the *PDS(SR)*;

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

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

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

j) 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*);

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

l) 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.

m) 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 function*s);

n) all interfaces, necessary for *functional safety*, between the *PDS(SR)* and any other systems (either directly associated within, or outside, the *installation*).

5.5.3 *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-related functions), *SIL capability* (or *SIL*) and an upper limit of *PFH* value.

NOTE 1 *SIL capability* is relevant if the *PDS(SR)* is to be considered as a component which implements a *safety sub-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 be lower than the target failure measure associated with the *SIL* allocated to the complete *safety sub-function*. However, it can also be higher, if the *PDS(SR)* is to be used to implement the *safety sub-function* in a redundant configuration with other components.

NOTE 3 Where a *PDS(SR)* implements a *safety sub-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 sub-function*, and the *safety sub-function*s are used simultaneously, the probability of dangerous random hardware failure of the common hardware can 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 sub-function* is required for more than one axis, the probability of dangerous random hardware failure of common hardware can be considered only once when determining the overall probability of dangerous random hardware failure.

b) the required *mission time*;

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

NOTE 6 This information can 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.

d) any requirement for increased EM immunity (see 6.2.6);

e) limiting and constraint conditions for the realisation of *PDS(SR)* due to the possibility of *common cause failure*s;

f) the quality assurance/quality control measures necessary for management of functional safety (see IEC 61508-1:2010, Clause 6).

5.6 *PDS(SR)* safety system architecture specification

5.6.1 General

5.6.1.1 The objective of the safety system architecture specification is to specify the architectural decomposition of the *PDS(SR)* and the requirements for the resulting *subsystems* and parts of *subsystems* (see Annex A).

NOTE 1 The Safety system architecture specification is normally derived from the *PDS(SR)* safety requirement specification by decomposing the *safety sub-function*s and allocating parts of the *safety sub-function*s to *subsystems* (for example *safety sub-function* logic, input/output circuitry, power supply, software). The representation of the *PDS(SR)* in form of *subsystems* describes the *PDS(SR)* on an architectural level which allows the specification of the requirements for these *subsystems*. The requirements can be included in the safety system architecture specification or kept separate and referenced by the safety system architecture specification. The *subsystems* can be further decomposed to parts to satisfy the design and development requirements.

NOTE 2 A more general approach to this kind of specification is given in IEC 61508-2:2010 as an E/E/PE system design requirement specification.

5.6.1.2 The description of the *subsystems* and parts and the respective requirements shall be expressed and structured in such a way that they are:

- clear, precise, unambiguous, feasible, verifiable, testable and maintainable;
- written to aid the comprehension by those who are likely to utilise the information at any stage of the *PDS(SR)* safety lifecycle;
- traceable to the *PDS(SR) safety requirements specification*.

5.6.2 Requirements for safety system architecture specification

5.6.2.1 The safety system architecture specification shall contain design requirements related to *safety sub-functions* and to *safety integrity*.

5.6.2.2 The safety system architecture specification shall contain details of all hardware and software necessary to implement the required *safety sub-functions*, as specified by the *safety sub-functions requirements specification* of the *PDS(SR)* (see 5.5.2). The architecture shall include, for each *safety sub-function*:

a) requirements for the *subsystem*s and parts as appropriate;

b) requirements for the integration of the *subsystem*s and parts to meet the *PDS(SR)* safety requirement specification;

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

d) accuracy and stability requirements for measurements and controls;

e) safety-related *PDS(SR)* and operator interfaces;

f) interfaces between the *PDS(SR)* and any other systems (either within, or outside, the *installation*);

g) all modes of behaviour of the *PDS(SR)*, in particular, failure behaviour and the required response (for example alarms, automatic shut-down) of the *PDS(SR)*;

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

i) any limiting and constraint conditions for the *PDS(SR)* and its associated subsystems, for example timing constraints or constraints due to the possibility of *common cause failure*s;

j) any specific requirements related to the procedures for starting-up and restarting the *PDS(SR)*.

5.6.2.3 The safety system architecture specification shall contain details, relevant to the design, to achieve the *safety integrity level* for the *safety sub-function*, as specified by the *PDS(SR) safety integrity* requirements specification (see 5.5.3), including:

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

b) all relevant reliability modelling parameters such as the required *diagnostic test* interval of the hardware necessary to achieve the target failure measure;

5.6.2.4 The *PDS(SR)* safety system architecture specification shall be completed in detail as the design progresses and updated as necessary after modification.

5.6.2.5 For the avoidance of mistakes during the development of the specification for the *PDS(SR)* safety system architecture specification, an appropriate group of techniques and measures according to IEC 61508-2:2010, Table B.2 shall be used.

5.6.2.6 The implications imposed on the architecture by the *PDS(SR)* safety system architecture specification shall be considered.

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

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 *hazard*ous 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 cannot 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 other applicable parts of the IEC 61800 series, listed in the normative references.

6.1.3 Realisation

The *PDS(SR)* shall be realised in accordance with its *safety requirements specification* (see 5.5).

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 6.2.3), and

– the requirements for the *PFH* value (see 6.2.2 or 6.2.3);

b) the requirements for *systematic safety integrity* comprising:

- the requirements for the avoidance of failures (see 6.2.5.1), and the requirements for the control of systematic faults (see 6.2.5.2), or
- evidence that components used are 'proven-in-use'. In this case the components shall fulfil the relevant requirements of IEC 61508-2:2010

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

NOTE If PL and category are to be claimed refer to ISO 13849-1:2006, 6.2 additionally.

6.1.5 Safety and non-*safety sub-functions*

Where a *PDS(SR)* is to perform both safety and non-*safety sub-function*s, then all of its hardware and software shall be treated as safety-related, unless adequate design measures ensure that the failures of non-*safety sub-functions* cannot adversely affect *safety sub-functions*.

See IEC 61508-3:2010, Annex F, for techniques for achieving non-interference between software parts on a single computer.

6.1.6 *SIL* for multiple *safety sub-function*s within one *PDS(SR)*

The *safety integrity level* of one *safety sub-function* can be different from the others, and the requirements for design of each *safety sub-function* are defined as follows.

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

As an example see Table 2:

Table 2 – Example for determining the *SIL* from hardware and software independence

***PDS(SR)* implementing two *safety sub-function*s (Y and Z) with different *SIL* requirements: Function Z: *SIL* H[a] / function Y: *SIL* L[a]**				
Design type	**Evidence of sufficient independence between *safety sub-functions* Y and Z**		**Final *SIL* requirement for *safety sub-function***	
	for hardware	**for software**	**Z**	**Y**
Hardware (HW) **and** software (SW) design	Yes	Yes	*SIL* H	*SIL* L
	No	Yes	SW: *SIL* H HW: *SIL* H	SW: *SIL* L HW: *SIL* H [b]
		No	*SIL* H	*SIL* H
	Yes	No	SW: *SIL* H HW: *SIL* H	SW: *SIL* H [b] HW: *SIL* L
Hardware **only** design	Yes	not applicable	*SIL* H	*SIL* L
	No		*SIL* H	*SIL* H [b]

[a] with *SIL* H higher than *SIL* L

[b] HW and/or SW separation is not sufficient

Sufficient independence shall be established by showing that the probability of a dependent failure between the parts implementing *safety sub-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 sub-functions* involved.

6.1.7 Integrated circuits with on-chip redundancy

Digital ICs which implement on-chip redundancy with the goal of increasing fault tolerance in a *PDS(SR)* shall satisfy all of the special requirements for ICs with on-chip redundancy according to IEC 61508-2:2010, Annex E, in case of duplicated circuitry. Alternatively a justification shall be given that the same level of independence between different channels is achieved by applying a different set of measures.

6.1.8 Software requirements

If software is used to implement a *safety sub-function* of the *PDS(SR)* with a specific *SIL* or *SIL capability* (see 5.5.3), then this software shall be implemented in accordance with the requirements defined by IEC 61508-3:2010 for that specific *SIL*.

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* capability (for example failure mode and effects analysis, fault tree analysis).

6.2 *PDS(SR)* design requirements

6.2.1 Basic and well-tried safety principles

Basic and well-tried safety principles shall be considered where applicable when a category is claimed for the *PDS(SR)*.

- For electrical and electro-mechanical *PDS(SR)*, these principles correspond to ISO 13849-2:2012, Table D.1 and Table D.2
- For mechanical parts (e.g. encoders), these principles correspond to ISO 13849-2:2012, Table A.1 and Table A.2

6.2.2 Requirements for the estimation of the probability of dangerous random hardware failures per hour (*PFH*)

6.2.2.1 General requirements

6.2.2.1.1 *PFH* for each *safety sub-function*

The *PFH* of each *safety sub-function* (or group of simultaneously activated *safety sub-functions*) to be performed by the *PDS(SR)*, estimated according to 6.2.2.1.2 and Annex B, shall be equal to or less than the target failure measure (see Table 3) as specified in the *safety integrity* requirements specification (see 5.5.3).

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

The target failure measure, expressed in terms of the *PFH*, is determined by the *SIL* of the *safety sub-function* (see IEC 61508-1:2010, Table 3), unless there is a requirement in the *PDS(SR) safety integrity* requirements specification (see 5.5.3) for the *safety sub-function* to meet a specific target failure measure, rather than a specific *SIL*.

Table 3 – *Safety integrity levels*: target failure measures for a *PDS(SR) safety sub-function*

Safety integrity level SIL	***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 failure*s, or *dangerous failure* rate, in units of *dangerous failures* per hour.	

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

NOTE 1 Different *safety sub-functions* can have common components and/or unique components, resulting in different *PFH* for each *safety sub-function* (or group of simultaneously used *safety sub-functions*).

NOTE 2 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);
- parts count (see IEC 61709:2011);
- procedure description (see IEC 61508-6:2010);
- simplified procedure for estimating PL (see ISO 13849-1:2006, 4.5.4).

See also IEC 60300-3-1.

NOTE 3 The mean time to restoration (see IEC 60050, 192-07-23) that is considered in the reliability model will need to take into account the diagnostic intervals, the repair time and any other delays prior to restoration, and the *mission time*.

NOTE 4 Failures due to common cause effects and data communication processes can 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 IEC 61508-6:2000, Annex D).

NOTE 5 If PL is to be claimed refer to ISO 13849-1:2006, Table 3, additionally.

6.2.2.1.2 Estimation of *PFH*

The *PFH* of each *safety sub-function* (or group of simultaneously activated *safety sub-functions*) to be performed by the *PDS(SR)*, due to random hardware failures shall be estimated using IEC 61508-2:2010, Annex A, taking into account:

a) the architecture of the *PDS(SR)* as it relates to each *safety sub-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 failure*s (see IEC 61508-6:2010, Annex D);

e) the *diagnostic coverage* (DC) of the *diagnostic tests* (determined according to IEC 61508-2:2010, Annex A and Annex C) and the associated *diagnostic test* interval, and 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 repair times for detected failures;

NOTE 1 The repair time will constitute one part of the mean time to restoration (see IEC 60050-192:2015, 192-07-23), 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 61508-6:2010 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 equipment or machinery driven by the *PDS(SR)* 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.

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

NOTE 2 For information about estimation of the PFD_{avg} value from the *PFH* value for low demand applications, see Annex F.

6.2.2.1.3 Failure rate data

Component failure rate data shall be obtained from:

– a recognised source; or

– estimate based upon those Type A components that are considered to be "proven in use" (see IEC 61508-2:2010, 7.4.10).

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

If site-specific failure data are available, then this is preferred. If this is not the case, then generic data can be used.

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

NOTE 2 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 can 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).

NOTE 3 The fault lists given in Annex D can be used to assist in determination of failure modes.

Any failure rate data used shall have a confidence level of at least 70 %.

6.2.2.1.4 *Diagnostic test* interval when the hardware fault tolerance is greater than zero

The *diagnostic test* interval of any *subsystem* of the *PDS(SR)* shall be appropriate to meet the required *PFH* (see 6.2.2.1.1).

NOTE 1 For information regarding mathematical impact of diagnostic test interval see Clause B.4

NOTE 2 For redundant parts of a *PDS(SR)* which cannot be tested without disrupting the application in which the *PDS(SR)* is used (machine or plant) and where no justifiable technical solution can be implemented, the following maximum diagnostic test intervals can be considered as acceptable:

– one test per year for *SIL* 2, PL d / category 3;

– one test per three months for *SIL* 3, PL e / category 3;

– one test per day for *SIL* 3, PL e / category 4.

PL and category according to ISO 13849-1.

6.2.2.1.5 Diagnostic test interval when the hardware fault tolerance is zero

The *diagnostic test* interval of any *subsystem* of a *PDS(SR)* having a hardware fault tolerance of zero, on which a *safety sub-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 process safety time.

6.2.3 Architectural constraints

6.2.3.1 Limitations of *SIL*

In the context of hardware *safety integrity*, the highest *safety integrity level* that can be claimed for a *safety sub-function* is limited by the hardware fault tolerance and *safe failure* fraction of the *subsystem*s of a *PDS(SR)* that carry out that *safety sub-function*. A hardware fault tolerance of *N* means that *N*+1 faults could cause a loss of the *safety sub-function*. Table 4 and Table 5 specify the highest *safety integrity level* that can be claimed for a *safety sub-function* which uses a *subsystem*, taking into account the hardware fault tolerance and *safe failure* fraction of that *subsystem* (see IEC 61508-2:2010, Annex C). The requirements of Table 4 or Table 5, whichever is appropriate, shall be applied to each *subsystem* carrying out a *safety sub-function* and hence every part of the *PDS(SR)*; 6.2.3.2.2 and 6.2.3.2.3 specify which one of Table 4 or Table 5 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 Clause D.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 can 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 fault tolerance requirements can 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 clause is based on route 1_H of IEC 61508-2:2010, 7.4.4; for the requirements related to route 2_H see IEC 61508-2:2010, 7.4.4.3.

6.2.3.2 Type A and Type B *subsystems*

6.2.3.2.1 General

(See also IEC 61508-2:2010; 7.4.4.1.2 and 7.4.4.1.3)

6.2.3.2.2 Type A

A *subsystem* can be regarded as type A if, for the components required to achieve the *safety sub-function*, the following criteria are satisfied:

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 can be considered.

6.2.3.2.3 Type B

A *subsystem* shall be regarded as type B if, for the components required to achieve the *safety sub-function*, one or more of the criteria of 6.2.3.2.2 are not satisfied. 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* shall be regarded as type B rather than type A.

NOTE 1 For example, the control section consisting of microcontrollers etc. is considered as a type B *subsystem*.

NOTE 2 Clause D.3 lists faults and fault exclusions that can be considered.

6.2.3.3 Architectural constraints

The architectural constraints of either Table 4 or Table 5 shall apply: Table 4 applies for every type A *subsystem* forming part of the *PDS(SR)*; Table 5 applies for every type B *subsystem* forming part of the *PDS(SR)*.

NOTE For information about type A and type B refer to IEC 61508-2:2010, 7.4.4.1.2 and 7.4.4.1.3

Table 4 – Maximum allowable safety integrity level for a *safety sub-function* carried out by a type A safety-related *subsystem*

***Safe failure* fraction** [a]	**Hardware fault tolerance *N* (see 6.2.3.1)**		
	0	**1**	**2**
< 60 %	*SIL* 1	*SIL* 2	*SIL* 3
60 % to < 90 %	*SIL* 2	*SIL* 3	*SIL* 3
90 % to < 99 %	*SIL* 3	*SIL* 3	*SIL* 3
≥ 99 %	*SIL* 3	*SIL* 3	*SIL* 3

[a] See 6.2.4 for details of how to estimate *safe failure* fraction.

Table 5 – Maximum allowable safety integrity level for a *safety sub-function* carried out by a type B safety-related *subsystem*

***Safe failure* fraction** [a]	**Hardware fault tolerance *N* (see 6.2.3.1)**		
	0	**1**	**2**
< 60 %	Not permitted	*SIL* 1	*SIL* 2
60 % to < 90 %	*SIL* 1	*SIL* 2	*SIL* 3
90 % to < 99%	*SIL* 2	*SIL* 3	*SIL* 3
≥ 99 %	*SIL* 3	*SIL* 3	*SIL* 3

[a] See 6.2.4 for details of how to estimate *safe failure* fraction.

Exception:

For a *subsystem* with a hardware fault tolerance of zero and where fault exclusions have been applied to faults of electrical or electronic parts that could lead to a *dangerous failure*, then the maximum *SIL* that can be claimed due to architectural constraints of that *subsystem* is limited to:

- *SIL* 3, if tables D.1, D.3, D.5, D.6, D.7 and D.8 apply
- *SIL* 2 in all other cases.

NOTE If category is to be claimed refer to ISO 13849-1:2006, 6.2 additionally.

6.2.4 Estimation of *safe failure fraction (SFF)*

6.2.4.1 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).

For calculation of *SFF* see IEC 61508-2:2010, Annex A and Annex C

For *PDS(SR)* the route 1_H is preferred. Route 2_H shall be restricted for *PDS(SR)* to Type A *subsystem*s.

NOTE This clause is based on route 1_H of IEC 61508-2:2010, 7.4.4.2; for the requirements related to route 2_H see IEC 61508-2:2010, 7.4.4.3.

Basis of data is given in 6.2.2.1.3.

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

6.2.5 Requirements for *systematic safety integrity* of a *PDS(SR)* and *PDS(SR) subsystems*

6.2.5.1 Requirements for the avoidance of failures

6.2.5.1.1 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)* according to IEC 61508-2:2010, table B.2.

Tests, as planned according to 6.2.5.1.4, shall be performed. See also Clause 9.

NOTE For claiming a PL refer to ISO 13849-1:2006, Annex G.

6.2.5.1.2 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*.

6.2.5.1.3 Design measures

The following design measures shall be applied.

a) Proper design of the *PDS(SR)* and/or *subsystem*s 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 *subsystem*s, for example cabling, wiring and any interconnections;
- the use of reviews and inspections for early detection of design defects.

b) Compatibility:

- use *subsystem*s 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.

6.2.5.1.4 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 7.2).

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.

6.2.5.1.5 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.

6.2.5.2 Requirements for the control of systematic faults

6.2.5.2.1 General

NOTE For claiming a PL refer to ISO 13849-1:2006, Annex G.

6.2.5.2.2 Design features

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

a) residual design faults in the hardware;
b) environmental stresses according IEC 61800-2:2015, Table 6 as applicable for the environment specified for the *PDS(SR)*;
c) electromagnetic disturbances, see 6.2.6;
d) mistakes made by the operator of the *PDS(SR)* (see IEC 61508-2:2010, Clause A.3 and Table A.17);
e) residual design faults in the software (see IEC 61508-3:2010, 7.4.3 and associated table);
f) errors and other effects arising from any data communication process (see 6.4).

When application specific integrated circuits (ASICs) are used to implement *safety sub-functions* in a *PDS(SR)*, an appropriate group of techniques and measures that are essential to prevent the introduction of faults during the design and development shall be used. The informative Annex F of IEC 61508-2:2010, provides an example of techniques and measures. The related ASIC development lifecycle is shown in IEC 61508-2:2010, Figure 3.

6.2.5.2.3 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)*.

6.2.5.2.4 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.

6.2.5.2.5 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 IEC 61508-7:2010, B.4.8.

6.2.5.2.6 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 sub-function*s of the *PDS(SR)*) via plausibility checks.

NOTE See IEC 61508-7:2010, B.4.6 and B.4.9.

6.2.5.2.7 *PDS(SR)* parameterization

Almost all *PDS(SR)* need configuration parameters which determine the behaviour of *safety sub-function*s. The software-based parameterization shall be considered as a safety-related aspect of the *PDS(SR)* design to be described in the software *safety requirements specification*.

Parameterization during act of installing and maintenance shall be carried out using a dedicated parameterization tool provided by the supplier of the *PDS(SR)*. This tool shall have its own identification (name, version, etc.) and shall prevent unauthorized modification, for example, by use of a password. There are no *functional safety* requirements to be fulfilled by this parameterization tool.

A special procedure shall be used for setting the safety-related parameters. This procedure shall include confirmation of input parameters to the *PDS(SR)* by

– retrieval, display and check by operator of the modified parameters and
– a *verification* of the correctness of the parameters in the *PDS(SR)* by
  - a configuration test (see 7.2f) or
  - other suitable means defined by the *PDS(SR)* manufacturer

as well as subsequent documented confirmation of the safety-related parameters, e.g. by a suitably skilled person and by means of an automatic check by a parameterization tool.

NOTE 1 For reference, see IEC 61508-3:2010, 7.4.4.

NOTE 2 This is of particular importance where parameterization is carried out using a device not specifically intended for the purpose (e.g. personal computer or equivalent).

NOTE 3 For more details on software-based parameterization see ISO 13849-1:2006, 4.6.4. and/or IEC 62061:2012, 6.11.2.

6.2.5.2.8 Loss of electrical supply

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

6.2.6 Design requirements for electromagnetic (EM) immunity of a *PDS(SR)*

The *PDS(SR)* shall be designed to have the appropriate EM immunity for operating within the specified or anticipated electromagnetic environment (first environment or second environment) as classified in IEC 61800-3.

The EM immunity test requirements are described in 9.2 and Annex E.

6.2.7 Design requirements for thermal immunity of a *PDS(SR)*

The *PDS(SR)* shall be designed to have the appropriate thermal immunity for operating within the specified or anticipated thermal environment as classified in IEC 61800-2.

The thermal immunity test requirements are described in 9.4.

6.2.8 Design requirements for mechanical immunity of a *PDS(SR)*

The *PDS(SR)* shall be designed to have the appropriate mechanical immunity for operating within the specified or anticipated mechanical environment as classified in IEC 61800-5-1 and IEC 61800-2.

The mechanical immunity test requirements are described in 9.5.

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 sub-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 sub-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 sub-function* within a *PDS(SR)* then the probability of undetected failure of the communication process shall be estimated. This probability shall be taken into account when estimating the *PFH* of the *safety sub-function* due to random failures (see 6.2.2.1.2). This does not cover all data communication within a *PDS(SR)*. For example data communication within one printed wiring board is not covered by this requirement.

For details see IEC 61508-2:2010, 7.4.11.

NOTE Additional information regarding safety communication channels can be found in IEC 61784-3.

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 *subsystem*s 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.

6.5.2 Software integration

The integration of safety-related software part/module into the *PDS(SR)* shall be carried out according to IEC 61508-3:2010. 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 IEC 61508-7:2010, B.5.2) can suffice. Static analysis (see IEC 61508-7:2010, B.6.4), dynamic analysis (see IEC 61508-7:2010, B.6.5) or failure analysis (see IEC 61508-7:2010, B.6.6) can 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 sub-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 General

PDS(SR) manufacturers shall provide information for the users in a safety manual. General requirements of the safety manual are referred to IEC 61508-2:2010, Annex D, and IEC 61508-3:2010, Annex D. This clause describes additional requirements for a *PDS(SR)*.

