BS EN 61800-5-2:2017

BSI Standards Publication

Adjustable speed electrical power drive systems

Part 5-2: Safety requirements – Functional (IEC 61800-5-2:2016)

bsi.

National foreword

This British Standard is the UK implementation of EN 61800-5-2:2017. It is identical to IEC 61800-5-2:2016. It supersedes BS EN 61800-5-2:2007, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/22, Power electronics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2017

ISBN 978 0 580 81980 3

ICS 29.200; 13.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2017.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61800-5-2

April 2017

ICS 13.110; 29.200

Supersedes EN 61800-5-2:2007

English Version

Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional (IEC 61800-5-2:2016)

Entraînements électriques de puissance à vitesse variable - Partie 5-2: Exigences de sécurité - Fonctionnelle (IEC 61800-5-2:2016)

Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl - Teil 5-2: Anforderungen an die Sicherheit - Funktionale Sicherheit (IEC 61800-5-2:2016)

This European Standard was approved by CENELEC on 2016-05-23. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 22G/332/FDIS, future edition 2 of IEC 61800-5-2, prepared by SC 22G “Adjustable speed electric drive systems incorporating semiconductor power converters” of IEC/TC 22 “Power electronic systems and equipment" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61800-5-2:2017.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2017-10-28
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2020-04-28

This document supersedes EN 61800-5-2:2007.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 61800-5-2:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-3-1:2003	NOTE	Harmonized as 60300-3-1:2003.
IEC 60664-1:2007	NOTE	Harmonized as EN 60664-1:2007.
IEC 606643	NOTE	Harmonized as EN 60664-3.
IEC 61025	NOTE	Harmonized as EN 61025.
IEC 61078	NOTE	Harmonized as EN 61078.
IEC 61165	NOTE	Harmonized as EN 61165.
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010.
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010.
IEC 61511 (series)	NOTE	Harmonized as EN 61511 (series).
IEC 61511-1	NOTE	Harmonized as EN 61511-1.
IEC 61513	NOTE	Harmonized as EN 61513.
IEC 61558 (series)	NOTE	Harmonized as EN 61558 (series).
IEC 61558-1:2005	NOTE	Harmonized as EN 61558-1:2005.
IEC 61558-1:2005/AMD1:2009	NOTE	Harmonized as EN 61558-1:2005/A1:2009.

IEC 61784-3	NOTE	Harmonized as EN 61784-3.
IEC 62061	NOTE	Harmonized as EN 62061.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.

IEC 61784-3	NOTE	Harmonized as EN 61784-3.
IEC 62061	NOTE	Harmonized as EN 62061.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.

IEC 61400-21	2008	Wind turbines -- Part 21: Measurement and assessment of power quality characteristics of grid connected wind turbines	EN 61400-21	2008
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 1: General requirements	EN 61508-1	2010
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	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 3: Software requirements	EN 61508-3	2010
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	EN 61508-6	2010
IEC 61508-7	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 7: Overview of techniques and measures	EN 61508-7	2010
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	EN 61800-1	-
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	EN 61800-2	2015
IEC 61800-3	2004	Adjustable speed electrical power drive systems -- Part 3: EMC requirements and specific test methods	EN 61800-3	2004
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	EN 61800-4	-
IEC 61800-5-1	2007	Adjustable speed electrical power drive systems - Part 5-1: Safety requirements - Electrical, thermal and energy	EN 61800-5-1	2007
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	EN ISO 13849-2	2012

This page deliberately left blank

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-function*s 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.