NOTE For claiming a PL refer to ISO 13849-1:2006, Clause 11.

7.2 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 *safety sub-function* and interface which is available for use in the implementation of *safety sub-function*s. This shall comprise:

- a detailed description of the *safety sub-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 function*s;
- the condition(s) (for example, operating mode) in which the *safety sub-function* is intended to be active or disabled;
- the priority of those *safety sub-function* that are simultaneously active and can conflict with each other.

b) The *safety integrity* information for each *safety sub-function*, including:

- the *SIL* or *SIL* capability; (includes systematic capability, see IEC61508-2);
- the PFH value for each *safety sub-function*;
- resulting PFH-value for a group of simultaneously activated *safety sub-function*s;
- PL and category according to ISO 13849-1 when applicable.

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, IEC 61800-2, IEC 61800-3, IEC 61800-4 and IEC 61800-5-1). This shall take into account storage, transport, act of installing, commissioning, testing, operation and maintenance.

NOTE As an example for an EMC related information for use: “Warning: handheld radio transmitters held closer than 20 cm to *PDS(SR)* can disturb the *safety sub-function*s of the *PDS(SR)*” or similar (see E.2, footnote p)

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)*;
- any testing, calibration or maintenance requirements (e.g. limited number of operations of a relay);
- any limits on the application of the *PDS(SR)* which should be observed in order to avoid *systematic failure*s;
- any information valid hardware and software versions and the combinations permitted for the *safety sub-functions;* the fact that *safety sub-function*s cannot prevent any failure of non-*safety sub-function*s of the *PDS(SR).*

NOTE 1 For example, the failure of deceleration initiated by SS1-t is not prevented.

NOTE 2 For example, while function STO is active, a limited amount of movement is still possible in the event of failure in the power section of the *PDS(SR).*

e) The act of installing and commissioning guidance (see IEC 61800-5-1:2007, Clause 6), including setting and parameterisation.

f) The requirements for configuration test of *safety sub-function*s, in cases where the integrity of the means of configuration of a *safety sub-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 sub-function*s 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 sub-function*s that will be used in the application of the *PDS(SR)*;

   – the results of each test of these *safety sub-function*s, 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 sub-function*s 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;

   – the routine actions which need to be carried out to maintain the *functional safety* of the application of the *PDS(SR)*, including the compatibility of hardware and software versions and safety parameters such as *PFH* and *SIL*

   NOTE The *PDS(SR)* operation and maintenance procedures can 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 *PDS(SR)* development lifecycle (see 5.3).

NOTE If PL is to be claimed refer to ISO 13849-1 and/or ISO 13849-2.

8.2 *Verification*

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

The requirements of IEC 61508-2:2010, 7.9.2 apply.

8.3 *Validation*

The objective of the requirements of this subclause is to validate that the *PDS(SR)* meets in all respects the requirements for safety in terms of the required *safety sub-functions* and *safety integrity*.

The requirements of IEC 61508-2:2010, 7.7.2 apply.

8.4 Documentation

Appropriate documentation concerning *PDS(SR) verification* and *validation* shall be produced, according to the appropriate requirements of 8.2 and 8.3.

9 Test requirements

9.1 Planning of tests

Testing of the *safety sub-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 sub-function*;

b) the functional testing of each diagnostic function for each *safety sub-function*; (fault insertion testing);

c) the environmental testing of each *safety sub-function* for immunity to each of the following environmental stresses:

   1) electromagnetic (EM)

   2) thermal

   3) mechanical (shock & vibration)

d) the acceptance criteria.

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

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

NOTE When it is difficult to perform *safety sub-function* tests on the complete *PDS(SR)* because of e.g. size, parts of the *PDS(SR)* that are considered to be safety-relevant can be tested individually.

9.2 Functional testing

Functional testing of each *safety sub-function*, including related diagnostics (fault insertion testing), shall be performed.

9.3 Electromagnetic (EM) immunity testing

9.3.1 General

The performance criterion that shall be applied when performing EM immunity tests on the *PDS(SR)* is specified in 9.3.3. This criterion does not apply to the normal (non-safety related) functions of the equipment.

NOTE Functional electromagnetic compatibility (EMC) of the *PDS(SR)* is achieved when it complies with the requirements of IEC 61800-3.

9.3.2 Intended EM environment

Where the EM environment is not known or not declared by the *PDS(SR)* manufacturer or the intended environment is the second environment, the *PDS(SR)* shall be verified to the immunity requirements given in the second environment columns of Tables E.1, E.2 and E.3.

When the environment of the intended use of the *PDS(SR)* is the first environment, the *PDS(SR)* shall be verified to the immunity requirements given in the first environment columns of Tables E.1 and E.3.

The performance criterion of 9.3.3 shall be applied.

The specified mitigation measures shall be in place during the tests to verify their effectiveness.

9.3.3 Performance criterion (fail safe state – FS)

The following performance criterion shall be satisfied while the *PDS(SR)* exercises all safety-related hardware parts during the tests. The behaviour of non-safety related functions of the *PDS(SR)* are not considered, unless non-safety related components are used as indicators of the *safety sub-functions* and have been verified to be operating properly.

Additionally no hazards shall be introduced by the *PDS(SR)* when the EM immunity tests are applied.

Safety sub-functions of the *PDS(SR)*:

- do not deviate outside their specified limits for *functional safety* (equal to criterion A of IEC 61800-3), 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 (fail safe state) of the *PDS(SR)* is maintained or achieved within the specified maximum fault reaction time.

Permanent degradation of the *safety sub-function* or destruction of components is permitted provided a defined safe state shall be 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.

9.4 Thermal immunity testing

9.4.1 General

Thermal immunity testing of each *safety sub-function*, including related diagnostics, shall be performed.

9.4.2 Functional thermal test

The test shall be performed according to the temperature rise test of IEC 61800-5-1:2007 to determine that each *safety sub-function* of the *PDS(SR)* works properly under the rated temperature operating conditions.

9.4.3 Component thermal test

For all components of each *safety sub-function*, the component manufacturer's specified maximum operating temperature shall not be exceeded during the test.

NOTE 1 Testing whether all safety-related components are operated in the specified temperature range when the *PDS(SR)* is applied to its specified minimum and maximum ambient temperatures can be performed at a lower temperature than the rated maximum ambient air temperature of the *PDS(SR)*. The maximum temperatures attained during testing can be corrected to the maximum rated ambient temperature for the *PDS(SR)* by adding the difference between the ambient temperature during the test and the maximum rated ambient temperature for the *PDS(SR)*.

NOTE 2 IEC 61800-5-1 provides information regarding thermal test methods.

9.5 Mechanical immunity testing

9.5.1 General

Shock and vibration immunity testing of each *safety sub-function*, including related diagnostics, shall be performed.

9.5.2 Vibration test

Testing shall be performed according to the test conditions of the vibration test of IEC 61800-5-1:2007, except that the *PDS(SR)* shall be powered and each *safety sub-function* shall be verified while operating.

9.5.3 Shock test

Testing shall be performed according to the test conditions of the shock test of IEC 61800-2:2015, except that the *PDS(SR)* shall be powered and each *safety sub-function* shall be verified while operating.

9.5.4 Performance criterion for mechanical immunity tests (fail safe state – FS)

Safety sub-functions of the *PDS(SR)*:

- 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 mechanical disturbance in such a way that a defined safe state (fail safe state) of the *PDS(SR)* is maintained or achieved within the specified maximum fault reaction time.

9.6 Test documentation

During *PDS(SR)* testing for *safety sub-function*s, the following details shall be documented:

a) the version of the test plan used;

b) the criteria for acceptance of tests;

c) the model 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 pass/fail status of the test. If the test has failed, the mode of failure shall be documented.

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

10.2.1 General

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.

10.2.2 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 modification;

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

NOTE For the selection of appropriate techniques to implement the requirements for software modifications, see IEC 61508-3:2010, Table A.8.

10.2.3 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 performed.

10.2.4 Authorization

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

10.2.5 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 modifications;

d) the test cases for components including re*validation* data;

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

f) the deviation from previous operations and conditions;

g) the necessary modifications 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 in Table A.1 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 “architecture“ 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 can be established at the start of the design procedure.

Table A.1 – Design and development procedure for *PDS(SR)*

	Tasks	References
1	**General requirements**	
	All relevant documents should be under the control of an appropriate document control scheme Software quality management system **Safety Concept:** a) Hardware design on an architectural level, including – Block diagrams of safety related hardware – User and process interfaces – Safety relevant signal paths – Power supply – Separation of independent channels to achieve fault tolerance – Communication links between independent channels to achieve diagnostic coverage b) Software design on an architectural level, including: – description of the functions provided by the safety related software – interaction with hardware – state machine diagrams of the intended behaviour of the software – user and process interfaces – fault detection possibilities and fault reactions – overview of software structure, for example with block diagram – control and storage of safety related data – version procedures – used tools, for example compiler, code checker, etc.	IEC 61508-1:2010, Clause 5 IEC 61508-3:2010, Clause 6 Phase 3 of *PDS(SR)* safety lifecycle (see 4.2 of this standard) a) See Clause 5 of this standard IEC 61508-2:2000, 7.4, Annex A, Tables B.2, B.6 Examples in IEC 61508-6:2000, Annexes A and D b) IEC 61508-2:2000, 7.2.3.1(h) IEC 61508-3:2010, 7.2.2.8, 7.2.2.10, 7.4.2, 7.4.3, Tables A.2, B.1, B.7, B.9 IEC 61508-7:2000, Table C.1

	Tasks	References
2	**Planning of *PDS(SR) functional safety* management**	Phase 1 of *PDS (SR)* safety lifecycle (see 5.3 and 5.4 of this standard)
	Generation of a plan which defines the activities required to satisfy Clauses 5 to 10 of this standard and identifies persons, department(s), or organization(s) responsible for completing these activities. “Plan shall be updated as necessary throughout the entire development of the *PDS(SR)*”	See 5.4 of this standard IEC 61508-1:2010, 6.2 IEC 61508-3:2010, 6.2
3	**Specification of *PDS(SR)* safety requirements**	Phase 2 of *PDS(SR)* safety lifecycle (see 5.3 and 5.5 of this standard)
	Development of a *safety requirements specification* (*SRS*) including *safety sub-function*s requirements and *safety integrity* requirements	See 5.5 of this standard IEC 61508-1:2010, 7.5, 7.10 IEC 61508-2:2010, 7.2, Tables B.1, B.6 IEC 61508-2:2010, 7.4.6 to 7.4.8, Annex A IEC 61508-3:2010, 7.2,Tables A.1, B.7 IEC 61508-3:2010, 7.4.2 to 7.4.4, Tables A.3, B.1 IEC 61508-7:2010, Table C.1 IEC 61508-6:2010, Annex A Examples in IEC 61508-5:2010
4	***Verification* of *PDS(SR) safety requirements specification***	
	a) Reviews of the *safety requirements specification* b) Check by an independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:2010 and IEC 61508-3:2010, 7.9
5	**Safety system architecture specification for a *PDS(SR)***	Phase 3 of *PDS(SR)* safety lifecycle (see 5.3 and 5.6 of this standard)
	a) Details of hardware and software necessary to implement *safety sub-functions* specified by the *SRS*. For each *safety sub-function*, the architecture should also include: • requirements for *subsystems* and parts of *subsystems* as appropriate; • requirements for the integration of the *subsystems* and parts to satisfy the *SRS;* • throughput performance that enables response time requirements to be met; • accuracy and stability requirements for measurements and controls; • safety-related operator interfaces; • other items specified in 5.6.2.2.	a) See 5.6 of this standard IEC 61508-2:2010, 7.4, Annex A IEC 61508-3:2010, 7.4.2, 7.4.3 Examples in IEC 61508-6:2010, Annexes A and D
	b) Details of how the design will achieve the *safety integrity level* and required target failure measure for the *safety sub-function* including: • architecture of each *subsystem* required to meet architectural constraints on hardware *safety integrity;* • relevant reliability modelling parameters such as required *diagnostic test* interval of all hardware components necessary to achieve the target failure measure; • actions taken in the event of a detected *dangerous failure;* • how the safety-related hardware will achieve immunity to all required environmental conditions, including EM, over the entire safety lifecycle; • QA/QC measures necessary for safety management.	b) IEC 61508-2:2010, 7.4, Tables 2, 3, Annexes A, C IEC 61508-3:2010, 7.2.2.8, 7.2.2.10, 7.4.2, 7.4.3, Tables A.2, B.1, B.7, B.9 IEC 61508-6:2010, Clause A.2 IEC 61508-7:2010, Table C.1

	Tasks	References
	c) **Recommendation** Pre-estimation of the probability of failure of *safety sub-function*s due to random hardware failures on a level of functional block diagrams	c) IEC 61508-1:2010, Table 2 IEC 61508-2:2010, 7.4.4, Tables 3, A.1, Annex C IEC 61508-3:2010, Clause 8, Table A.10, B.4 (FMEA) Examples in IEC 61508-6:2010, Annexes C and D
6	***Verification*** **of safety system architecture specification**	
	a) Reviews of system architecture b) Check by independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:2010 and IEC 61508-3:2010, 7.9
7	***Validation*** **planning**	Phase 4 of *PDS(SR)* safety lifecycle (see 5.4 d) of this standard)
	a) Detailed planning of the *validation* of safety related *PDS(SR)*. b) The *validation* plan should be generated in parallel to Phase 9.3 Design and Development.	a) See 8.3 of this standard b) IEC 61508-2:2010, 7.3, Table B.5 IEC 61508-3:2010, 7.3, Tables A.7, B.3, B.5
8	***Verification*** **of** ***validation*** **plan**	
	a) Reviews of the *validation* plan b) Check by independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:2010 and IEC 61508-3:2010, 7.9
9	**Design and development**	Phase 5 of *PDS(SR)* safety lifecycle (see 5.3 of this standard)
	a) Hardware design b) Software design c) Reliability prediction (calculation of the probability of failure of *safety sub-function*s due to random hardware failures) including: • type of *PDS(SR)* • SFF • functional block diagram • reliability model • data base of the model (device lists) • *PFH* estimation • *mission time* • repair interval	See Clause 6 of this standard a) IEC 61508-2:2010, 7.4, Annex A, Tables B.2, B.3, B.6 b) IEC 61508-3:2010, 7.4.5, 7.4.6, Table A.4 c) IEC 61508-1:2010, Table 2 IEC 61508-2:2010, 7.4.3, 7.4.9, Tables 3, A.1, Annex C IEC 61508-3:2010, Table B.4 (FMEA) Examples in IEC 61508-6:2010, Annexes C and D
10	***Verification*** **of the design**	
	a) Reviews of the system design b) Functional tests on module level c) Check by an independent person or department where required	a) See 8.2 of this standard c) IEC 61508-2:2010, 7.9 IEC 61508-3:2010, 7.4.7, 7.4.8, 7.9, Tables A.5, A.9
11	***PDS(SR)*** **integration**	Phase 6 of *PDS(SR)* safety lifecycle (see 5.3 of this standard)
	Integration and test of the safety related *PDS(SR)*.	See 6.5 of this standard IEC 61508-2:2010, 7.5 IEC 61508-3:2010, 7.4.8, 7.5

	Tasks	References
12	***Verification* of integration**	
	Review of HW/SW integration test results and documentation	See 8.2 of this standard IEC 61508-2:2010, 7.5, 7.9, Tables B.3, B.6 IEC 61508-3:2010, 7.4.3.2 f), 7.4.5.5, 7.4.6.1, 7.4.7, 7.4.8, 7.5, 7.9, Tables A.5, A.6, A.9
13	**Act of installing, commissioning and operation (user documentation)**	Phase 7 of *PDS(SR)* safety lifecycle (see 5.3 of this standard)
	Develop user documentation describing the *PDS(SR)* act of installing, commissioning, operation and maintenance.	See Clause 7 of this standard IEC 61508-2:2010, 7.6, Table .B.4
14	***Verification* of user documentation**	
	a) Reviews of user documentation describing the *PDS(SR)* act of installing, commissioning, operation and maintenance. b) Check by an independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:2010, 7.9
15	***Validation* of *PDS(SR)***	Phase 8 of *PDS(SR)* safety lifecycle (see 5.3 of this standard)
	a) Provide all necessary information needed for *PDS(SR) validation* b) Complete software and appropriate documentation c) *Validation* tests and procedures according to the *validation* plan d) Documentation of the results of the *validation* tests e) Prepare appropriate documentation for third party *validation* where necessary	a) See 8.3 of this standard c) IEC 61508-2:2010, 7.3, 7.7, Tables B.5, B.6 IEC 61508-3:2010, 7.7, 7.9, Table A.7
16	***PDS(SR)* modification procedure**	
	a) Modification request and analysis b) Appropriate documentation of all modified parts of the *PDS(SR)* c) Re-*verification* of modified parts d) Update of reliability prediction if modification has an impact on fault tolerance, probability of dangerous faults, *diagnostic coverage* or *common cause failure* e) Re-*validation* of at least the modified parts of the *PDS(SR)* f) Software modification	a) See Clause 10 of this standard b) IEC 61508-1:2010, 7.16 IEC 61508-2:2010, 7.5.2.5, 7.8 Example in IEC 61508-1:2010, Figure 9 f) IEC 61508-3:2010, 7.1.2.9, 7.5.2.6, 7.6.2, 7.8.2, Table A.8

Annex B
(informative)

Example for estimation of *PFH*

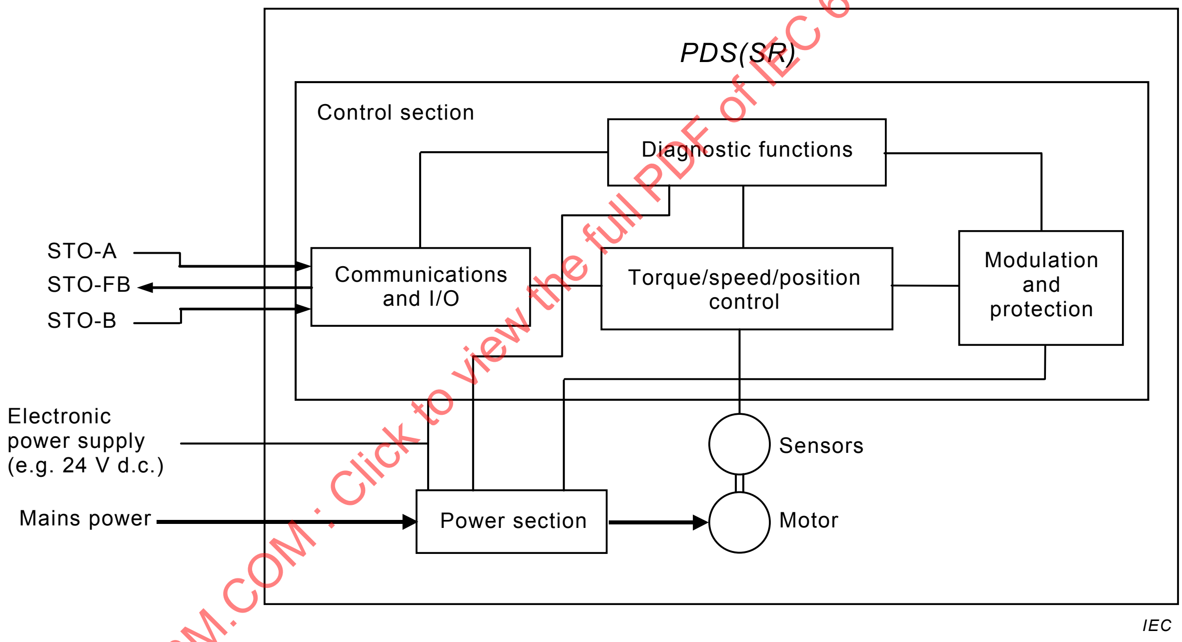
B.1 General

This clause describes the estimation of the *PFH* of an example *PDS(SR)* with the *safety sub-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 sub-function* STO, which is triggered by two redundant digital inputs and gives a single feedback signal through a digital output (see Figure B.1).



Key

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*.

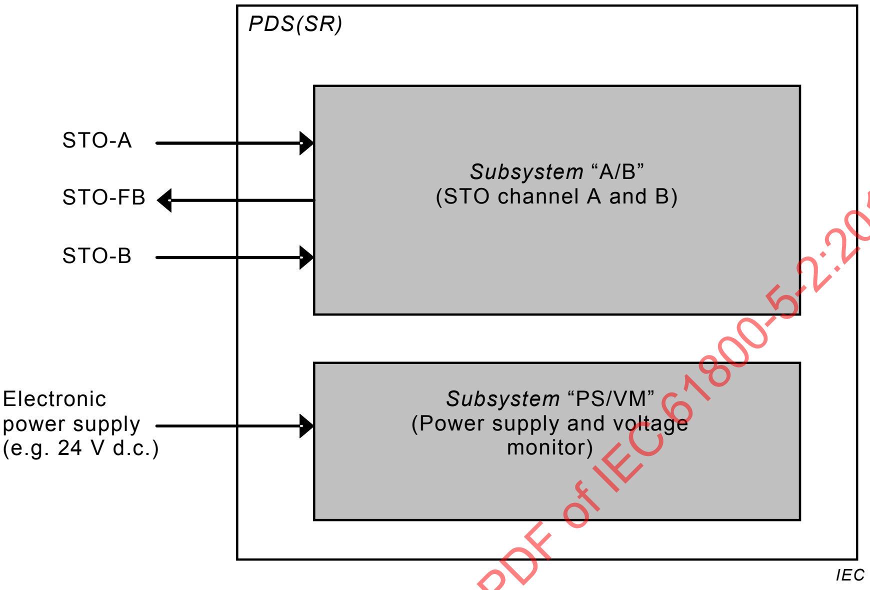
Within the *PDS(SR)*, the *safety sub-function* STO is implemented together with the non-safety-related functionality of the *PDS(SR)* using only a few *safety sub-function* exclusive components.

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 sub-function* STO of this example *PDS(SR)* is calculated as follows:

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

where $PFH_{\mathrm{A/B}}$ and $PFH_{\mathrm{PS/VM}}$ are the *PFH* values of *subsystem* A/B and *subsystem* PS/VM respectively.



Key

STO-A	STO trigger input channel A
STO-B	STO trigger input channel B
STO-FB	STO feedback output

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

B.2.2 *Subsystem* A/B

The *safety sub-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 sub-function*:

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

The architectural constraints of a type B *subsystem* (see 6.2.3.3) show that, for *SIL* 2 and hardware fault tolerance 1, the *safe failure fraction (SFF)* shall 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 sub-function*:

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

The architectural constraints of a type B *subsystem* (see 6.2.3.3) 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

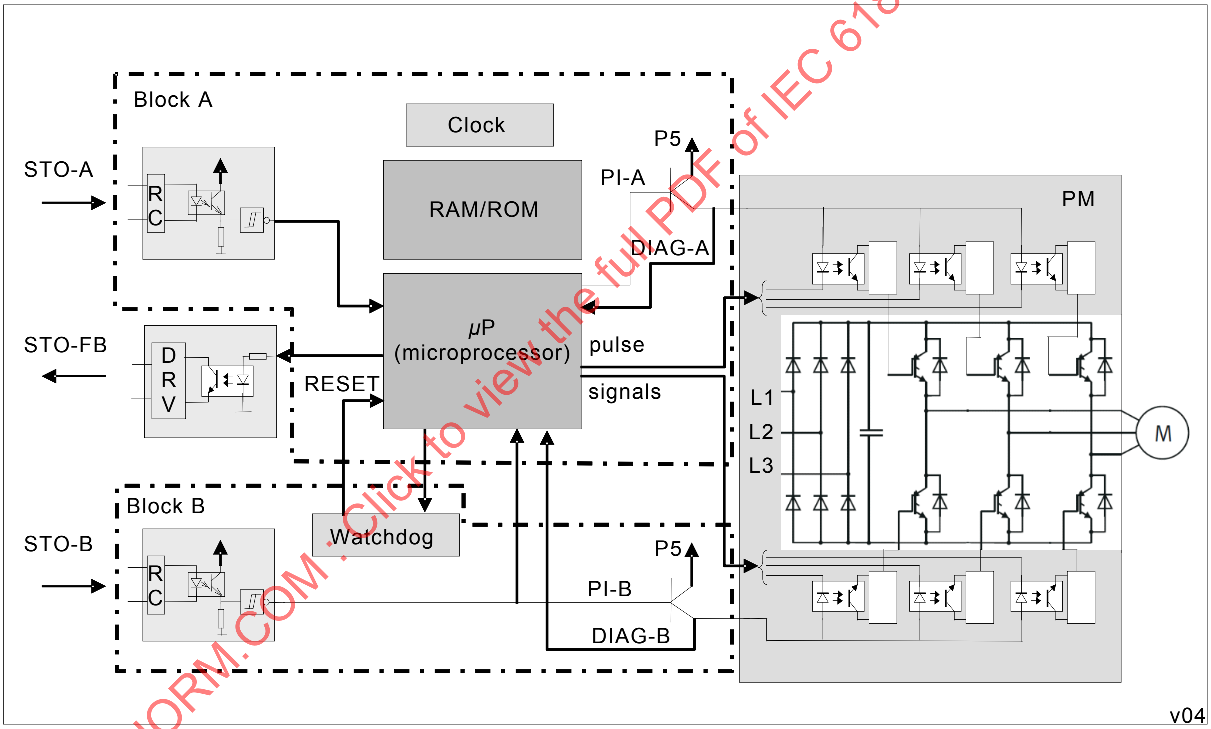
B.3.1 *Subsystem* "A/B" (main *subsystem*)

B.3.1.1 Function block division

Within the *PDS(SR)*, the *subsystem* A/B is part of the implementation of the *safety sub-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 sub-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, each channel is merged in one function block (Block A and B).

Component failures within the power module itself do not cause a loss of the *safety sub-function*. Therefore, the power module is not to be included in any subsystem contributing to the *PFH* value.



Key

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

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

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 can 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 sub-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, IEC 61508-6:2010, Annex C, 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 can be defined using the tables in IEC 61508-2:2010. This proportioning defines the failure rates λ_{DD} (dangerous detected) and λ_{DU} (dangerous undetected) of the component.

The total failure rates of the function block (λ_{S}, λ_{DD}, λ_{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 IEC 61508-6:2010, Annex C, 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 failure*s and a 50 % portion of *dangerous failure*s. The portion of detected failures is determined by using the tables of IEC 61508-2.

NOTE Use of this simplified method is more efficient than a detailed analysis but can result in failure rates λ_{S}, λ_{DD} and λ_{DU} less favorable (i.e. more conservative) than if a detailed analysis is conducted

This method will also lead to the failure rates λ_{S}, λ_{DD} and λ_{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 61508-2:2010.

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

Method (IEC 61508-2:2010)	DC level claim	*Diagnostic test* implementation
Table A.3 Failure detection by on-line 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:	λ_A	(total failure rate)		450 FIT
	λ_{AS}	(proportion of *safe failures*)	0,5*450 FIT	225 FIT
	λ_{AD}	(proportion of *dangerous failures*)	0,5*450 FIT	225 FIT
	λ_{ADD}	DC_A*λ_{AD}	0,9*225 FIT	202,5 FIT
	λ_{ADU}	(1-DC_A)*λ_{AD}	(1-0,9)*225 FIT	22,5 FIT
Block B:	λ_B	(total failure rate)		70 FIT
	λ_{BS}	(proportion of *safe failures*)	0,5*70 FIT	35 FIT
	λ_{BD}	(proportion of *dangerous failures*)	0,5*70 FIT	35 FIT
	λ_{BDD}	DC_B*λ_{BD}	0,9*35 FIT	31,5 FIT
	λ_{BDU}	(1-DC_B)*λ_{BD}	(1-0,9)*35 FIT	3,5 FIT

The *safe failure fraction* of *subsystem* A/B, calculated according to IEC 61508-2:2010, Clause C.1, item h, is:

$$
\begin{aligned}
SFF_{A/B} &= [(\lambda_{AS}+\lambda_{BS}) + (DC_A * \lambda_{AD}) + (DC_B * \lambda_{BD})] / [(\lambda_{AS}+\lambda_{BS}) + (\lambda_{AD}+\lambda_{BD})] \\
&= [(225 + 35) + (0{,}9 * 225) + (0{,}9 * 35)]\ \text{FIT} / [(225 + 35) + (225 + 35)T]\ \text{FIT} \\
&= 494\ \text{FIT} / 520\ \text{FIT};
\end{aligned}
$$

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

NOTE The calculation of $SFF_{A/B}$ is shown to demonstrate the principal. Due to the determined test intervals in Table B.1, $SFF_{A/Bresulting}$ can be applied (see Clause B.4).

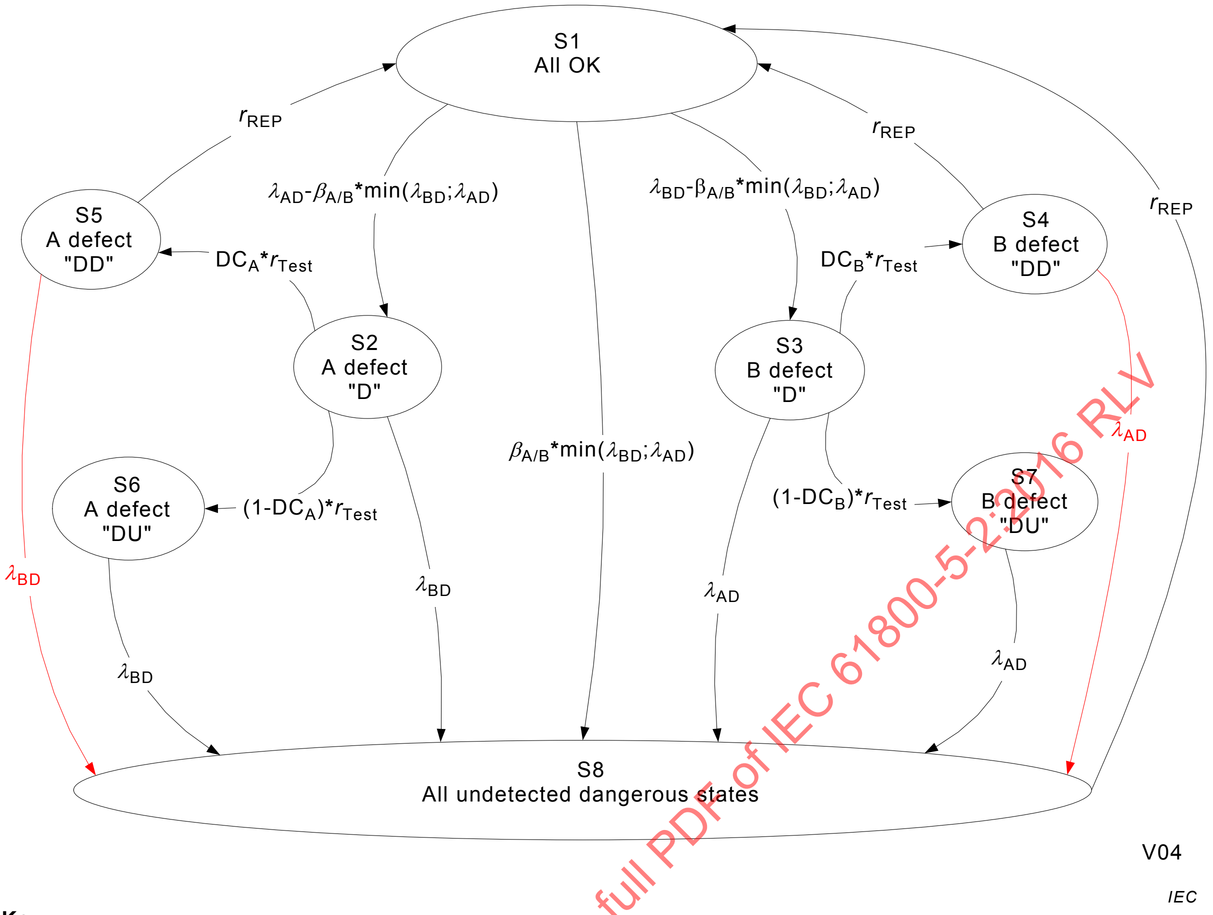
B.3.1.4 *Common cause failure* factor $\beta_{A/B}$

The *common cause failure* factor $\beta_{A/B}$ is estimated by using IEC 61508-6:2010, Table D.4.

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

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.



Key:

S1, S2, S3, S4, S5, S6, S8: states of the Markov model

"D": defect

"DD": defect detected

"DU" defect undetected

other terms are explained in the clause above

NOTE 1 The above Markov model Figure B.4 can 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 test*s 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(λ_{BD};λ_{AD}) means λ_{BD} or λ_{AD}, whichever is smaller. Due to the fact that the common cause failure rate, while increasing the beta factor, can reach only the λ value of the channel with the smaller value the minimum function for calculating the common cause failure rate is justified.

NOTE 4 The Model assumes continuous mode of operation, i.e. permanent presence of the demand to perform the *safety sub-function*. Therefore, any entering to state S8 causes a contribution to *PFH* and no additional transitions are needed to represent the occurrence of a demand. Thus the model covers the entire range of possible demand rates. On the other hand, in the present case of a redundant architecture the assumption of continuous demand does not lead to a significant increase of PFH as compared to high demand.

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

The model does not take into account “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 The rate of simultaneous failure of both blocks can never be greater than the lower of 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 sub-function* is no longer available and the test is not effective any longer. Since continuous *mode of operation* is assumed for the *PDS(SR)*, state S8 also represents the "*hazard*ous event" resulting from a dangerously failed *PDS(SR)* confronted with demand of the *safety sub-function*.

B.3.1.6 *PFH* value calculation

λ values, DC and β 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 [$p_{\text{i}}(t)$] of each state [S*i*] of the Markov model can 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 can be done up to the *mission time* T_{M}.

$$PFH_{A/B} = \frac{1}{T_M}\int_0^{T_M}\left\{\beta_{A/B}\cdot\min\left(\lambda_{AD},\lambda_{BD}\right)\cdot p_1(t)+\lambda_{AD}\left[p_3(t)+p_4(t)+p_7(t)\right]+\lambda_{BD}\left[p_2(t)+p_5(t)+p_6(t)\right]\right\}dt$$

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

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

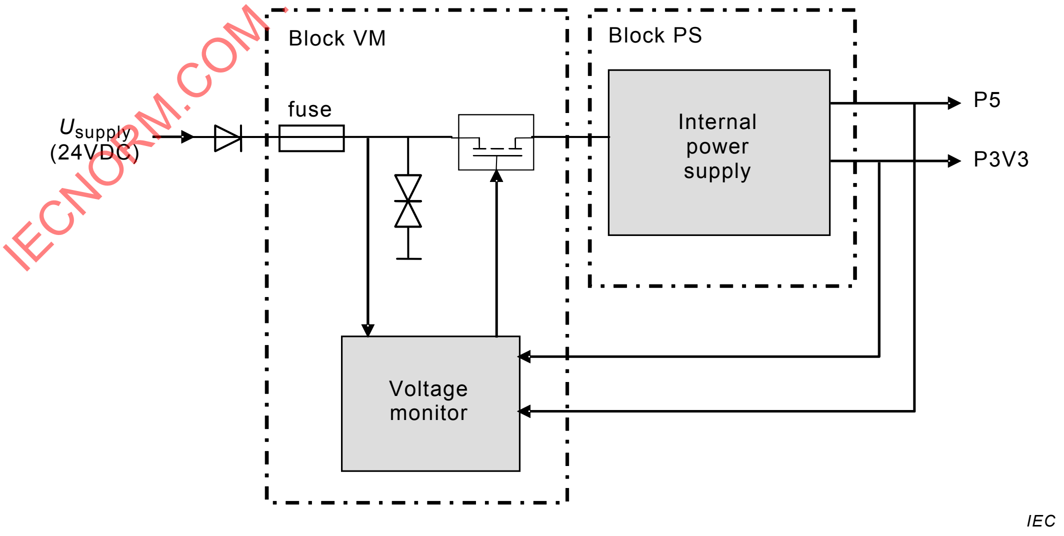
$\beta_{A/B}$	r_{Rep}	r_{Test}	T_M years	$PFH_{A/B}$
2 %	1/8 h	1/8 h	10	$7{,}67 \times 10^{-10}$ /h
2 %	1/8 h	**1/24 h**	10	$7{,}68 \times 10^{-10}$ /h
2 %	1/8 h	**1/168 h**	10	$7{,}70 \times 10^{-10}$ /h
2 %	1/8 h	**1/672 h**	10	$7{,}76 \times 10^{-10}$ /h
2 %	1/8 h	**1/8760 h**	10	$8{,}76 \times 10^{-10}$ /h
2 %	**1/8760 h**	1/8 h	10	$8{,}76 \times 10^{-10}$ /h
2 %	1/8 h	1/8 h	**20**	$8{,}34 \times 10^{-10}$ /h
2 %	1/8 h	**1/672 h**	20	$8{,}43 \times 10^{-10}$ /h
3 %	1/8 h	1/8 h	20	$1{,}18 \times 10^{-9}$ /h
5 %	1/8 h	1/8 h	20	$1{,}88 \times 10^{-9}$ /h
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. Nevertheless, not all of the parameter values may be realistic. Regarding the achievable overall accuracy of a PFH calculation, the PFH value of a complete safety device should be specified using a mantissa with one decimal place only. Table B.2 provides two decimal places only in order to demonstrate even low effects of particular parameter variations.

B.3.2 *Subsystem* "PS/VM"

B.3.2.1 Function block division

For the *safety sub-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).



Key

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 IEC 61508-2:2010, Annex A.

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).

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

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

The *safe failure* fraction of *subsystem* PS/VM is calculated according to IEC 61508-2:2010, Clause C.1, item g (see Note):

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

$$= [125 + (125 * 0{,}99)] \text{ FIT} / 250 \text{ FIT}$$

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

NOTE The monitor block does not contribute to the *SFF* but only to the *PFH*.

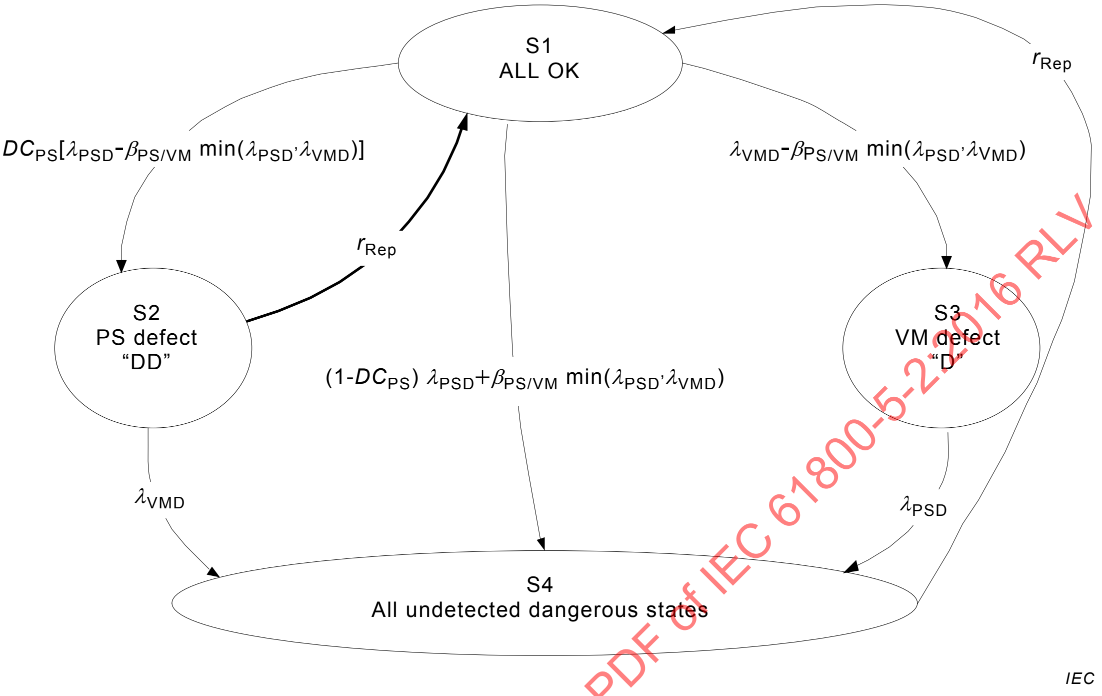
B.3.2.4 *Common cause failure* factor $\beta_{\mathbf{PS/VM}}$

The *common cause failure* factor $\beta_{PS/VM}$ is estimated by using of IEC 61508-6:2010, Table D.4.

$\beta_{PS/VM}$ = 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.


S1
ALL OK
r_{Rep}
$DC_{\text{PS}}[\lambda_{\text{PSD}}\text{-}\beta_{\text{PS/VM}}\ \min(\lambda_{\text{PSD}},\lambda_{\text{VMD}})]$
$\lambda_{\text{VMD}}\text{-}\beta_{\text{PS/VM}}\ \min(\lambda_{\text{PSD}},\lambda_{\text{VMD}})$
r_{Rep}
S2
PS defect
“DD”
S3
VM defect
“D”
$(1\text{-}DC_{\text{PS}})\ \lambda_{\text{PSD}}+\beta_{\text{PS/VM}}\ \min(\lambda_{\text{PSD}},\lambda_{\text{VMD}})$
λ_{VMD}
λ_{PSD}
S4
All undetected dangerous states
IEC

Key:

S1, S2, S3, S4: states of the Markov model

"D":	defect
"DD":	defect detected
"DU"	defect undetected

Other terms are explained in Subclause B.3.2

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.

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

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 $\beta_{\text{PS/VM}}$ and the lower of the *dangerous failure* rates of function block PS and VM (see Note 3).

NOTE 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 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 sub-function* is no more available

State S4 represents the dangerous situation where the *safety sub-function* is no longer available and the test is not effective any longer. Since continuous *mode of operation* is assumed for the *PDS(SR)*, state S4` represents the "*hazard*ous event" resulting from a dangerously failed *PDS(SR)* confronted with demand of the *safety sub-function*.

B.3.2.6 *PFH* value calculation

λ values, DC and β 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 can 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 can be done up to the *mission time* T_{M}.

$$\mathrm{PFH}_{\mathrm{PS/VM}} = \frac{1}{\mathrm{T_M}} \int_{0}^{\mathrm{T_M}} \left[\left((1 - \mathrm{DC_{PS}}) \cdot \lambda_{\mathrm{PSD}} + \beta_{\mathrm{PS/VM}} \cdot \min(\lambda_{\mathrm{PSD}}, \lambda_{\mathrm{VMD}}) \right) \cdot p_1(t) + \lambda_{\mathrm{VMD}} \cdot p_2(t) + \lambda_{\mathrm{PSD}} \cdot p_3(t) \right] dt$$

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

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

$\beta_{\text{PS/VM}}$	r_{Rep}	T_{M} years	$PFH_{\text{PS/VM}}$
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
Values in bold characters give the modified value regarding the previous line.			

B.3.3 *PFH* value of the *safety sub-function* STO of *PDS(SR)*

Example *PFH* values with r_{Rep} = 1/8 h, r_{Test} = 1/8 h and varied parameter T_{M}:

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

$PFH_{\text{STO}/PDS(SR)}$ (T_{M} = 10 years) = $(7{,}67 \times 10^{-10}/\text{h} + 4{,}39 \times 10^{-9}/\text{h}) = 5{,}16 \times 10^{-9}/\text{h}$;

$PFH_{\text{STO}/PDS(SR)}$ (T_{M} = 20 years) = $(8{,}34 \times 10^{-10}/\text{h} + 5{,}03 \times 10^{-9}/\text{h}) = 5{,}86 \times 10^{-9}/\text{h}$.

B.4 Reduction of DC and SFF depending on test interval

Increasing the test interval will lead to a lower resulting *diagnostic coverage* (DC$_{\text{resulting}}$) and lower resulting *safe failure fraction*.

In the following the deduction of DC and SFF including the dependence on the diagnostic test interval is given:

Refer to IEC 61508-6: 2010, B.3.3.2.1, Formula for t(CE)

t(CE) = (1-DC)(T1/2 + MRT) + DC * MTTR; (1)

with T1 = TM;

MRT = 0; and (no repair during operation time of PDS)

MTTR = DI/2; (average time until fault detection, no repair time)

follows:

t(CE) = (1-DC)TM/2 + DC*DI/2; (2)

For reference to normative requirements a ‘resulting DC‘ will be calculated which depends on the diagnostic interval DI

Assuming:

t(CE) = (1-DC‘)TM/2;

then:

(1-DC’)TM/2 = (1-DC)TM/2 + DC*DI/2;

resolving for DC’ leads to

DC‘ (= DC$_{\text{resulting}}$) depending on DC and DI

DC’ = DC$_{\text{resulting}}$ = DC(1-DI/TM);

SFF‘ (= SFF$_{\text{resulting}}$) according IEC 61508:

SFF$_{\text{resulting}}$ = $\boldsymbol{SFF'} = \frac{\lambda_S}{\lambda} + \left(1 - \frac{\lambda_S}{\lambda}\right) DC'$;

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: 2004**,** Reliability data handbook – *Universal model for reliability prediction of electronics components, PCBs and equipment*
- Siemens Standard SN 29500, Failure rates of components*, (parts 1 to 16); can be obtained from: Siemens AG, CT TIM IR SI, D-80200, Munich.*
- Reliability Prediction of Electronic Equipment, MIL-HDBK-217F, *Notice 2:1995, Department of Defense, Washington DC, 20301.*
- Reliability Prediction Procedure for Electronic Equipment, Telcordia SR-332*, Issue 03, Jan 2011 (telecom-info.telcordia.com),*
- Electronic Parts Reliability Data (RAC-STD-6100), *Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).*
- 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.*
- China 299B Electronic Reliability Prediction
- AT&T reliability manual – *Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors,l, AT&T Reliability Manual, Van Nostrand Reinhold, 1990, ISBN:0442318480.*
- 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.,*
- IRPH ITALTEL Reliability Prediction Handbook
- PRISM (RAC / EPRD) – *is the new Reliability Analysis Center (RAC) software tool that ties together several tools into a comprehensive system reliability prediction methodology. The PRISM concept accounts for the myriad of factors that can influence system reliability, combining all those factors into an integrated system reliability assessment resource. PRISM was developed to overcome inherent limitations in MIL-HDBK-217 that is no longer being actively maintained or updated by the Department of Defense (DoD) The PRISM software is available from the address below, RELIASS; Cams Hall, Cams Hill; FAREHAM; Hampshire, PO16 8AB;United Kingdom*
- Analog Devices Component MTTF data – *www.analog.com under "about ADI"*
- FIDES – *Reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA, new version from 2009 (http://fides-reliability.org*).

C.2 Helpful standards concerning component failure

IEC 60300-3-2:2004, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-5:2001, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60319:1999, *Presentation and specification of reliability data for electronic components*

IEC 60706-3:2006, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60721-1:2002, *Classification of environmental conditions – Part 1: Environmental parameters and their severities*

IEC 61709:2011, *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 D.3.1 up to D.3.16 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 can 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 can be helpful for evaluation:

Test Method for Measuring Whisker Growth on Tin and Tin Alloy Surface Finishes, JESD22A121A, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834,http://www.jedec.org/standards-documents/results/JESD22A121

Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes, JESD201A, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, http://www.jedec.org/standards-documents/results/JESD201

Tin whiskers on printed circuit boards – Consequences for safety components in machine construction, IFA Institut für Arbeitsschutz, Alte Heerstrasse 111, 53757 Sankt Augustin, http://www.dguv.de/ifa/Praxishilfen/Zinnwhisker-auf-Leiterplatten/index-2.jsp

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 can be regarded.

NOTE 4 Whiskers on tracks of printed circuit boards have not been reported yet. Tracks usually consist of copper without tin coating. Pads can 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.1 is made.

D.3 Fault models

D.3.1 Conductors/cables

The requirements of ISO 13849-2: 2012,Table D.4, apply.

D.3.2 Printed wiring boards/assemblies

The requirements of Table D.1 apply.

Table D.1 – 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. 2) The creepage distances and clearances are dimensioned to at least IEC 61800-5-1 with pollution degree 2/ OVC III; if both tracks are PELV/SELV –powered, pollution degree 2/ OVC II apply with a minimum clearance of 0,1 mm. 3) The assembled board is mounted in an enclosure giving protection against conductive contamination and the printed side(s) are coated with an ageing-resistant varnish or protective layer covering all conductor paths. NOTE 1 Alternative methods to ensure protection against conductive contamination are: • enclosure of safety relevant circuitry of at least IP54 according to IEC 60529, • cabinet for safety relevant *BDM/CDM* of at least IP54 according to IEC 60529, • environmentally controlled location for the *BDM/CDM* which does not contain conductive contamination. NOTE 2 Experience has shown that a solder mask is satisfactory as a protective layer. NOTE 3 A protective layer covering according to IEC 60664-3 can reduce the creepage distances and clearances dimensions. Compliance with NEMA 250, Type 12 enclosure requirements is considered to be sufficient to demonstrate compliance with IP54 requirements.
Open-circuit of any track	None	–

NOTE 1 Printed wiring board (PWB) is another term for printed circuit board (PCB).

NOTE 2 Over voltage category (OVC) is defined in IEC 61800-5-1.

D.3.3 Terminal block

The requirements of Table D.2 apply.

Table D.2 – 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. 2) Guaranteed by design, for example shaping shrink down plastic tubing over connection point.
Open-circuit of individual terminals	None	–

D.3.4 Multi-pin connector

The requirements of Table D.3 apply.

Table D.3 – 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). Remark 2) also applies if the connector is mounted on a PWB.	1) By using ferrules or other suitable means for multi-stranded wires, regarding Creepage distances and clearances and all gaps refer to IEC 61800-5-1:2007, 4.3.6. 2) The assembled board is mounted in an enclosure giving protection against conductive contamination and the printed side(s) are coated with an ageing-resistant varnish or protective layer covering all conductor paths NOTE 1 Alternative methods to ensure protection against conductive contamination are: • Enclosure of safety relevant circuitry of at least IP54 according to IEC 60529 • Cabinet for safety relevant *BDM/CDM* of at least IP54 according to IEC 60529 • Environmentally controlled location for the *BDM/CDM* which does not contain conductive contamination NOTE 2 Experience has shown that a solder mask is satisfactory as a protective layer. NOTE 3 A protective layer covering according to IEC 60664-3 can reduce the creepage distances and clearances dimensions. Compliance with NEMA 250, Type 12 enclosure requirements is considered to be sufficient to demonstrate compliance with IP54 requirements.
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	–

D.3.5 Electromechanical devices

The requirements of Table D.4 apply.

Table D.4 – 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 61800-5-1:2007, 4.3.6 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.

D.3.6 Transformers

The requirements of ISO 13849-2:2012, Table D.12 apply.

D.3.7 Inductances

The requirements of ISO 13849-2:2012, Table D.13 apply.

D.3.8 Resistors

The requirements of ISO 13849-2:2012, Table D.14 apply.

D.3.9 Resistor Networks

The requirements of ISO 13849-2:2012, Table D.15 apply .

D.3.10 Potentiometers

The requirements of ISO 13849-2:2012, Table D.16 apply.

D.3.11 Capacitors

The requirements of ISO 13849-2:2012, Table D.17 apply.

D.3.12 Discrete semiconductors

(For example diodes, Zener diodes, transistors, triacs, GTO thyristors, IGBTs, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs]) .

The requirements of ISO 13849-2:2012, Table D.18 apply.

D.3.13 Signal Isolation components

The requirements of Table D.5 apply.

Table D.5 – Signal Isolation components

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 across the isolation barrier	Short-circuit across the isolation barrier can be excluded if remarks 1) and 2) are fulfilled.	1) The Signal Isolation component is built in accordance with OVC III according to IEC 61800-5-1. If a SELV/PELV power supply is used, pollution degree 2/ OVC II applies. NOTE All requirements of IEC 61800-5-1:2007, 4.3.6 apply. 2) Measures are taken to ensure that an internal failure of the Signal Isolation component cannot result in excessive temperature of its insulating material.

D.3.14 Non-programmable integrated circuits

The requirements of Table D.6 apply.

Table D.6 – Non-programmable integrated circuits

Fault considered	Fault exclusions	Remarks
Open-circuit of each individual connection	None	Refer to IEC 61508-2:2010, Annex E
Short-circuit between any two connections	Possible exclusion – see remark.	
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	
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.		

D.3.15 Programmable and/or complex integrated circuits

The requirements of Table D.7 apply.

Table D.7 – Programmable and/or complex integrated circuits

Fault considered	Fault exclusions	Remarks
Faults in all or part of the function	None	Refer to IEC 61508-2:2010, Annex E
Open-circuit of each individual connection	None	
Short-circuit between any two connections	Possible exclusion – see remark.	
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	
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 sub-function*.		

D.3.16 Motion and position feedback sensors

The requirements of Table D.8 apply.

Table D.8 – Motion and position feedback sensors

Fault considered	Fault exclusion	Remarks
General		
Short-circuit between any two conductors of the connecting cable	The requirements of D.3.1 applies	
Open-circuit of any conductor of the connecting cable	None	
Stuck-at Ground, $U_B/2$, U_B on single or on several inputs/outputs at the same time	None	U_B is the power supply of the sensor. Sensor inputs are applied e. g. for parameter settings. The behavior of the individual sensor in case of a fault has to be considered.
Open circuit 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 or loosening of attachment during standstill or during motion: – sensor housing from motor chassis – sensor shaft from motor shaft – mounting of the read head	Preparing FMEA and prove: – permanent fastness for form-locked connections – fastness for force-locked connections	The maximum permissible loading of the sensor is known or limited on the sensor's data sheet. a) For form-locked connections: 1) Design for permanent fastness in accordance with generally acknowledged technical experience with a high safety factor – Verification is performed by calculation and with a suitable test. – Example for steel components: Overdimensioning with a safety factor $S \geq 2$ against fatigue fracture. or 2) Overdimensioning with a safety factor $S \geq 5$ against fatigue fracture – Verification is performed by calculation. b) For force-locked connections: 1) Overdimensioning with a safety factor $S \geq 4$ against slipping – Detailed measures for application and maintaining the preloading force are to be defined in the user documentation (e.g. defined pairs of materials, surfaces and torque-controlled tightening methods). – Verification is performed by calculation and with a suitable test. or 2) Overdimensioning with a safety factor $S \geq 10$ against slipping – Measures for application and maintaining the preloading force are to be defined in the user documentation – Verification is performed by calculation.
Loosening of solid measure[a] (e.g. optical encoder disc)	None	Output indicates wrong position
No light from diode	None	Not applicable on encoders not using any light emitting diodes, e.g. resolvers
Additionally for sensors with Sin/Cos – output signals, analogue signal generation		

Fault considered	Fault exclusion	Remarks
Static input and output, on one single or several signals, amplitude within power supply voltage	None	
Change of sine-/cosine output signal(s) into square wave: each half period sine wave replaced by square wave with same amplitude.	None	For example, no Sin/Cos – type signal, signal offset It is impossible to consider all possible signal shapes caused by component faults. Instead, square wave is assumed representative.
Exchange of Sin and Cos output signal	Fault exclusion is permitted if there are no electronic components applied to select an output signal from several sources	
Change of DC part of sine-/cosine output signal(s) within power supply voltage.	none	
Additionally for incremental 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
Additionally for encoder with incremental and absolute signals		
Simultaneous wrong position signal from both 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 sensors with processor based interface		
Communication faults: – repeating – loss – insertion – wrong order – wrong data – delay – masquerade	None	Equals fault model for communication busses which are addressed by the IEC 61784 series.
Additionally for rotary sensor, multiturn		
Wrong number of revolutions	None	May be without impact on single turn signals
Additionally for sensors with synthesised output signals		
Wrong output signal due to synthesiser failure	None	
Additionally for sensors with position value acquired by counter		
Wrong position due to incorrect count	None	
Additionally for linear sensors		
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	

Fault considered	Fault exclusion	Remarks
– Central timer fails – No conversion start for A/D converter – Wrong timing of Sample & Hold	None	
A/D converter generates wrong values	None	For example due to over modulation 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		
This table has been written assuming the use of optical sensors and resolvers. If other sensors (for example inductive sensors) are used, corresponding faults apply.		

Annex E
(normative)

Electromagnetic (EM) immunity requirement for *PDS(SR)*

E.1 General

To show compliance with the design requirements for a *PDS(SR)* regarding electromagnetic (EM) immunity described in 6.2.6, the immunity requirements provided in the following tables E.1, E.2 and E.3 shall apply with performance criteria of 9.3.3.

According to IEC Guide 107 the requirements of this Annex E are based on IEC 61000-6-7:2014.

Due to the differences of port/interface definitions between IEC 61000-6-7 and IEC 61800-3, the EM immunity requirements for *PDS(SR)* are given in Tables E.1, E.2 and E.3.

It is permitted to verify immunity of safety sub-functions for all phenomena in Tables E.1 and E.2 using calculation or simulation, as well as by testing.

E.2 Immunity requirements – low frequency disturbances

These requirements apply to the following power ports:

- all power ports which provide power for *safety sub-function*s in low voltage *PDS(SR)*, and
- all auxiliary low voltage power ports which provide power for *safety sub-function*s in *PDS(SR)* of rated voltage above 1 000 V (only second environment).

Table E.1 – Minimum immunity requirements for voltage deviations, dips and short interruptions

Phenomenon		First environment		Second environment	
	Reference document	**Level**		**Level**	
Voltage deviations (> 60 s)	IEC 61000-2-4 Class 2	±10 % [a]		+10 % / –15 % [a]	
Voltage dips [c]	IEC 61000-4-11 [d] or IEC 61000-4-34 [d]	Volts remaining	Cycles	Volts remaining	Cycles
		0 % 40 % 70 % –	1 25/30 [b] 25/30 [b] –	0 % 40 % 70 % 80 %	1 10/12 [b] 25/30 [b] 250/300 [b]
Voltage dips for auxiliary DC power ports below 60 V [e]	IEC 61000-4-29	40 % 70 %	0,5 0,5	40 % 70 %	0,5 0,5
Short interruptions	IEC 61000-4-11 [d] or IEC 61000-4-34 [d]	Volts remaining	Cycles	Volts remaining	Cycles
		– 0 % 0 %	– 25/30 [b] 250/ 300 [b]	0 % 0 % 0 %	10/12 [b] 25/30 [b] 250/300 [b]

[a] "Voltage deviation" is a supply voltage variation from the nominal supply voltage. Testing of voltage deviations for three phase PDS requires increasing or reducing the voltage of all three phases simultaneously.

[b] "x/y cycles" means "x cycles for 50 Hz test" and "y cycles for 60 Hz test"

[c] Power ports with current rating ≥75 A, the method of the voltage drop test according to IEC 61400-21:2008, 7.5 can be used.

[d] IEC 61000-4-11 applies to equipment rated less than or equal to 16 A and IEC 61000-4-34 to equipment rated above 16 A.

[e] This test addresses external DC power supplies which provide power to the safety sub-function(s)

NOTE No conducted common mode tests are required due to the higher emission of conducted common mode voltage by a *PDS(SR)* compared to the test levels of IEC 61000-6-7.

Table E.2 – *PDS(SR)* minimum immunity requirements for voltage deviations, dips and short interruptions on main power ports with a rated voltage above 1 000 V

Phenomenon	Reference document	Level	
Voltage deviations exceeding 1 min	IEC 61000-2-4 Class 3	+10 % / –15 %	
Voltage deviations not exceeding 1 min	IEC 61000-2-4 Class 3	+10 % / –15 %	
Voltage dips	IEC 61000-4-34 [b]	Volts remaining	Cycles
		0 %	1
		40 %	10/12 [c]
		70 %	25/30 [c]
		80 %	250/300 [c]
Voltage dips for auxiliary DC power ports below 60 V [e]	IEC 61000-4-29	40 %	0,5
		70 %	0,5
Short interruptions	IEC 61000-4-34 [b]	Volts remaining	Cycles
		0 %	10/12 [b]
		0 %	25/30 [b]
		0 %	250/300 [c]

[a] "Voltage deviation" is a supply voltage variation from the nominal supply voltage. Testing of voltage deviations for three phase PDSs requires increasing or reducing the voltage of all three phases simultaneously.

When considering voltage deviations, any voltage steps shall not exceed ±12 % of nominal voltage and the time between steps shall not be less than 2 s.

When the voltage is below nominal, the maximum output power ratings – speed and/or torque – can be reduced, because they are voltage dependent.

[b] Typical depths and durations of voltage dips are given in IEC 61000-2-8.

[c] "x/y cycles" means "x cycles for 50 Hz test" and "y cycles for 60 Hz test".

[d] Opening of fuses is permitted for line-commutated converters operating in inverting mode.

[e] This test addresses external DC power supplies which provide power to the safety sub-function(s).

E.3 Immunity requirements – high frequency disturbances

Table E.3 – Immunity requirements – high frequency disturbances

1	2	3	4	5
Port/interface	**Phenomenon**	**Basic standard for test method**	**Level for first environment**	**Level for second environment**
Enclosure port	ESD [m,n] air discharge (AD) [o] contact discharge (CD)	IEC 61000-4-2 [q]	4 kV CD or 8 kV AD if CD impossible	6 kV CD or 8 kV AD if CD impossible 8kV CD or 15 kV AD [m]
	Radio-frequency electromagnetic field, amplitude modulated [p]	IEC 61000-4-3*	80 MHz to 1 000 MHz 10 V/m 80 % AM (1 kHz)	80 MHz to 1 000 MHz 20 V/m [i,g] 80 % AM (1 kHz)
	Radio-frequency electromagnetic field, amplitude modulated [p]	IEC 61000-4-3*	1,4 GHz to 2,0 GHz 3 V/m 80 % AM (1 kHz)	1,4 GHz to 2,0 GHz 10 V/m [i,g] 80 % AM (1 kHz)
	Radio-frequency electromagnetic field, amplitude modulated [p]	IEC 61000-4-3*	2,0 GHz to 2,7 GHz 1 V/m 80 % AM (1 kHz)	2,0 GHz to 6 GHz 3 V/m [i,g] 80 % AM (1 kHz)
Power ports (except auxiliary DC power ports below 60 V)	Fast transient-burst	IEC 61000-4-4 [h]	2 kV/5 kHz [a]	4 kV/5kHz [a]
	Surge [b] 1,2/50 µs, 8/20 µs	IEC 61000-4-5 [r]	1 kV [c] 2 kV [d]	2 kV [c] 4 kV [d]
	Conducted radio-frequency common mode [e]	IEC 61000-4-6*	0,15 MHz to 80 MHz 10 V 80 % AM (1 kHz)	0,15 MHz to 80 MHz [k] 20 V [g] 80 % AM (1 kHz)
Power interfaces	Fast transient-burst [e]	IEC 61000-4-4 [h]	2 kV/5 kHz Capacitive clamp	4 kV/5 kHz Capacitive clamp
Signal interfaces	Fast transient-burst [e]	IEC 61000-4-4 [h]	1 kV/5 kHz Capacitive clamp	2 kV/5 kHz Capacitive clamp
	Conducted radio-frequency common mode [e]	IEC 61000-4-6*	0,15 MHz to 80 MHz 10 V 80 % AM (1 kHz)	0,15 MHz to 80 MHz [k] 20 V [g] 80 % AM (1 kHz)
Ports for process measurement control lines Auxiliary DC power ports below 60 V	Fast transient-burst [e]	IEC 61000-4-4 [h]	2 kV/5 kHz Capacitive clamp	**4** kV/5 kHz Capacitive clamp
	Surge [f] 1,2/50 µs, 8/20 µs	IEC 61000-4-5 [r]	1 kV [d,f]	2 kV [d,f]
	Conducted radio-frequency common mode [e]	IEC 61000-4-6*	0,15 MHz to 80 MHz 10 V 80 % AM (1 kHz)	0,15 MHz to 80 MHz [k] 20 V [g] 80 % AM (1 kHz)

* See also IEC 61800-3:2012, 5.3.4.

NOTE The required immunity for *functional safety* purposes can be achieved through the use of external protection devices.

[a] Power ports with current rating <100 A: direct coupling using the coupling and decoupling network. Power ports with current rating ≥100 A: direct coupling or capacitive clamp without decoupling network. If the capacitive clamp is used, the test level shall be 4 kV/ 5 kHz or 100 kHz.

[b] Applicable only to power ports with current consumption <63 A during light load test conditions as specified in 5.1.3. of IEC 61800-3:2012. The rated impulse voltage of the basic insulation shall not be exceeded (see IEC 60664-1).

[c] Coupling line-to-line.

[d] Coupling line-to-earth.

[e] Applicable only to ports or interfaces with cables whose total length according to the manufacturer's functional specification can exceed 3 m.

[f] Applicable only to ports with cables whose total length according to the manufacturer's functional specification can exceed 30 m. In the case of a shielded cable, a direct coupling to the shield is applied. This immunity requirement does not apply to fieldbus or other signal interfaces where the use of surge protection devices is not practical for technical reasons. The test is not required where normal functioning cannot be achieved because of the impact of the coupling/decoupling network on the equipment under test (EUT).

[g] The test level specified is the r.m.s. value of the unmodulated carrier.

[h] For an *PDS(SR)* intended to be used in *safety integrity level SIL* 3 applications (according to IEC 61508), the duration of the test at the highest specified level shall be increased by a factor of 5 compared to the duration as given in the basic standard.

[i] These increased values shall be applied in the frequency ranges as given in Table E.4 used for mobile transmitters in general.

[k] These increased values shall be applied in the frequency ranges as given in Table E.5 used for mobile transmitters in general.

[m] The higher test levels apply in case the discharge is done onto cabinet enclosures.

[n] Levels shall be applied in accordance with the environmental conditions described in IEC 61000-4-2 on parts which can be accessible by persons other than trained personnel in accordance with defined procedures for the control of ESD but not to equipment where access is limited to service personnel only.

[o] For air discharge test not only the given level has to be tested, but all the levels up to the given one.

[p] If hand held radio transmitters could be used closer than 20 cm a warning shall be given in the safety manual that the *PDS (SR)* could be disturbed.

[q] For a *PDS(SR)* intended to be used in *safety integrity level SIL* 3 applications, the number of discharges shall be increased by the factor of 3.

[r] For a *PDS(SR)* intended to be used in *safety integrity level SIL* 3 applications, the number of surge pulses shall be increased by the factor of 3.

Table E.4 – General frequency ranges for mobile transmitters and ISM for radiated tests

Centre frequency MHz	Frequency range MHz	Purpose
84,000	83,996 to 84,004	ISM (UK only)
	137 to 174	Mobile and SRD
151,850	151,820 to 151,880	MURS
154,585	154,570 to 154,600	MURS
168,000	167,992 to 168,008	ISM UK only
219,500	219 to 220	AMATEUR
	380 to 400	TETRA
	420 to 470	AMATEUR
433,920	433,05 to 434,79	ISM (Region 1 only)
	450 to 470	4G/LTE-A
	698 to 894	3G/UMTS3.9G/LTE
	746 to 845	TETRA
	825 to 845	TETRA
	830 to 840	3G/FOMA
	860 to 915	3.9G/LTE
873,000	870 to 876	TETRA
	860 to 960	RFID
	886 to 906	ISM UK only
	880 to 915	GSM 3G/FOMA 3G/HSPA
918,000	915 to 921	NADC
	902 to 928	ISM (Region 2 only)
	925 to 960	GSM 3G/HSPA
	1 240 to 1 300	AMATEUR
	1 428 to 1 496	3G/UMTS 3G/HSPA 3.9G/LTE
	1476 to 1511 1525 to 1559 1627 to 1661 1710 to 1785	3.9G/LTE
	1 710 to 1 785	GSM 3G/UMTS 3G/FOMA 3G/HSPA
	1 805 to 1 880	GSM 3G/UMTS 3G/FOMA 3G/HSPA 3.9G/LTE
	1 900 to 2 025	3G/UMTS 3G/FOMA 3.9G/LTE
	2 110 to 2 200	3G/UMTS 3G/FOMA 3.9G/LTE
	2 300 to 2 450	AMATEUR
	2 400 to 2 500	ISM
	2300 to 2400	3.9G/LTE 4G/LTE-A
	2 500 to 2 690	3.9G/LTE
	3 300 to 3 500	AMATEUR
	3 400 to 3 600	4G/LTE-A
	5 150 to 5 350	HIPERLAN
	5 470 to 5 725	HIPERLAN
	5 650 to 5 925	AMATEUR
	5 725 to 5 875	ISM
	5 795 to 5 815	RTTT

Table E.5 – General frequency ranges for mobile transmitters and ISM for conducted tests

Centre frequency MHz	**Frequency range** MHz	**Purpose**
3,39	3,370 to 3,410	ISM Netherlands only
6,780	6,765 to 6,795	ISM
13,560	13,553 to 13,567	ISM
27,120	26,957 to 27,283	ISM/CB/SRD
40,680	40,66 to 40,70	ISM/SRD
For those frequency bands where a centre frequency is indicated the test shall be performed at the centre frequency only.		

Annex F
(informative)

Estimation of PFD$_{\text{avg}}$ value for low demand with given PFH value

F.1 General

While low demand mode operation is possible for a *PDS(SR)*,this standard concentrates on to high demand and continuous mode, no requirements are given for low demand mode. *Safety sub-functions* implemented for high demand or continuous mode can be used in low demand mode. For this case a simplified conservative method to estimate the PFD$_{\text{avg}}$ value from the PFH value is given in this annex.

NOTE 1 For the limits of the PFD$_{\text{avg}}$ value regarding *SIL* see IEC 61508-1.

NOTE 2 For the design of a *PDS(SR)* especially for low demand mode see IEC 61508 series.

F.2 Estimation of PFD$_{\text{avg}}$ value for low demand with given PFH value

For an electrical power drive system with a specified *safety sub-function* quantified by a related *PFH* value for high demand or continuous *mode of operation*, an estimated value for the PFD*avg* in a low demand application can be derived from the *PFH* under certain circumstances. Provided that

1) the *safety sub-function* to be used in the low demand application is exactly the same as specified for high demand or continuous *mode of operation*, e.g. safe torque off (STO), and the system states regarded as safe states in the context of the high demand or continuous mode *safety sub-function* are also safe states in the context of the low demand application (e.g. de-energized output),
2) compulsory actuations of the *safety sub-function* needed for testing, if any, are executed in accordance with the requirements of the manufacturer,

an estimated value for the PFD$_{avg}$ may be derived from the *PFH* value for high demand using the following equation:

$$PFD_{avg} = \frac{1}{2} PFH \cdot T_M$$

where T_M is the specified *mission time* of the *PDS(SR)* expressed in hours.

NOTE 1 The indicated PFD$_{avg}$ equation tends to deliver conservative results.

NOTE 2 Considering a particular *PDS(SR)*, PFD$_{avg}$ often consumes a higher proportion of the PFD$_{avg}$ limit of a certain *SIL* than its *PFH* will consume with respect to the *PFH* limit of the same *SIL*. It can occur that the *PFH* value complies with a certain *SIL* while the PFD$_{avg}$ value derived from the above given formula does not. For the limits of the PFD$_{\text{avg}}$ value regarding *SIL,* see IEC 61508-2:2010.

NOTE 3 For *PFH* value estimation see 6.2.2.1.2.

NOTE 4 For description of PFD$_{\text{avg}}$ see IEC 61508-4:2010; 3.6.18.

Bibliography

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

IEC 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 60664-1:2007, *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 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

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 application programming requirements*

IEC 61513, *Nuclear power plants – Instrumentation and control 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 61558-1:2005/AMD1:2009

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

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*

IEC 62425, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

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

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

EN 50495:2010, *Safety devices required for the safe functioning of equipment with respect to explosion risks*

IFA Report 7/2013e *"Safe drive controls with frequency converters"*
http://www.dguv.de/ifa/Publikationen/Reports-Download/Reports-2013/IFA-Report-7-2013/index-2.jsp

____

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 (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.

3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.

5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

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

Cette deuxième édition annule et remplace la première édition parue en 2007. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) ajout, dans le domaine d'application, de la justification pour laquelle le mode de fonctionnement à faible sollicitation n'est pas couvert par la présente norme

b) ajout des définitions de "*catégorie*" et de "*fonction de sécurité*"

c) “Autres sous-fonctions” réorganisées en “Sous-fonctions de contrôle” et en “Fonctions de sortie”

d) suppression du terme “essai périodique” dans l'ensemble du document dans la mesure où cet essai n'est pas applicable à un *PDS(SR)*

e) remplacement du terme “fonction de sécurité” par “*sous-fonction de sécurité*” dans l'ensemble du document

f) mise à jour des références à la série IEC 61508 Éd. 2010

g) ajout des règles de principe de l'ISO 13849-1 et d'une référence aux tableaux de l'ISO 13849-2

h) 6.1.6 texte remplacé par le Tableau 2

i) 6.1.7 Modification des Circuits intégrés avec redondance sur la puce pour correspondre aux exigences de l'Annexe E de l'IEC 61508-2:2010

j) 6.2.8 Exigences relatives à la conception pour l'immunité thermique d'un *PDS(SR)*

k) 6.2.9 Exigences relatives à la conception pour l'immunité mécanique d'un *PDS(SR)*

l) 6.1.6 *SIL* pour plusieurs *sous-fonctions de sécurité* dans un *PDS*(*SR*)

m) 6.1.7 Circuits intégrés avec redondance sur la puce

n) 6.2.1 Principes de sécurité de base et principes de sécurité éprouvés

o) 6.2.2.1.4 Intervalle entre *essais de diagnostic* pour une tolérance aux défauts supérieure à zéro du matériel

p) 6.2.5.2.7 *Paramétrage du PDS(SR)*

q) 9 Exigences relatives aux essais

r) 9.3 Essais d'immunité électromagnétique (EM)

s) 9.4 Essais d'immunité thermique

t) 9.5 Essais d'immunité mécanique

u) Annexe A Table de tâches séquentielles

v) Annexe D, D.3.16, mise à jour de Capteurs de signal de retour de mouvement et de position

w) Annexe E Exigences d'immunité électromagnétique (EM) pour le *PDS(SR)*

x) Annexe F Estimation de la valeur PFD$_{moy}$ pour une faible sollicitation avec la valeur de la *PFH* donnée

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
22G/332/FDIS	22G/335/RVD

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

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

Une liste de toutes les parties de la série IEC 61800, publiées sous le titre général *Entraînements électriques de puissance à vitesse variable*, peut être consultée sur le site web de l'IEC.

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 l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

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

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.

Les entraînements électriques de puissance à vitesse variable (PDS), utilisables dans des applications relatives à la sécurité (*PDS(SR)*) font partie des appareillages et systèmes les plus importants.

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 des *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 PL et 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 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.

De nombreuses situations témoignent de l'utilisation de systèmes de commande intégrant un *PDS(SR)* en tant qu'élément de mesures de sécurité par exemple qui ont été installés à des fins de réduction du risque. Le verrouillage de protection est un cas typique de protection du personnel dans le cas d'une *situation dangereuse* pour laquelle l'accès à l'emplacement dangereux n'est possible que lorsque les parties tournantes sont à l'arrêt. La présente partie de l'IEC 61800 spécifie une méthodologie permettant d'identifier la contribution apportée par un *PDS(SR)* aux *sous-fonctions* de sécurité identifiées, de réaliser la conception appropriée du *PDS(SR)* et de vérifier qu'elle satisfait aux performances exigées.

Les mesures indiquées permettent 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 défauts systématiques et aléatoires.

ENTRAÎNEMENTS ÉLECTRIQUES DE PUISSANCE À VITESSE VARIABLE –

Partie 5-2: Exigences de sécurité – Fonctionnelle

1 Domaine d'application

La présente partie de l'IEC 61800, qui est une norme de produit, spécifie des exigences et donne des recommandations pour la conception et le développement, l'intégration et la validation des entraînements de puissance relatifs à la sécurité (*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 de normes IEC 61800 à laquelle il est fait référence dans l'IEC 61800-2.

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

NOTE 2 Les autres parties de l'IEC 61800 concernent les spécifications de dimensionnement, la CEM, la sécurité électrique, etc.

La présente Norme internationale est applicable lorsque la sécurité fonctionnelle d'un *PDS(SR)* est revendiquée et que le *PDS(SR)* fonctionne principalement en mode à sollicitation élevée ou en mode continu (voir 3.15).

Bien qu'un *PDS(SR)* puisse fonctionner en mode à faible sollicitation, la présente norme traite plus particulièrement du mode à sollicitation élevée et du mode continu. Les *sous-fonctions* de sécurité mises en œuvre pour le mode à sollicitation élevée ou pour le mode continu peuvent également être utilisées pour le mode à faible sollicitation. Des exigences relatives au mode à faible sollicitation sont données dans la série IEC 61508. Des lignes directrices relatives à l'estimation de la valeur PFD_{moy} (probabilité moyenne de défaillance dangereuse en cas de sollicitation) sont données à l'Annexe F.

La présente partie de l'IEC 61800 expose des considérations relatives à la sécurité des *PDS(SR)* prises dans le cadre de l'IEC 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 parties électriques/électroniques/électroniques programmables (E/E/PE) d'un *PDS(SR)* en liaison avec la performance de sécurité d'une ou des *sous-fonctions de sécurité* d'un PDS.

En se référant aux exigences normatives de la présente partie de l'IEC 61800, les fabricants et les fournisseurs de *PDS(SR)* indiquent aux utilisateurs (intégrateur de système, fabricant original de l'équipement (OEM ou original equipment manufacturer en anglais) la performance de sécurité pour leur équipement. Ceci facilite l'incorporation d'un *PDS(SR)* dans un système de commande relatif à la sécurité appliquant les principes de l'IEC 61508 ou éventuellement ses applications sectorielles spécifiques (par exemple l'IEC 61511, l'IEC 61513, l'IEC 62061 ou l'ISO 13849).

Lorsque les exigences de la présente partie de la série IEC 61800 sont appliquées, les exigences correspondantes de l'IEC 61508 nécessaires à un *PDS(SR)* sont satisfaites.

La présente partie de l'IEC 61800 ne spécifie pas d'exigences pour:

- l'analyse des *dangers* et des risques pour une application particulière;
- l'identification des *sous-fonctions de sécurité* pour l'application concernée;

- l'attribution initiale des *SIL* pour ces *sous-fonctions de sécurité*;
- l'équipement entraîné, à l'exception des aménagements de l'interface;
- des *dangers* secondaires (issus par exemple d'une défaillance d'un procédé de production ou de fabrication);
- les considérations de sécurité électrique, thermique et d'énergie, qui sont couvertes par l'IEC 61800-5-1;
- le procédé de fabrication du *PDS(SR)*;
- la validité des signaux et des commandes du *PDS(SR)*.
- les considérations de sécurité (par exemple cyber sécurité ou sécurité d'accès au *PDS(SR)*

NOTE 3 Les exigences en sécurité fonctionnelle d'un *PDS(SR)* dépendent de l'application et peuvent être considérées comme une partie de l'appréciation globale du risque de l'*installation*. Lorsque le fournisseur du *PDS(SR)* n'est pas responsable de l'équipement entraîné, il incombe au concepteur de l'*installation* de réaliser l'appréciation du risque et de spécifier les exigences fonctionnelles et d'intégrité de sécurité du *PDS(SR)*.

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

La Figure 1 représente l'installation et les parties fonctionnelles d'un *PDS(SR)* qui sont prises en compte dans la présente partie de l'IEC 61800. Il s'agit d'une représentation logique – et non physique – d'un *PDS(SR)*.

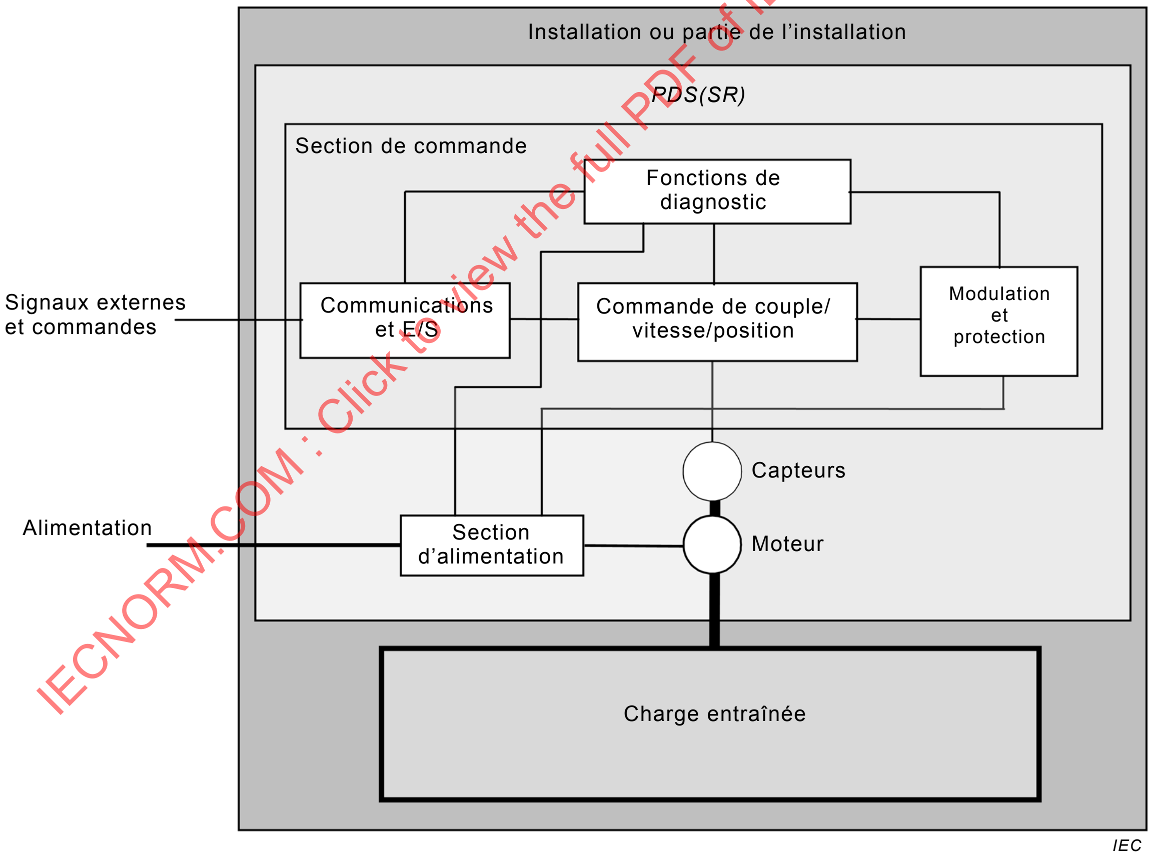


Figure 1 – Installation et parties fonctionnelles d'un *PDS(SR)*

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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).

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

IEC 61000-2-4:2002, *Compatibilité électromagnétique (CEM) – Partie 2-4: Environnement – Niveaux de compatibilité dans les installations industrielles pour les perturbations conduites à basse fréquence*

IEC 61000-4-2:2008, *Compatibilité électromagnétique (CEM) – Partie 4-2: Techniques d'essai et de mesure – Essai d'immunité aux décharges électrostatiques*

IEC 61000-4-3:2010, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques / Associée à l'IEC 61000-4-3 (2006-02), amendement 1 (2007-11) et amendement 2 (2010-03) ou à l'IEC 61000-4-1 Édition 3.1 (2008-04) et amendement 2 (2010-03)*

IEC 61000-4-4:2012, *Compatibilité électromagnétique (CEM) – Partie 4-4: Techniques d'essai et de mesure – Essai d'immunité aux transitoires électriques rapides en salves*

IEC 61000-4-5:2014, *Compatibilité électromagnétique (CEM) – Partie 4-5: Techniques d'essai et de mesure – Essai d'immunité aux ondes de choc*

IEC 61000-4-6:2013, *Compatibilité électromagnétique (CEM) – Partie 4-6: Techniques d'essai et de mesure – Immunité aux perturbations conduites, induites par les champs radioélectriques*

IEC 61000-4-29:2000, *Compatibilité électromagnétique (CEM) – Partie 4-29: Techniques d'essai et de mesure – Essais d'immunité aux creux de tension, coupures brèves et variations de tension sur les accès d'alimentation en courant continu*

IEC 61000-4-34:2009, *Compatibilité électromagnétique (CEM) – Partie 4-29: Techniques d'essai et de mesure – Essais d'immunité aux creux de tension, coupures brèves et variations de tension pour matériel ayant un courant d'alimentation de plus de 16 A par phase; Amendement 1; Corrigendum 1*

IEC 61000-6-7:2014, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

IEC 61400-21:2008, *Éoliennes – Partie 21: Mesurage et évaluation des caractéristiques de qualité de puissance des éoliennes connectées au réseau*

IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

IEC 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

IEC 61508-7:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

IEC 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*

IEC 61800-2:2015, *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*

IEC 61800-3:2012, *Entraînements électriques de puissance à vitesse variable – Partie 3: Exigences de CEM et méthodes d'essais spécifiques*

IEC 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*

IEC 61800-5-1:2007, *Entraînements électriques de puissance à vitesse variable – Partie 5-1: Exigences de sécurité – Électrique, thermique et énergétique*

ISO 13849-1:2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent. Le Tableau 1 donne une liste alphabétique des termes et définitions.

Tableau 1 – Liste alphabétique des termes et définitions

3.1	module d’entraînement principal variateur BDM	3.12	danger	3.23	Sous-fonction(s) de sécurité (d’un PDS(SR))
3.2	catégorie	3.13	installation	3.24	intégrité de sécurité
3.3	module d’entraînement complet équipement variateur CDM	3.14	durée de mission TM	3.25	niveau d’intégrité de sécurité SIL
3.4	défaillance de cause commune	3.15	mode de fonctionnement	3.26	système relatif à la sécurité
3.5	défaillance dangereuse	3.16	PDS(SR)	3.27	Spécification des exigences de sécurité SRS
3.6	couverture du diagnostic DC	3.17	fréquence moyenne de défaillance dangereuse PFH	3.28	capacité SIL
3.7	Essai(s) de diagnostic	3.18	niveau de performance PL	3.29	sous-système
3.8	de sécurité intrinsèque, à sûreté intégrée	3.19	défaillance en sécurité	3.30	défaillance systématique
3.9	état de sécurité intrinsèque, état à sûreté intégrée FS	3.20	proportion de défaillances en sécurité SFF	3.31	intégrité de sécurité systématique
3.10	fonction de réaction au défaut	3.21	état de sécurité	3.32	validation
3.11	sécurité fonctionnelle	3.22	fonction de sécurité	3.33	vérification

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

3.1
module d’entraînement principal
variateur BDM
convertisseur électronique de puissance et commande associée, connecté entre une source d'alimentation électrique et un moteur

Note 1 à l'article: Le *BDM* est capable de transmettre l'énergie de la source d'alimentation électrique au moteur et peut être également capable de transmettre l'énergie produite par le moteur à la source d'alimentation électrique.

Note 2 à l'article: Le *BDM* commande tout ou partie des paramètres suivants relatifs à l'énergie transmise au moteur et à celle fournie par celui-ci: courant, fréquence, tension, vitesse, couple, force.

Note 3 à l'article: L’abréviation «BDM» est dérivée du terme anglais développé correspondant «basic drive module».

[SOURCE: IEC 61800-3:2004/AMD1:2011, 3.1.1]

3.2
catégorie
classification des parties relatives à la sécurité d’un *PDS(SR)* liée à leur résistance aux défauts et à leur comportement consécutif à des défauts et qui est obtenue par l’architecture des parties, la détection des défauts et/ou leur fiabilité

[SOURCE: ISO 13849-1, définition 3.1.2 modifiée] remplacement de “système de commande” par “*PDS(SR)”*

3.3
module d'entraînement complet
MEC
équipement variateur, CDM
module d'entraînement comprenant, de manière non exhaustive, le *BDM* et des composants associés, tels que des dispositifs de protection, des transformateurs et des dispositifs auxiliaires. Toutefois, le moteur et les capteurs mécaniquement couplés à l'arbre du moteur ne sont pas inclus

Note 1 à l'article: L'abréviation "CDM" est dérivée du terme anglais développé correspondant "complete drive module".

[SOURCE: IEC 61800-3:2004/AMD1:2011, 3.1.2]

3.4
défaillance de cause commune
défaillance résultant d'un ou plusieurs événements qui, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance de la *sous-fonction de sécurité*

[SOURCE: IEC 61508-4:2010, 3.6.10 modifiée] remplacement de "conduit à la défaillance du système" par "conduit à la défaillance de la *sous-fonction de sécurité*"

3.5
défaillance dangereuse
défaillance d'un composant et/ou *sous-système* et/ou système ayant une influence sur la mise en œuvre de la *sous-fonction de sécurité* qui:

a) provoque la défaillance d'une *sous-fonction de sécurité* d'un *PDS(SR)* de sorte que l'équipement ou la machine entraîné(e) par le *PDS(SR)* est mis(e) dans un état dangereux ou potentiellement dangereux, ou

b) diminue la probabilité que la *sous-fonction de sécurité* fonctionne correctement

[SOURCE: IEC 61508-4:2010, 3.6.7 modifiée – remplacement de "EUC" par "*PDS(SR)*", suppression de "lorsque c'est nécessaire"]

3.6
couverture du diagnostic
DC
proportion de défaillances dangereuses détectées par les *essais de diagnostic* automatiques

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

Note 2 à l'article: 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 les *sous-systèmes* logiques et/ou le *sous-système* de sortie.

Note 3 à l'article: L'abréviation "DC" est dérivée du terme anglais développé correspondant "diagnostic coverage".

[SOURCE: IEC 61508-4:2010; 3.8.6 modifiée – suppression de "en ligne" dans "essais de diagnostic en ligne"]

3.7
essai de diagnostic
essai visant à détecter d'éventuels défauts ou défaillances et à produire des informations spécifiques au moment de la détection d'un défaut ou d'une défaillance

3.8
de sécurité intrinsèque
à sûreté intégrée
qualifie une entité qui est conçue en vue d'éviter que ses défaillances n'entraînent des pannes dangereuses

[SOURCE: IEC 60500:1998, 821-01-10 modifiée – remplacement de “critiques” par “dangereuses”]

3.9
état de sécurité intrinsèque
état à sûreté intégrée
FS
état de sécurité défini, issu généralement d’une défaillance

Note 1 à l'article: État de sécurité intrinsèque, état à sûreté intégrée (*FS*) est utilisé dans la présente norme en lieu et place de l’état défini (DS ou defined state en anglais) de l’IEC 61000-6-7.

Note 2 à l'article: L’abréviation “FS” est dérivée du terme anglais développé correspondant “fail safe”.

3.10
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 *sous-fonction de sécurité*. La fonction de réaction au défaut vise à maintenir la sécurité de l'*installation* ou à prévenir l'émergence de situations *dangereuses* dans l'*installation*

3.11
sécurité fonctionnelle
sous-ensemble de la sécurité globale se rapportant au *PDS(SR)* qui dépend du fonctionnement correct des *parties du PDS(SR) relatives à la sécurité* et des dispositifs externes de réduction de risque

Note 1 à l'article: 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)*.

[SOURCE: IEC 61508-4:2010, définition 3.1.12 modifiée – remplacement de “l’EUC et au système de commande de l’EUC” par “*PDS(SR)* ”*;* remplacement de “systèmes E/E/PE relatifs à la sécurité et des” par “*parties du PDS(SR) relatives à la sécurité* et des dispositifs externes”]

3.12
danger
phénomène dangereux
source potentielle de dommage

Note 1 à l'article: Ce terme comprend le danger sur des personnes survenant dans un laps de temps très court (par exemple, feu et explosion), mais aussi le danger à long terme sur la santé d’une personne (par exemple, dégagement d’une substance toxique).

[SOURCE: IEC 60050-351:2013, 351-57-01, note 1 à l'article modifiée]

3.13
installation
PDS(SR), équipement entraîné par le *PDS(SR)* et éventuellement un autre équipement (voir Figure 1)

Note 1 à l'article: 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 “action d’installation” est utilisé dans la présente norme.

3.14
durée de mission
TM
durée spécifiée de fonctionnement des parties relatives à la sécurité du *PDS(SR*), cumulée au cours de l'ensemble de son cycle de vie

Note 1 à l'article: L'abréviation "TM" est dérivée du terme anglais développé correspondant "mission time".

3.15
mode de fonctionnement
utilisation prévue d'une *sous-fonction de sécurité*, en rapport avec la fréquence des sollicitations, qui peut être soit en mode à faible sollicitation, soit en mode à sollicitation élevée, soit en mode continu

Note 1 à l'article: Mode à faible sollicitation: lorsque la fréquence des sollicitations de fonctionnement avec une *sous-fonction de sécurité* n'est pas supérieure à une par an.

Note 2 à l'article: Mode à sollicitation élevée et mode continu: lorsque la fréquence des sollicitations de fonctionnement avec une *sous-fonction de sécurité* est supérieure à une par an.

Note 3 à l'article: En général, le *mode de fonctionnement* à faible sollicitation est défini comme inadapté aux applications *PDS(SR*). De ce fait, la présente norme considère que les *PDS(SR*) fonctionnent principalement dans le mode à sollicitation élevée ou le mode continu.

[SOURCE: IEC 61508-4:2010; 3.5.16 modifiée] combinaison de "mode à sollicitation élevée" et ''mode continu"; définition réduite à des indications de durée

3.16
PDS(SR)
entraînement électrique de puissance à vitesse variable, fournissant des *sous-fonctions de sécurité*

3.17
fréquence moyenne de défaillance dangereuse
PFH
fréquence moyenne d'une défaillance dangereuse d'un *PDS(SR)* pour exécuter la *sous-fonction de sécurité* spécifiée pendant une période de temps donnée

Note 1 à l'article: Dans l'IEC 62061, l'abréviation PFH_D est utilisée.

Note 2 à l'article: L'abréviation "PFH" est dérivée du terme anglais développé correspondant "probability of a failure per hour".

[SOURCE: IEC 61508-4:2010; 3.6.19 modifiée – remplacement de "systèmes E/E/PE relatifs à la sécurité" par "*PDS(SR)"*]

3.18
niveau de performance
PL
niveau discret d'aptitude de parties relatives à la sécurité à réaliser une *sous-fonction de sécurité* dans des conditions prévisibles

Note 1 à l'article: L'abréviation «PL» est dérivée du terme anglais développé correspondant «performance level».

[SOURCE: ISO 13849-1:2006, 3.1.23 modifiée – remplacement de "*fonction de sécurité*" par "*sous-fonction de sécurité"*]

3.19
défaillance en sécurité
défaillance d'un composant et/ou *sous-système* et/ou système ayant une influence sur la mise en œuvre de la *sous-fonction de sécurité* qui:

a) conduit au fonctionnement parasite de la *sous-fonction de sécurité* avec la potentialité de mettre le *PDS(SR)* (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité, ou

b) augmente la probabilité du fonctionnement parasite de la *sous-fonction de sécurité* avec la potentialité de mettre le *PDS(SR)* (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité

[SOURCE: IEC 61508-4:2010; 3.6.8 modifiée – remplacement de "élément" par "composant"; remplacement de "EUC" par "*PDS(SR)*"]

3.20
proportion de défaillances en sécurité
SFF
propriété d'un composant et *sous-systèmes* relatifs à la sécurité définie par le rapport des taux de défaillance moyens des défaillances en sécurité et dangereuses détectées et des défaillances en sécurité et dangereuses

Note 1 à l'article: Ce rapport est représenté par l'équation suivante: *SFF* = $(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

Note 2 à l'article: Voir l'Annexe C de l'IEC 61508-2:2010.

Note 3 à l'article: L'abréviation «SFF» est dérivée du terme anglais développé correspondant «Safe failure fraction».

[SOURCE: IEC 61508-4:2010; 3.6.15 modifiée – remplacement de "élément" par "composant et *sous-systèmes*"]

3.21
état de sécurité
état du *PDS(SR)* lorsque la sécurité est réalisée

Note 1 à l'article: Pendant son évolution depuis un état potentiellement dangereux vers un état de sécurité final, le *PDS(SR)* est susceptible de passer par un certain nombre d'états de sécurité intermédiaires.

[SOURCE: IEC 61508-4: 2010; 3.1.13 modifiée – remplacement de "EUC" par "*PDS(SR)*"]

3.22
fonction de sécurité
fonction à réaliser par un système relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'équipement ou de la machine entraîné(e) par le *PDS(SR)*, par rapport à un événement dangereux spécifique

[SOURCE: IEC 61508-4:2010; 3.5.1 modifiée – suppression de " E/E/PE"; remplacement de "EUC" par "l'équipement ou de la machine entraîné(e) par le *PDS(SR)*"]

3.23
***sous-fonction 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(nt) à maintenir la sécurité de l'*installation* ou à prévenir l'émergence de toute condition *dangereuse* dans l'*installation*

Note 1 à l'article: Dans de rares cas, la fonction de sécurité de l'application complète est exclusivement mise en œuvre au sein du *PDS(SR)*. Dans ce cas, la fonction de sécurité est toujours appelée "*sous-fonction de sécurité*" dans la présente norme (par exemple, une SLS toujours active sans intervention extérieure).

3.24
intégrité de sécurité
probabilité pour qu'un *PDS(SR)* exécute de manière satisfaisante une *sous-fonction de sécurité* spécifiée dans toutes les conditions énoncées et dans une période de temps spécifiée

Note 1 à l'article: Plus le niveau d'*intégrité de sécurité* du ou des *PDS(SR)* est élevé, plus la probabilité d'une défaillance du ou des *PDS(SR)* dans l'exécution de la *sous-fonction de sécurité* spécifiée est faible.

Note 2 à l'article: L'*intégrité de sécurité* peut être différente pour chaque *sous-fonction de sécurité* réalisée par le *PDS(SR)*.

[SOURCE: IEC 61508-4:2010; 3.5.4 modifiée – remplacement de “système E/E/PE relatif à la sécurité” par “*PDS(SR)*”]

3.25
niveau d'intégrité de sécurité
SIL
niveau discret (un parmi trois possibles) permettant de spécifier les exigences concernant l'*intégrité de sécurité* d’une *sous-fonction de sécurité* attribuée (tout ou partie) à un *PDS(SR)*

Note 1 à l'article: Le niveau 3 d'*intégrité de sécurité* possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas.

Note 2 à l'article: 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 l’IEC 61508.

Note 3 à l'article: Plusieurs conventions d’écriture sont utilisées pour *SIL*x. Dans l’ensemble du présent document, c’est la forme *SIL* × qui est utilisée.

Note 4 à l'article: L’abréviation “SIL” est dérivée du terme anglais développé correspondant “safety integrity level”.

[SOURCE: IEC 61508-4:2010; 3.5.8 modifiée – remplacement de “correspondant à une plage de valeurs d’intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas” par “permettant de spécifier les exigences concernant l'*intégrité de sécurité* d’une *sous-fonction de sécurité* attribuée (tout ou partie) à un *PDS(SR)*”]

3.26
système relatif à la sécurité
système désigné qui, à la fois:

- met en œuvre les fonctions de sécurité requises pour atteindre ou maintenir un état de sécurité de l’équipement ou de la machine entraîné(e) par le *PDS(SR)*;
- est prévu pour atteindre, par lui-même ou grâce à d’autres dispositifs externes de réduction de risque, l’intégrité de sécurité nécessaire pour les fonctions de sécurité requises

[SOURCE: IEC 61508-4:2010; 3.4.1 modifiée – remplacement de “EUC” par “l’équipement ou de la machine entraîné(e) par le *PDS(SR)*”; suppression de “E/E/PE”]

3.27
spécification des exigences de sécurité
SRS
spécification qui contient l'ensemble des exigences concernant les *sous-fonctions de sécurité* à exécuter par le *PDS(SR)*

Note 1 à l'article: L’abréviation «SRS» est dérivée du terme anglais développé correspondant «safety requirements specification»

3.28
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 1 à l'article: Une *capacité SIL* différente peut être associée à chacune des *sous-fonctions de sécurité* désignées qu'un *PDS(SR)* est censé assurer.

Note 2 à l'article: La capacité *SIL* inclut la capabilité systématique, la satisfaction aux contraintes architecturales et le taux de défaillance du matériel ou la valeur de la PFH.

3.29
sous-système
partie de la conception architecturale de haut niveau d'un *système relatif à la sécurité* où une défaillance du sous-système conduit à une défaillance d'une *fonction relative à la sécurité*

Note 1 à l'article: Un *PDS(SR)* peut être un *sous-système* en soi, ou être constitué de plusieurs *sous-systèmes* distincts qui, une fois assemblés, exécutent la *sous-fonction de sécurité* à l'étude. Un *sous-système* peut disposer de plusieurs canaux.

Note 2 à l'article: 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).

3.30
défaillance systématique
défaillance liée 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 1 à l'article: Parmi les exemples de causes de défaillances systématiques figurent les erreurs humaines dans:

- la *spécification des exigences de sécurité*;
- la conception, fabrication, action d'installation et exploitation du matériel;
- la conception et la mise en œuvre du logiciel.

Note 2 à l'article: Dans la présente norme, les défaillances d'un système relatif à la sécurité sont classées en défaillances aléatoires du matériel ou en défaillances systématiques

[SOURCE: IEC 61508-4:2010; 3.6.6]

3.31
intégrité de sécurité systématique
partie de l'*intégrité de sécurité* d'un *système relatif à la sécurité* qui se rapporte aux *défaillances systématiques* dans un mode de défaillance dangereux

Note 1 à l'article: L'*intégrité de sécurité systématique* ne peut normalement pas être quantifiée (à la différence de l'intégrité de sécurité du matériel qui, habituellement, peut l'être).

[SOURCE: IEC 61508-4:2010; 3.5.6]

3.32
validation
confirmation, par examen et apport de preuves tangibles, que les exigences particulières pour un usage spécifique prévu sont satisfaites

Note 1 à l'article: La *validation* est l'activité qui consiste à démontrer que le *PDS(SR)*, avant ou après l'action d'installation, correspond en tout point à la *spécification des exigences de sécurité*.

[SOURCE: IEC 61508-4:2010; 3.8.2, Note 1 à l'article modifiée]

3.33
vérification
confirmation, par examen et apport de preuves tangibles, que les exigences ont été satisfaites

[SOURCE: IEC 61508-4:2010; 3.8.1, modifiée – Note 1 à l'article enlevée]

4 *Sous-fonctions de sécurité* désignées

4.1 Généralités

Cet article décrit les fonctions d'un *PDS(SR)* qui peuvent être désignées comme relatives à la sécurité par le fournisseur du *PDS(SR)*. Cependant, la liste des *sous-fonctions de sécurité* désignées dans cet article n'est pas exhaustive. Les détails de mise en œuvre des *sous-fonctions de sécurité* de base et des *sous-fonctions de sécurité* complexes comprenant plusieurs *sous-fonctions de sécurité* de base, n'ont pas été fournis en raison du grand nombre de possibilités existant. Dans certains cas, d'autres *systèmes relatifs à la sécurité*, externes au *PDS(SR)* (par exemple un frein mécanique), peuvent être nécessaires pour maintenir la sécurité en l'absence de puissance électrique.

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

Chaque *sous-fonction de sécurité* peut inclure des entrées et/ou des sorties sûres afin d'établir la communication nécessaire avec d'autres fonctions, *sous-systèmes* ou systèmes (qui peuvent ou non être relatifs à la sécurité) ou de les activer.

Certaines *sous-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 (pertinente uniquement pour les fonctions de contrôle):

  la fonction de réaction quand une violation de limites est détectée durant le fonctionnement correct de la *sous-fonction de sécurité*; et
- la *fonction de réaction au défaut* (pertinente pour toutes les *sous-fonctions de sécurité*):

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

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

La sélection de la fonction de réaction appropriée doit tenir compte du fait que des parties du *PDS(SR)* peuvent ne pas fonctionner.

Les exigences liées au temps, pour les actions exigées après une détection de défaut, sont données par la *spécification des exigences de sécurité* (voir 5.5).

Les noms des *sous-fonctions de sécurité* comportent les mots «sûr(e)» ou «en toute sécurité» afin d'indiquer que ces fonctions peuvent être utilisées dans une application relative à la sécurité sur les bases d'une analyse (c'est-à-dire une analyse du risque) de l'application spécifique, permettant ainsi au *PDS(SR)* de mettre en œuvre les fonctions de sécurité et assurer leur intégrité

NOTE Pour des exemples détaillés des sous-fonctions du *PDS(SR)* spécifiées dans le présent article, voir la Bibliographie (rapport IFA 7/2013e).

4.2 *Sous-fonctions de sécurité*

4.2.1 Généralités

Dans la plupart des cas, les *fonctions de sécurité* du *PDS(SR)* font partie des *fonctions de sécurité* d'une application, par conséquent les *fonctions de sécurité* du *PDS(SR)* sont appelées *sous-fonctions de sécurité* dans ce document. La Figure 2 donne un exemple de *fonction de sécurité* comprenant des *sous-fonctions de sécurité*:

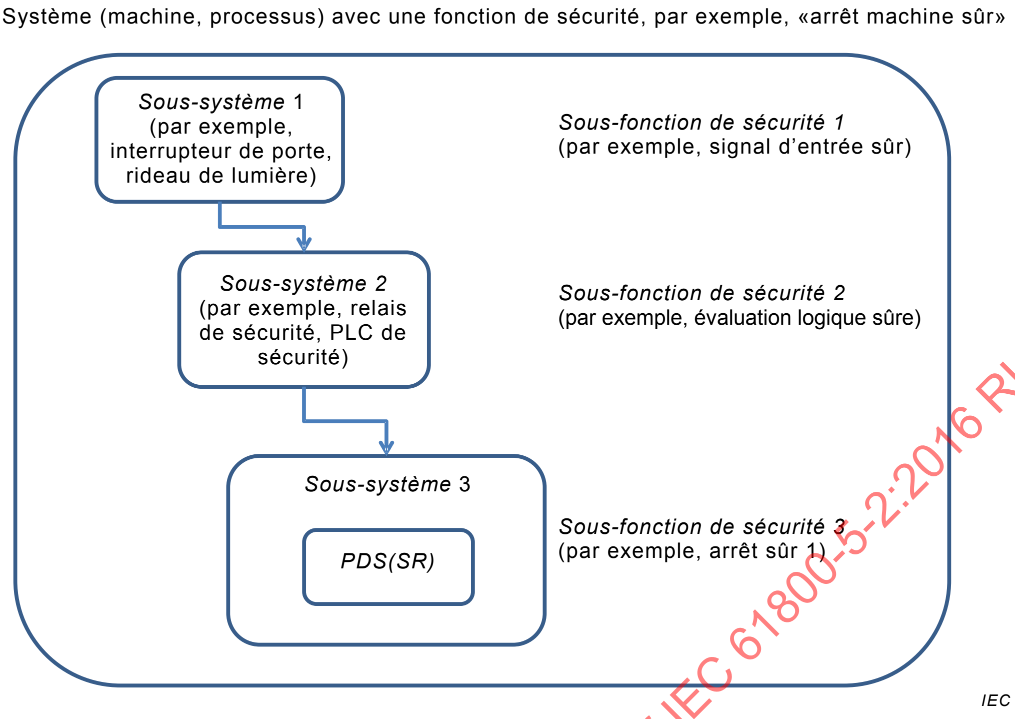

Système (machine, processus) avec une fonction de sécurité, par exemple, «arrêt machine sûr»
Sous-système 1 (par exemple, interrupteur de porte, rideau de lumière)
Sous-système 2 (par exemple, relais de sécurité, PLC de sécurité)
Sous-système 3
PDS(SR)
Sous-fonction de sécurité 1 (par exemple, signal d'entrée sûr)
Sous-fonction de sécurité 2 (par exemple, évaluation logique sûre)
Sous-fonction de sécurité 3 (par exemple, arrêt sûr 1)
IEC

Figure 2 – *Fonction de sécurité* comprenant des *sous-fonctions de sécurité*

NOTE Pour de plus amples informations sur les *sous-fonctions de sécurité*, voir le rapport IFA 7/2013e: “Safe drive controls with frequency converters” (voir Bibliographie).

4.2.2 Valeurs limites

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

NOTE La spécification de toute valeur limite peut prendre en compte un éventuel dépassement de la valeur limite en cas de violation de cette limite. Par exemple, la spécification de(s) valeur(s) limite(s) de position en 4.2.4.9 peut prendre en compte la(les) distance(s) maximale(s) permise(s) pour le dépassement.

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

4.2.3 Fonctions d’arrêt

4.2.3.1 Généralités

Diverses méthodes d’arrêt sont applicables à chaque type de *PDS(SR).*

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.

NOTE Lors de l’application de fonctions d’arrêt de sécurité pour des fonctions telles que la prévention d’un démarrage ou d’un arrêt d’urgence intempestif, les normes correspondantes peuvent être prises en considération, par exemple, IEC 60204-1, ISO 13850, ISO 12100, ISO 14118.

Les exigences particulières à la réalisation de l’arrêt peuvent être spécifiées par les clients du fabricant du *PDS(SR)*. En pratique, les exemples suivants de fonctions d’arrêt sont souvent utilisés.

4.2.3.2 Suppression sûre du couple (STO ou safe torque off en anglais)

Cette fonction empêche toute délivrance de la puissance de génération de forces au moteur.

Cette *sous-fonction de sécurité* correspond à un arrêt non contrôlé conformément à l'arrêt de catégorie 0 de l'IEC 60204-1.

NOTE 1 Cette *sous-fonction de sécurité* peut être utilisée lorsque la suppression de la puissance est exigée afin d'éviter un démarrage intempestif conformément à l'ISO 14118.

NOTE 2 En présence d'influences externes (par exemple, la chute de charges suspendues), des mesures complémentaires (par exemple, des freins mécaniques) peuvent être nécessaires afin de prévenir tout *danger*.

NOTE 3 Des moyens électroniques et certains contacteurs ne conviennent pas pour la protection contre des chocs électriques.

NOTE 4 La fonction étant active, un mouvement limité demeure possible en cas de défaillance de la section d'alimentation du *PDS(SR)*.

4.2.3.3 Arrêt sûr 1 (SS1)

Cette fonction est spécifiée soit comme:

a) Arrêt sûr 1 à commande de décélération

SS1-d

initie et commande le taux de décélération du moteur dans des limites choisies pour arrêter le moteur et exécute la fonction STO (voir 4.2.3.2) lorsque la vitesse du moteur est en dessous d'une limite spécifiée; soit

b) Arrêt sûr 1 à contrôle de rampe

SS1-r

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

c) Arrêt sûr 1 à contrôle du temps

SS1-t

initie la décélération du moteur et exécute la fonction STO après écoulement d'un temps spécifique à l'application.

Cette *sous-fonction de sécurité* correspond à un arrêt contrôlé conformément à l'arrêt de catégorie 1 de l'IEC 60204-1.

NOTE L'arrêt contrôlé de SS1-t peut échouer de manière non détectée, par conséquent SS1-t ne peut pas être appliqué si cette défaillance peut entraîner une situation dangereuse dans le cadre de l'application finale.

4.2.3.4 Arrêt sûr 2 (SS2)

Cette fonction est spécifiée soit comme:

a) Arrêt sûr 2 à commande de décélération

SS2-d

initie et commande le taux de décélération du moteur dans des limites choisies pour arrêter le moteur et exécute la fonction «maintien sûr à l'arrêt» (voir 4.2.4.1) lorsque la vitesse du moteur est en dessous d'une limite spécifiée; soit

b) Arrêt sûr 2 à contrôle de rampe

SS2-r

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

c) Arrêt sûr 2 à contrôle du temps

SS2-t

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

Cette *sous-fonction de sécurité* SS2 correspond à un arrêt contrôlé conformément à l'arrêt de catégorie 2 de l'IEC 60204-1.

NOTE L'arrêt contrôlé de SS2-t peut échouer de manière non détectée, par conséquent, l'arrêt sûr SS2-t ne peut pas être appliqué si cette défaillance peut entraîner une situation dangereuse dans le cadre de l'application finale.

4.2.4 Fonctions de contrôle

4.2.4.1 Généralités

Dans les descriptions de fonctions suivantes, le terme "empêche" indique qu'il n'y a qu'une seule limite et le terme "maintient" indique qu'il existe une limite supérieure et une limite inférieure. Dans les autres cas, aucune différence n'est faite.

4.2.4.2 Maintien sûr à l'arrêt (SOS ou safe operating stop en anglais)

Cette fonction empêche le moteur de dépasser une valeur 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 œuvre au moyen d'un *PDS(SR)* sans freins externes (par exemple mécaniques).

4.2.4.3 Limitation sûre de l'accélération (SLA ou safely-limited acceleration en anglais)

Cette fonction empêche le moteur de dépasser la limite spécifiée d'accélération et/ou de décélération.

4.2.4.4 Fenêtre d'accélération sûre (SAR ou safe acceleration range en anglais)

Cette fonction maintient l'accélération et/ou la décélération du moteur dans les limites spécifiées.

4.2.4.5 Limitation sûre de la vitesse (SLS ou safely-limited speed en anglais)

Cette fonction empêche le moteur de dépasser la limite spécifiée de la vitesse.

4.2.4.6 Fenêtre de vitesse sûre (SSR ou safe speed range en anglais)

Cette fonction maintient la vitesse du moteur dans les limites spécifiées.

4.2.4.7 Limitation sûre du couple (SLT ou safely-limited torque en anglais)

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

4.2.4.8 Plage de couple sûre (STR ou safe torque range en anglais)

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

4.2.4.9 Limitation sûre de la position (SLP ou safely-limited position en anglais)

Cette fonction empêche l’arbre moteur (ou l'entraînement, quand un moteur linéaire est utilisé) de dépasser la ou les limites de position spécifiées.

4.2.4.10 Limitation sûre de l'incrément (SLI ou safely-limited increment en anglais)

Cette fonction empêche l'arbre moteur (ou l'entraînement, quand un moteur linéaire est utilisé) de dépasser la limite spécifiée pour l'incrément de position.

NOTE Cette fonction permet au *PDS(SR)* de contrôler 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 contrôlée en toute sécurité.
- après accomplissement de la course exigée pour cet incrément, le moteur est arrêté et est maintenu dans cet état, de façon appropriée à l’application.

4.2.4.11 Sens de rotation sûr (SDI ou safe direction en anglais)

Cette fonction empêche l’arbre moteur de tourner dans le sens non prévu au-delà d’une limite définie.

4.2.4.12 Température moteur sûre (SMT ou safe motor temperature en anglais)

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

NOTE La *sous-fonction de sécurité* SMT peut être utilisée pour la protection contre la surchauffe d’un moteur en atmosphère explosive. Cependant, elle n’assure pas de protection contre d’autres risques tels que les étincelles. Pour de plus amples informations, voir la série de normes IEC 60079. Des informations générales pour l’utilisation d’un *PDS(SR)* dans des applications en atmosphère explosive sont fournies dans l’IEC 61800-2:2015.

4.2.4.13 Position sûre de la came (SCA ou safe cam en anglais)

Cette fonction fournit un signal de sortie sûr pour indiquer que la position de l’arbre moteur se situe dans une plage spécifiée.

4.2.4.14 Contrôle sûr de la vitesse (SSM ou safe speed monitor en anglais)

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

4.2.5 Fonctions de sortie – Commande sûre des freins (SBC)

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

5 Gestion de la *sécurité fonctionnelle*

5.1 Objectif

Le premier objectif de cet article est de spécifier les responsabilités de gestion de la *sécurité fonctionnelle* et des activités à effectuer par les personnes responsables.

Le second objectif de cet article est de présenter le cycle de vie du développement du *PDS(SR)* et de donner une vue d’ensemble de ses phases.

NOTE Les mesures organisationnelles traitées dans cet article prévoient la mise en œuvre effective des exigences techniques et ont pour unique objectif la réalisation et le maintien de la *sécurité fonctionnelle* des systèmes du *PDS(SR)*. Ces mesures sont distinctes et séparées des mesures de santé et de sécurité générales nécessaires à l’obtention de la sécurité sur le lieu de travail.

5.2 Exigences concernant la gestion de la *sécurité fonctionnelle*

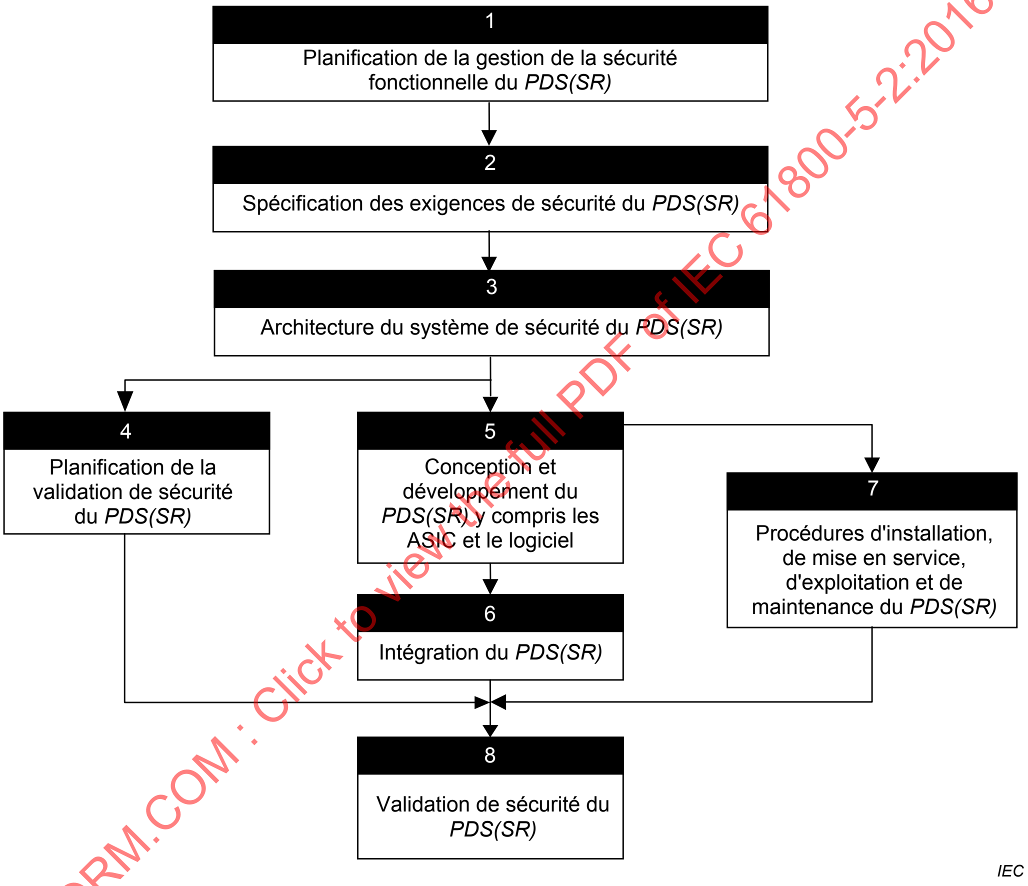
Les exigences de l'Article 6 de l'IEC 61508-1:2010 s'appliquent.

5.3 Cycle de vie du développement du *PDS(SR)*

La Figure 3 représente le cycle de vie du développement du *PDS(SR)* avec des références croisées avec les paragraphes appropriés de la présente norme, ce cycle étant composé des phases 1 à 8.

NOTE Ceci correspond aux phases de spécification des exigences de sécurité (phase 9) et de réalisation (phase 10) du cycle de vie de sécurité global de l'IEC 61508-1:2010.

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


1
Planification de la gestion de la sécurité fonctionnelle du *PDS(SR)*
2
Spécification des exigences de sécurité du *PDS(SR)*
3
Architecture du système de sécurité du *PDS(SR)*
4
Planification de la validation de sécurité du *PDS(SR)*
5
Conception et développement du *PDS(SR)* y compris les ASIC et le logiciel
6
Intégration du *PDS(SR)*
7
Procédures d'installation, de mise en service, d'exploitation et de maintenance du *PDS(SR)*
8
Validation de sécurité du *PDS(SR)*
IEC

Pour la phase 1, voir 5.4. (phase 9 – voir NOTE)	Pour la phase 2, voir 5.5. (phase 9 – voir NOTE)	Pour la phase 3, voir 5.6. (phase 10.1 – voir NOTE)	Pour la phase 4, voir 5.4 e) (phase 10.2 – voir NOTE)
Pour la phase 5, voir l'Article 6 (phase 10.3 – voir NOTE)	Pour la phase 6, voir 6.5 (phase 10.4 – voir NOTE)	Pour la phase 7, voir l'Article 7 (phase 10.5 – voir NOTE)	Pour la phase 8, voir l'Article 8 (phase 10.8 – voir NOTE)

NOTE Phase correspondante du cycle de vie de sécurité global de l'IEC 61508-1:2010.

Figure 3 – Cycle de vie du développement du *PDS(SR)*

5.4 Planification de la gestion de la *sécurité fonctionnelle* du *PDS(SR*

Un plan doit être généré et mis à jour si nécessaire tout au long du développement complet du *PDS(SR)*. Il doit définir les activités exigées pour satisfaire aux Articles 5 à 10 et spécifier les personnes et leurs compétences, le ou les services, ou la ou les organisations responsables pour accomplir ces activités.

En particulier, le plan doit prendre en compte ou comprendre les éléments suivants en fonction de la complexité du *PDS(SR)*.

a) Génération de la *spécification des exigences de sécurité* (voir 5.5), incluant des facteurs tels que:

   – le personnel responsable de la génération et du maintien de la *spécification des exigences de sécurité;*

   – le choix de méthodes permettant d'éviter de commettre des erreurs durant la génération de la *spécification des exigences de sécurité* (voir Annexe B de l'IEC 61508-2:2010);

   – la prise en compte des exigences issues de directives et de normes pour des applications cibles spécifiques du *PDS(SR*);

   – 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) Génération de la spécification de l'architecture du système de sécurité (voir 5.6), incluant des facteurs tels que:

   – le personnel responsable de la génération et du maintien de la spécification de l'architecture du système de sécurité;

   – le choix de méthodes permettant d'éviter de commettre des erreurs durant la génération de la spécification de l'architecture du système de sécurité (voir Annexe B de l'IEC 61508-2:2010);

   – la prise en compte des exigences issues de directives et de normes pour des applications cibles spécifiques du *PDS(SR*);

   – le personnel responsable de la *vérification* de la spécification de l'architecture du système de sécurité;

   – le processus pour la modification de la spécification de l'architecture du système de sécurité lorsque le développement a débuté.

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

   – le personnel responsable de la conception et du développement;

   – la sélection des méthodes de développement de produit et de gestion de projet (voir B.1.1 de l'IEC 61508-7:2010);

   – la prise en compte des directives et des normes de *sécurité fonctionnelle* applicables à la conception d'équipements incorporant le *PDS(SR*) d'une application cible, tels qu'un équipement de contrôle de processus ou une machine (par exemple, ISO 13849-1 et IEC 62061);

   – la méthode de documentation de projet (voir B.1.2 de l'IEC 61508-7:2010);

   – l'application des techniques structurées de conception (voir B.3.2 de l'IEC 61508-7:2010);

   – l'application de techniques de modularisation (voir B.3.4 de l'IEC 61508-7:2010);

   – l'utilisation d'outils de conception basés sur des méthodes informatisées (voir B.3.5 de l'IEC 61508-7:2010);

   – la méthodologie de *vérification* de la conception;

   – la gestion de modifications en conception (aussi bien matérielle que logicielle).

d) Un plan de *vérification* de la ou des *sous-fonctions de sécurité* incluant des facteurs tels que:

   – le personnel responsable de la *vérification*;

   – la sélection des stratégies, des techniques et des outils de *vérification*;

   – la sélection et la documentation des activités de *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*.

e) Un plan de *validation* de la ou des *sous-fonctions de sécurité* comprenant:

- le personnel responsable des essais de *validation*;
- l'identification des modes de fonctionnement pertinents pour le *PDS(SR*);
- les procédures à appliquer afin de valider la mise en œuvre correcte de chaque *sous-fonction de sécurité* du *PDS(SR)*, ainsi que les critères de réussite/échec pour la réalisation des essais;
- les procédures à appliquer afin de valider l'*intégrité de sécurité* exigée de chaque *sous-fonction de sécurité* du *PDS(SR)*, ainsi que les critères de réussite/échec pour la réalisation des essais;
- l'environnement exigé pour les essais à effectuer, y compris tous les outils et équipements nécessaires (planifier également les outils et équipements qu'il convient d'étalonner);
- les procédures d'évaluation des essais (avec justifications);
- les procédures d'essai et les critères de performance à appliquer pour valider les limites d'immunité électromagnétique spécifiées;
- les actions à mettre en œuvre dans l'éventualité d'un échec à satisfaire aux critères d'acceptation.

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

- le personnel responsable de la documentation de l'utilisateur;
- une liste d'informations significatives relatives à la sécurité qui doivent être fournies;
- le processus de revue pour s'assurer de l'exactitude de la documentation.

g) Lorsqu'une évaluation est exigée (voir l'Article 8 de l'IEC 61508-1:2010), un plan d'évaluation de la *sécurité fonctionnelle*, fournissant toutes les informations nécessaires pour faciliter une évaluation efficace et comprenant:

- le domaine d'application de l'évaluation de la *sécurité fonctionnelle*;
- les organisations impliquées;
- les ressources exigées;
- les personnes en charge de l'évaluation de la *sécurité fonctionnelle*;
- le niveau d'indépendance des personnes en charge de l'évaluation de la *sécurité fonctionnelle*;
- la compétence de chaque personne impliquée dans l'évaluation de la *sécurité fonctionnelle*;
- les résultats de l'évaluation de la *sécurité fonctionnelle*;
- la façon dont l'évaluation de la *sécurité fonctionnelle* est associée à d'autres évaluations de la *sécurité fonctionnelle*, et la manière selon laquelle elle doit y être intégrée le cas échéant;
- les exigences de réalisation d'une analyse d'impact afin de déterminer quelles parties de l'évaluation doivent être répétées dans le cas d'une modification (voir également 7.16.2 de l'IEC 61508-1:2010)

Pour établir le domaine d'application de chaque évaluation de la *sécurité fonctionnelle*, il est nécessaire de spécifier les documents et leur statut de révision, qui doivent être utilisés comme éléments d'entrée de chaque activité d'évaluation.

NOTE Le plan peut être établi par les personnes en charge de l'évaluation de la *sécurité fonctionnelle* ou par les personnes en charge de la gestion de la *sécurité fonctionnelle*, ou peut être partagé entre elles.

5.5 Spécification des exigences de sécurité (*SRS*) pour un *PDS(SR*)

5.5.1 Généralités

Une *spécification des exigences de sécurité* pour un *PDS(SR*) doit être documentée et doit comprendre:

- une spécification des exigences des *sous-fonctions de sécurité* (voir 5.5.2); et
- une spécification des exigences d'*intégrité de sécurité* (voir 5.5.3).

Ces spécifications doivent être exprimées et structurées selon les critères suivants:

- être claires, précises, non ambiguës, réalisables, vérifiables, vérifiables par essai et actualisables;
- être rédigées afin d'en faciliter la compréhension par les personnes susceptibles d'utiliser les informations à tout stade du cycle de vie de sécurité du *PDS(SR)*;
- être formulées dans un langage naturel ou formel et/ou sous forme de schémas logiques et séquentiels ou de diagrammes cause-effet qui définissent les *sous-fonctions de sécurité* nécessaires, chaque *sous-fonction de sécurité* étant définie de manière individuelle.

Afin d'éviter de commettre des erreurs durant la compilation de ces spécifications, des mesures et des techniques appropriées doivent être employées (voir le Tableau B.1 de l'IEC 61508-2:2010).

Les exigences concernant les matériels et les logiciels relatifs à la sécurité doivent faire l'objet d'une revue afin de s'assurer que leur spécification est appropriée.

5.5.2 Spécification des exigences des *sous-fonctions de sécurité*

La spécification des exigences des *sous-fonctions de sécurité* doit fournir suffisamment d'exigences complètes et détaillées pour la conception et le développement du *PDS(SR*).

La spécification des exigences des *sous-fonctions de sécurité* doit décrire, selon le cas:

a) toutes les *sous-fonctions de sécurité* à exécuter;

b) des exigences complètes et détaillées suffisantes pour la conception et le développement du *PDS(SR*) incluant toutes les exigences normatives à satisfaire;

   NOTE Des exigences telles que les mesures choisies d'évitement et de maîtrise des défauts et les mesures et techniques choisies pour la conception et les essais des logiciels, etc., peuvent figurer dans la spécification des exigences des *sous-fonctions de sécurité*.

c) le *mode de fonctionnement* applicable concernant la *sécurité fonctionnelle*;

d) la manière selon laquelle il est prévu que le *PDS(SR)* atteigne ou maintienne un état de sécurité pour les applications prévues;

e) les modes de fonctionnement du *PDS(SR*) et son *installation* – par exemple, les réglages, le démarrage, la maintenance, le fonctionnement normal prévu;

f) tous les modes de comportement exigés du *PDS(SR*);

g) les fonctions prioritaires actives simultanément susceptibles de créer une situation de conflit;

h) la ou les actions exigées lorsqu'une violation des limites est détectée durant le fonctionnement normal d'une *sous-fonction de sécurité* (c'est-à-dire la réaction à la violation de limites, voir 4.1);

i) la ou les *fonctions de réaction au défaut* (voir 4.1 et 6.3);

j) le temps maximal de réaction au défaut nécessaire afin d'activer la réaction au défaut correspondante à réaliser avant qu'un *danger* ne se produise dans les applications prévues (nécessaire seulement si des *essais de diagnostic* sont réalisés pour atteindre la *capacité SIL*);

k) le temps de réponse maximal de chaque fonction relative à la sécurité (c'est-à-dire les *fonctions de réaction au défaut* et de sécurité (voir 6.3);

l) 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.

m) 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 (c'est-à-dire les *fonctions de réaction au défaut* et de sécurité);

n) toutes les interfaces, nécessaires pour la *sécurité fonctionnelle*, entre le *PDS(SR)* et les autres systèmes éventuels (associées directement à l'intérieur ou à l'extérieur de l'*installation*).

5.5.3 Spécification des exigences d'*intégrité de sécurité*

La spécification des exigences d'*intégrité de sécurité* relative à un *PDS(SR)* doit comprendre:

a) pour chaque fonction relative à la sécurité (ou groupe de fonctions relatives à la sécurité utilisées simultanément), une *capacité SIL* (ou *SIL*) ainsi qu'une limite supérieure de la valeur de la *PFH*.

NOTE 1 La *capacité SIL* est pertinente si le *PDS(SR)* doit être défini comme un composant qui met en œuvre une *sous-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 inférieure à l'objectif chiffré de défaillance associé au *SIL* attribué à la *sous-fonction de sécurité* complète. Toutefois, elle peut également être supérieure si le *PDS(SR)* doit être utilisé afin d'exécuter la *sous-fonction de sécurité* dans une configuration redondante, avec d'autres composants.

NOTE 3 Lorsqu'une *sous-fonction de sécurité* est entièrement exécutée au sein d'un *PDS(SR)*, la spécification des exigences d'*intégrité de sécurité* n'identifie pas une *capacité SIL* mais un *SIL*.

NOTE 4 En cas d'utilisation de matériel courant pour exécuter plusieurs *sous-fonctions de sécurité* simultanément, la probabilité de défaillance matérielle dangereuse aléatoire du matériel courant peut être prise en considération seulement une fois lors de la détermination de la probabilité globale de défaillance matérielle dangereuse aléatoire.

NOTE 5 En ce qui concerne un *PDS(SR)* comportant plusieurs axes, lorsqu'une *sous-fonction de sécurité* est nécessaire sur plusieurs axes, la probabilité de défaillance matérielle dangereuse aléatoire du matériel courant peut être prise en considération seulement une fois lors de la détermination de la probabilité globale de défaillance matérielle dangereuse aléatoire.

b) la *durée de mission* exigée;

c) 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 action d'installation, son fonctionnement et sa maintenance;

NOTE 6 Cette information peut avoir été obtenue pour satisfaire aux exigences de l'IEC 61800-1, l'IEC 61800-2 ou l'IEC 61800-4. Dans ce cas, il n'est pas nécessaire d'apporter d'autres précisions.

d) toute exigence relative à l'augmentation de l'immunité électromagnétique (voir 6.2.6);

e) les conditions aux limites et de contraintes pour la réalisation du *PDS(SR)* en raison de la possibilité de *défaillances de cause commune*;

f) les mesures d'assurance/contrôle de la qualité nécessaires pour la gestion de la sécurité fonctionnelle (voir Article 6 de l'IEC 61508-1: 2010).

5.6 Spécification de l'architecture du système de sécurité du *PDS(SR)*

5.6.1 Généralités

5.6.1.1 L'objectif de la spécification de l'architecture du système de sécurité est de préciser la décomposition architecturale du *PDS(SR)* et les exigences concernant les *sous-systèmes* et parties de *sous-systèmes* obtenus. (voir Annexe A)

NOTE 1 La spécification de l'architecture du système de sécurité est normalement déduite de la spécification des exigences de sécurité du *PDS(SR)* en décomposant les *sous-fonctions de sécurité* et en attribuant les parties des *sous-fonctions de sécurité* aux *sous-systèmes* (par exemple, logique de *sous-fonction de sécurité*, circuits d'entrée/sortie, alimentation, logiciel). La représentation du *PDS(SR)* sous forme de *sous-système*s décrit le *PDS(SR)* à un niveau architectural qui permet de spécifier les exigences concernant ces *sous-systèmes*. Les exigences peuvent être incluses dans la spécification de l'architecture du système de sécurité ou être conservées à part et référencées par la spécification. Les *sous-systèmes* peuvent être par ailleurs décomposés en parties afin de satisfaire aux exigences de conception et de développement.

NOTE 2 Une approche plus générale de ce type de spécification est donnée dans l'IEC 61508-2: 2010 sous forme de spécification des exigences relatives à la conception d'un système E/E/PE.

5.6.1.2 La description des *sous-systèmes* et des parties et les exigences respectives doivent être exprimées et structurées selon les critères suivants:

- être claires, précises, non ambiguës, réalisables, vérifiables, vérifiables par essai et actualisables;
- être rédigées afin d'en faciliter la compréhension par les personnes susceptibles d'utiliser les informations à tout stade du cycle de vie de sécurité du *PDS(SR)*;
- être traçables par rapport à la spécification des *exigences de sécurité* du *PDS(SR)*.

5.6.2 Exigences concernant la spécification de l'architecture du système de sécurité

5.6.2.1 La spécification de l'architecture du système de sécurité doit comprendre les exigences de conception relatives aux *sous-fonctions de sécurité* et à l'*intégrité de sécurité*.

5.6.2.2 La spécification de l'architecture du système de sécurité doit comprendre les détails de tous les matériels et logiciels nécessaires à l'exécution des *sous-fonctions de sécurité* exigées, comme précisé par la *spécification des exigences des sous-fonctions de sécurité* du *PDS(SR)* (voir 5.5.2). L'architecture doit inclure, pour chaque *sous-fonction de sécurité*:

a) les exigences concernant les *sous-systèmes* et leurs parties selon le cas;

b) les exigences concernant l'intégration des *sous-systèmes* et des parties afin de satisfaire à la spécification des exigences de sécurité du *PDS(SR)*;

c) la performance de débit qui permet de satisfaire aux exigences du temps de réponse;

d) les exigences d'exactitude et de stabilité pour les mesurages et les commandes;

e) le *PDS(SR)* et les interfaces des opérateurs relatives à la sécurité;

f) les interfaces entre le *PDS(SR)* et les autres systèmes (internes ou externes à l'*installation*);

g) tous les modes de comportement du *PDS(SR)*, notamment le comportement à la défaillance et la réponse exigée (par exemple, alarmes, arrêt automatique) du *PDS(SR)*;

h) l'importance de toutes les interactions matériel/logiciel et, le cas échéant, les contraintes exigées entre le matériel et le logiciel;

i) les conditions aux limites et de contraintes pour le *PDS(SR)* et ses sous-systèmes associés, par exemple, contraintes de temporisation ou contraintes dues à la possibilité de *défaillances de cause commune*;

j) les exigences spécifiques relatives aux procédures de démarrage et de redémarrage du *PDS(SR)*.

5.6.2.3 La spécification de l'architecture du système de sécurité doit comprendre les détails relatifs à la conception, qui permettent d'obtenir le *niveau d'intégrité de sécurité* pour la *sous-fonction de sécurité*, comme précisé par la spécification des exigences d'*intégrité de sécurité* du *PDS(SR)* (voir 5.5.3), y compris:

a) l'architecture de chaque *sous-système* exigée pour satisfaire aux contraintes architecturales concernant l'*intégrité de sécurité* du matériel;

b) tous les paramètres de modélisation de fiabilité pertinents tels que l'intervalle entre *essais de diagnostic* exigé du matériel nécessaire pour réaliser l'objectif chiffré de défaillance;

5.6.2.4 La spécification de l'architecture du système de sécurité du *PDS(SR)* doit être détaillée en fonction de l'évolution de la conception et mise à jour si nécessaire après modification.

5.6.2.5 Un groupe approprié de techniques et mesures conformes au Tableau B.2 de l'IEC 61508-2:2010 doit être utilisé pour éviter les erreurs au cours de l'élaboration de la définition de la spécification de l'architecture du système de sécurité du *PDS(SR)*.

5.6.2.6 Les implications de la spécification de l'architecture du système de sécurité du *PDS(SR)* sur l'architecture proprement dite doivent être prises en considération.

NOTE La simplicité de la mise en œuvre peut être prise en considération afin d'obtenir le *niveau d'intégrité de sécurité* exigé (y compris les considérations d'architecture et la répartition des fonctions pour les données de configuration et le système intégré).

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*) qui peut 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, toute défaillance d'un *PDS*(*SR*) qui est en état d'attente ne peut pas 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 l'IEC 61800-5-1 et aux autres parties applicables de la série IEC 61800 énumérées dans les références normatives.

6.1.3 Réalisation

Le *PDS(SR)* doit être réalisé conformément à la *spécification des exigences de sécurité* (voir 5.5).

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 6.2.3), et
   - les exigences relatives à la valeur de la *PFH* (voir 6.2.2 ou 6.2.3);

b) les exigences relatives à l'*intégrité de sécurité systématique*, notamment:
   - les exigences relatives à l'évitement des défaillances (voir 6.2.5.1) ainsi que les exigences relatives à la maîtrise des défauts systématiques (voir 6.2.5.2), ou
   - les preuves que les composants utilisés sont "éprouvés par une utilisation antérieure". Dans ce cas, les composants doivent satisfaire aux exigences de l'IEC 61508-2:2010;

c) les exigences relatives au comportement à adopter par suite de la détection d'un défaut (voir 6.3).

NOTE Lorsque le PL et la catégorie doivent être revendiqués, se reporter également à 6.2 de l'ISO 13849-1:2006.

6.1.5 *Sous-fonctions de sécurité* et *sous-fonctions non relatives à la sécurité*

Lorsqu'un *PDS(SR*) doit exécuter à la fois une *sous-fonction de sécurité* et une *sous-fonction non relative à la sécurité*, l'ensemble de son matériel et de son logiciel doit alors être traité comme relatif à la sécurité, à moins que des mesures de conception appropriées assurent que les défaillances des *sous-fonctions* non relatives à la *sécurité* ne puissent pas altérer les *sous-fonctions de sécurité*.

Voir l'Annexe F de l'IEC 61508-3:2010 pour les techniques de réalisation de non-interférence entre les composantes logicielles d'un seul ordinateur.

6.1.6 *SIL* pour plusieurs *sous-fonctions de sécurité* dans un *PDS(SR)*

Le *niveau d'intégrité de sécurité* d'une *sous-fonction de sécurité* peut être différent des autres, et les exigences relatives à la conception de chaque *sous-fonction de sécurité* sont définies comme suit.

Les exigences relatives aux matériels et logiciels doivent être déterminées selon le *niveau d'intégrité de sécurité* de la *sous-fonction de sécurité* présentant le *niveau d'intégrité de sécurité* le plus élevé, sauf s'il peut être démontré que la mise en œuvre des *sous-fonctions de sécurité* des différents *niveaux d'intégrité de sécurité* est suffisamment indépendante.

Voir le Tableau 2 ci-dessous à titre d'exemple:

Tableau 2 – Exemple de détermination du *SIL* à partir de l'indépendance du matériel et du logiciel

***PDS(SR)* mettant en œuvre deux *sous-fonctions de sécurité* (Y et Z) avec différentes exigences relatives au *SIL*: Fonction Z: *SIL* H[a] / fonction Y: *SIL* L[a]**				
Type de conception	**Preuve d'une indépendance suffisante entre les *sous-fonctions de sécurité* Y et Z**		**Exigences relatives au *SIL* final pour la *sous-fonction de sécurité***	
	pour le matériel	**pour le logiciel**	**Y**	**Z**
Conception matérielle (HW) **et** logicielle (SW)	Oui	Oui	*SIL* H	*SIL* L
	Non	Oui	SW: *SIL* H HW: *SIL* H	SW: *SIL* L HW: *SIL* H [b]
		Non	*SIL* H	*SIL* H
	Oui	Non	SW: *SIL* H HW: *SIL* H	SW: *SIL* H [b] HW: *SIL* L
Conception matérielle **uniquement**	Oui	**non applicable**	*SIL* H	*SIL* L
	Non		*SIL* H	*SIL* H [b]

[a] avec *SIL* H supérieur à *SIL* L

[b] L'indépendance entre HW et/ou SW n'est pas suffisante

Une indépendance suffisante doit être établie en démontrant que la probabilité de défaillance dépendante entre les parties exécutant des *sous-fonctions de sécurité* de niveaux d'intégrité différents est suffisamment faible comparée à la probabilité de défaillance dangereuse pour le niveau d'intégrité de sécurité le plus élevé associé aux *sous-fonctions de sécurité* impliquées.

6.1.7 Circuits intégrés avec redondance sur la puce

Les circuits intégrés numériques qui appliquent une redondance sur la puce dans le but d'augmenter la tolérance aux défauts d'un *PDS(SR)* doivent satisfaire à l'ensemble des exigences spéciales relatives aux circuits intégrés avec redondance sur la puce conformément à l'Annexe E de l'IEC 61508-2:2010 dans le cas de circuits redondants. En variante, le fait que le même niveau d'indépendance entre différents canaux soit obtenu par l'application d'un ensemble différent de mesures doit être justifié.

6.1.8 Exigences logicielles

Si un logiciel est utilisé pour exécuter une *sous-fonction de sécurité* du *PDS(SR*) comportant un *SIL* ou une *capacité SIL* spécifique (voir 5.5.3), ce logiciel doit alors être mis en œuvre conformément aux exigences définies dans l'IEC 61508-3:2010, relatives à ce *SIL* spécifique.

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 la *capacité SIL* (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 Principes de sécurité de base et principes de sécurité éprouvés

Ces principes doivent être pris en considération le cas échéant lorsqu'une catégorie est revendiquée pour le *PDS(SR)*.

- Pour un *PDS(SR)* électrique et électromécanique, ces principes correspondent aux Tableaux D.1 et D.2 de l'ISO 13849-2:2012
- Pour les parties mécaniques (par exemple, codeurs), ces principes correspondent aux Tableaux A.1 et A.2 de l'ISO 13849-2:2012

6.2.2 Exigences relatives à l'estimation de la probabilité de défaillances matérielles dangereuses aléatoires par heure (*PFH*)

6.2.2.1 Exigences générales

6.2.2.1.1 *PFH* pour chaque *sous-fonction de sécurité*

La *PFH* de chaque *sous-fonction de sécurité* (ou groupe de *sous-fonctions de sécurité* activées simultanément) à réaliser par le *PDS(SR*), selon l'estimation donnée en 6.2.2.1.2 et dans l'Annexe B, doit être inférieure ou égale à l'objectif chiffré de défaillance (voir Tableau 3), comme indiqué dans la spécification des exigences d'*intégrité de sécurité* (voir 5.5.3).

La valeur de *PFH*, telle que définie par le *SIL*, se rapporte à une *sous-fonction de sécurité* complète. Si un *PDS(SR*) est conçu pour ne réaliser qu'une partie d'une *sous-fonction de sécurité* au sein d'un système de commande relatif à la sécurité, il convient alors que la *PFH* du *PDS(SR*) soit suffisamment inférieure à la valeur définie par le *SIL*.

L'objectif chiffré de défaillance, exprimé en *PFH*, est déterminé par le *SIL* de la *sous-fonction de sécurité* (voir le Tableau 3 de l'IEC 61508-1:2010), sauf si l'une des exigences de la spécification des exigences *d'intégrité de sécurité* du *PDS(SR)* (voir 5.5.3) précise que la *sous-fonction de sécurité* doit respecter un objectif chiffré de défaillance spécifique plutôt qu'un *SIL* spécifique.

Tableau 3 – *Niveaux d'intégrité de sécurité*: objectifs chiffrés de défaillance de la *sous-fonction de sécurité* d'un *PDS(SR)*

Niveau d'intégrité de sécurité SIL	***PFH* [h^{-1}]**
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 *défaillances dangereuses* ou taux de *défaillance dangereuse*, en unités de *défaillances dangereuses* par heure.	

La *PFH* doit être estimée séparément pour chaque *sous-fonction de sécurité* (ou groupe de *sous-fonctions de sécurité* activées simultanément) du *PDS(SR)*.

NOTE 1 Il peut exister des *sous-fonctions de sécurité* différentes pour des composants communs et/ou uniques. La *PFH* est alors différente pour chaque *sous-fonction de sécurité* (ou groupe de *sous-fonctions de sécurité* utilisées simultanément).

NOTE 2 Il existe plusieurs méthodes de modélisation. Le choix relatif à la méthode la plus appropriée incombe à l'analyste, et ce choix dépend des circonstances. Les méthodes possibles sont, entre autres:

- l'analyse par arbre de panne (voir l'IEC 61025);
- les modèles de Markov (voir l'IEC 61165);
- les blocs-diagrammes de fiabilité (voir l'IEC 61078);
- le dénombrement des pièces (voir l'IEC 61709:2011);
- la description de procédure (voir l'IEC 61508-6:2010);
- la procédure simplifiée pour l'estimation d'un PL (voir 4.5.4 de l'ISO 13849:2006).

Voir également l'IEC 60300-3-1.

NOTE 3 La durée moyenne de panne (voir l'IEC 60050, 192-07-23) prise en considération dans le modèle de fiabilité nécessite la prise en compte des intervalles entre essais de diagnostic, du temps de réparation, de tout autre délai précédant le rétablissement et de la *durée de mission*.

NOTE 4 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 définies comme des défaillances matérielles aléatoires. (Voir l'Annexe D de l'IEC 61508-6:2000).

NOTE 5 Lorsque le PL doit être revendiqué, se reporter également au Tableau 3 de l'ISO 13849-1:2006.

6.2.2.1.2 Estimation de la *PFH*

La *PFH* de chaque *sous-fonction de sécurité* (ou groupe de *sous-fonctions de sécurité* activées simultanément) à réaliser par le *PDS(SR*), à cause de défaillances matérielles aléatoires, doit être estimée conformément à l'Annexe A de l'IEC 61508-2:2010 et en tenant compte des éléments suivants:

a) l'architecture du *PDS(SR*), car elle dépend de chaque *sous-fonction de sécurité* à l'étude;

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 l'IEC 61508-6:2010);

e) la *couverture du diagnostic* (DC) des *essais de diagnostic* (déterminée conformément à l'Annexe A et à l'Annexe C de l'IEC 61508-2:2010) et l'intervalle entre *essais de diagnostic* associé, ainsi que la prise en considération des intervalles entre chaque essai contribuant à la *couverture du diagnostic* au moment de déterminer l'intervalle entre les *essais de diagnostic*;

f) les temps de réparation des défaillances détectées;

NOTE 1 Le temps de réparation constitue une partie de la durée moyenne de panne (voir l'IEC 60050-192:2015, 192-07-23), qui inclut également le temps nécessaire pour détecter une défaillance, ainsi que toute période au cours de laquelle aucune réparation n'est possible (voir l'Annexe B de l'IEC 61508-6:2010 pour un exemple de la façon dont la durée moyenne de panne peut être utilisée pour calculer la probabilité de défaillance). Lorsque la réparation ne peut être effectuée qu'au cours d'une période spécifique, par exemple lorsque l'équipement ou la machine entraîné(e) par le *PDS(SR)* est hors tension ou dans un état de sécurité, il est particulièrement important de bien prendre en compte la période pendant laquelle aucune réparation ne peut être effectuée, notamment lorsque celle-ci est relativement longue.

g) la probabilité de *défaillance dangereuse* de tout processus de communication des données (voir 6.4).

NOTE 2 Pour les informations sur l'estimation de la valeur PFD_{moy} à partir de la valeur de la *PFH* pour les applications à faible sollicitation, voir l'Annexe F.

6.2.2.1.3 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
- une estimation basée sur les composants de type A définis comme "éprouvés par une utilisation antérieure" (voir 7.4.10 de l'IEC 61508-2:2010).

Il convient d'utiliser la température moyenne de fonctionnement attendue pour un composant lors de l'estimation de son taux de défaillance.

Si les données relatives aux défaillances spécifiques à un site sont connues, ces données sont alors à privilégier. À défaut, les données génériques peuvent alors être utilisées.

NOTE 1 Les données peuvent être déduites des données publiées dans de nombreuses sources du secteur (voir l'Annexe C).

NOTE 2 Bien que les méthodes d'estimation les plus probabilistes considèrent par hypothèse 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 par conséquent plus représentatifs. Ainsi, toute estimation probabiliste peut comprendre 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).

NOTE 3 Les listes de pannes données dans l'Annexe D peuvent être utilisées pour faciliter la détermination des modes de défaillance.

Le niveau de confiance de toutes les données utilisées relatives aux taux de défaillance doit être au moins égal à 70 %.

6.2.2.1.4 Intervalle entre *essais de diagnostic* pour une tolérance aux défauts supérieure à zéro du matériel

L'intervalle entre *essais de diagnostic* de tout *sous-système* du *PDS(SR*) doit permettre de satisfaire à la *PFH* exigée (voir 6.2.2.1.1).

NOTE 1 Pour de plus amples informations sur l'impact mathématique de l'intervalle entre essais de diagnostic, voir B.4.

NOTE 2 Pour les parties redondantes d'un *PDS(SR)* qui ne peuvent être soumises à l'essai sans interrompre l'application d'utilisation du *PDS(SR)* (machine ou usine) et lorsqu'aucune solution technique justifiable ne peut être appliquée, les intervalles maximaux entre essais de diagnostic suivants peuvent être acceptables:

- un essai par an pour *SIL* 2, PL d / catégorie 3;
- un essai par trimestre pour *SIL* 3, PL e / catégorie 3;
- un essai par jour pour *SIL* 3, PL e / catégorie 4.

PL et catégorie conformément à l'ISO 13849-1.

6.2.2.1.5 Intervalle entre essais de diagnostic 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 *sous-fonction de sécurité*, l'intervalle entre *essais de diagnostic* doit être tel que la somme de l'intervalle entre *essais de diagnostic* et de la durée de réalisation d'une action donnée (*fonction de réaction au défaut*) pour atteindre ou maintenir un état de sécurité soit inférieure au temps de sécurité du processus.

6.2.3 Contraintes architecturales

6.2.3.1 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 revendiqué pour une *sous-fonction de sécurité* est limité par la tolérance aux défauts du matériel et la proportion de *défaillances en sécurité* des *sous-systèmes* d'un *PDS(SR)* qui exécutent la *sous-fonction de sécurité*. Une tolérance aux défauts du matériel N signifie que $N+1$ défauts peuvent entraîner la perte de la *sous-fonction de sécurité*. Le Tableau 4 et le Tableau 5 spécifient le *niveau d'intégrité de sécurité* le plus élevé qui peut être revendiqué pour une *sous-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 l'IEC 61508-2:2010). Les exigences du Tableau 4 ou du Tableau 5, selon celui qui convient, doivent être appliquées à chaque *sous-système* exécutant une *sous-fonction de sécurité* et, de ce fait, à chaque partie du *PDS(SR)*. Les paragraphes 6.2.3.2.2 et 6.2.3.2.3 spécifient, entre le Tableau 4 ou le Tableau 5 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 qui peut contrôler les effets des défauts (telle 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 traités 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 l'Article D.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 possible de revendiquer, même si dans certains cas, un *niveau d'intégrité de sécurité* supérieur peut théoriquement être calculé si une approche uniquement mathématique a été adoptée pour le *PDS(SR)*.

NOTE 2 Les exigences de tolérance aux défauts peuvent être assouplies lorsque le *PDS(SR)* est en cours de réparation en ligne. Toutefois, les paramètres clés relatifs à tout assouplissement éventuel doivent avoir été préalablement évalués (par exemple, en comparant la durée moyenne de panne à la probabilité d'une sollicitation).

NOTE 3 Cet article est basé sur le parcours 1_H décrit en 7.4.4 de l'IEC 61508-2:2010; pour les exigences relatives au parcours 2_H, voir 7.4.4.3 de l'IEC 61508-2:2010.

6.2.3.2 *Sous-systèmes* de Type A et de Type B

6.2.3.2.1 Généralités

(Voir également 7.4.4.1.2 et 7.4.4.1.3 de l'IEC 61508-2:2010).

6.2.3.2.2 Type A

Un *sous-système* peut être défini de type A si, pour les composants nécessaires à l'exécution de la *sous-fonction de sécurité*, les critères suivants sont satisfaits:

a) les modes de défaillance de tous les composants qui le constituent sont bien définis; et

b) le comportement du *sous-système* dans des conditions 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 revendiqués 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.

6.2.3.2.3 Type B

Un *sous-système* doit être défini de type B si, pour les composants nécessaires à l'exécution de la *sous-fonction de sécurité*, un ou plusieurs des critères de 6.2.3.2.2 ne sont pas satisfaits. 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 défini de type B, et non de type A.

NOTE 1 À titre d'exemple, la section de commande constituée de microcontrôleurs est définie comme un *sous-système* de type B.

NOTE 2 L'Annexe D énumère les défauts exclus et les défauts qui peuvent être pris en considération.

6.2.3.3 Contraintes architecturales

Les contraintes architecturales du Tableau 4 ou du Tableau 5 doivent être appliquées: le Tableau 4 s'applique à tout *sous-système* de type A dont est constitué le *PDS(SR)*; le Tableau 5 s'applique à tout *sous-système* de type B dont est constitué le *PDS(SR)*.

NOTE Pour de plus amples informations sur le type A et le type B, voir 7.4.4.1.2 et 7.4.4.1.3 de l'IEC 61508-2:2010,

Tableau 4 – Niveau d'intégrité de sécurité maximal admissible pour une *sous-fonction de sécurité* exécutée par un *sous-système* de type A relatif à la sécurité

Proportion de *défaillances en sécurité* [a]	Tolérance aux défauts du matériel N (voir 6.2.3)		
	0	1	2
< 60 %	*SIL* 1	*SIL* 2	*SIL* 3
60 % à < 90 %	*SIL* 2	*SIL* 3	*SIL* 3
90 % à < 99 %	*SIL* 3	*SIL* 3	*SIL* 3
≥ 99 %	*SIL* 3	*SIL* 3	*SIL* 3

[a] Voir 6.2.4 pour de plus amples informations sur la façon d'estimer la proportion de *défaillances en sécurité*.

Tableau 5 – Niveau d'intégrité de sécurité maximal admissible pour une *sous-fonction de sécurité* exécutée par un *sous-système* de type B relatif à la sécurité

Proportion de *défaillances en sécurité* [a]	Tolérance aux défauts du matériel N (voir 6.2.3)		
	0	1	2
< 60 %	Non admise	*SIL* 1	*SIL* 2
60 % à < 90 %	*SIL* 1	*SIL* 2	*SIL* 3
90 % à < 99%	*SIL* 2	SIL3	*SIL* 3
≥ 99 %	*SIL* 3	*SIL* 3	*SIL* 3

[a] Voir 6.2.4 pour de plus amples informations sur la façon d'estimer la proportion de *défaillances en sécurité*.

Exception:

Pour un *sous-système* avec une tolérance zéro aux défauts du matériel et lorsque les exclusions de défauts ont été appliquées aux défauts des parties électriques ou électroniques qui peuvent entraîner une *défaillance dangereuse, le SIL* maximum qui peut être revendiqué en raison des contraintes architecturales de ce *sous-système* est alors limité à:

- *SIL* 3, dans le cas où les Tableaux D.1, D.3, D.5, D.6, D.7 et D.8 s'appliquent
- *SIL* 2, pour tout autre cas.

NOTE Lorsque la catégorie doit être revendiquée, voir également 6.2 de l'ISO 13849-1:2006.

6.2.4 Estimation de la *proportion* de *défaillances en sécurité* (*SFF*)

6.2.4.1 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.

Pour le calcul de la *SFF*, voir l'Annexe A et l'Annexe C de l'IEC 61508-2:2010.

Pour le *PDS(SR),* le parcours 1_H est préférentiel. Pour le *PDS(SR)*, le parcours 2_H doit être limité aux *sous-systèmes* de Type A.

NOTE Cet article est basé sur le parcours 1_H décrit en 7.4.4.2 de l'IEC 61508-2:2010; pour les exigences relatives au parcours 2_H, voir 7.4.4.3 de l'IEC 61508-2:2010.

La base de données est fournie en 6.2.2.1.3.

NOTE Voir l'Annexe C pour une liste informative des sources connues.

6.2.5 Exigences relatives à l'*intégrité de sécurité systématique* d'un *PDS(SR*) et des *sous-systèmes* d'un *PDS(SR*)

6.2.5.1 Exigences relatives à l'évitement des défaillances

6.2.5.1.1 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*), conformément au Tableau B.2 de l'IEC 61508-2:2010.

Des essais, tels que prévus en 6.2.5.1.4, doivent être effectués. Voir également l'Article 9.

NOTE Pour revendiquer un PL, voir l'Annexe G de l'ISO 13849-1:2006.

6.2.5.1.2 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,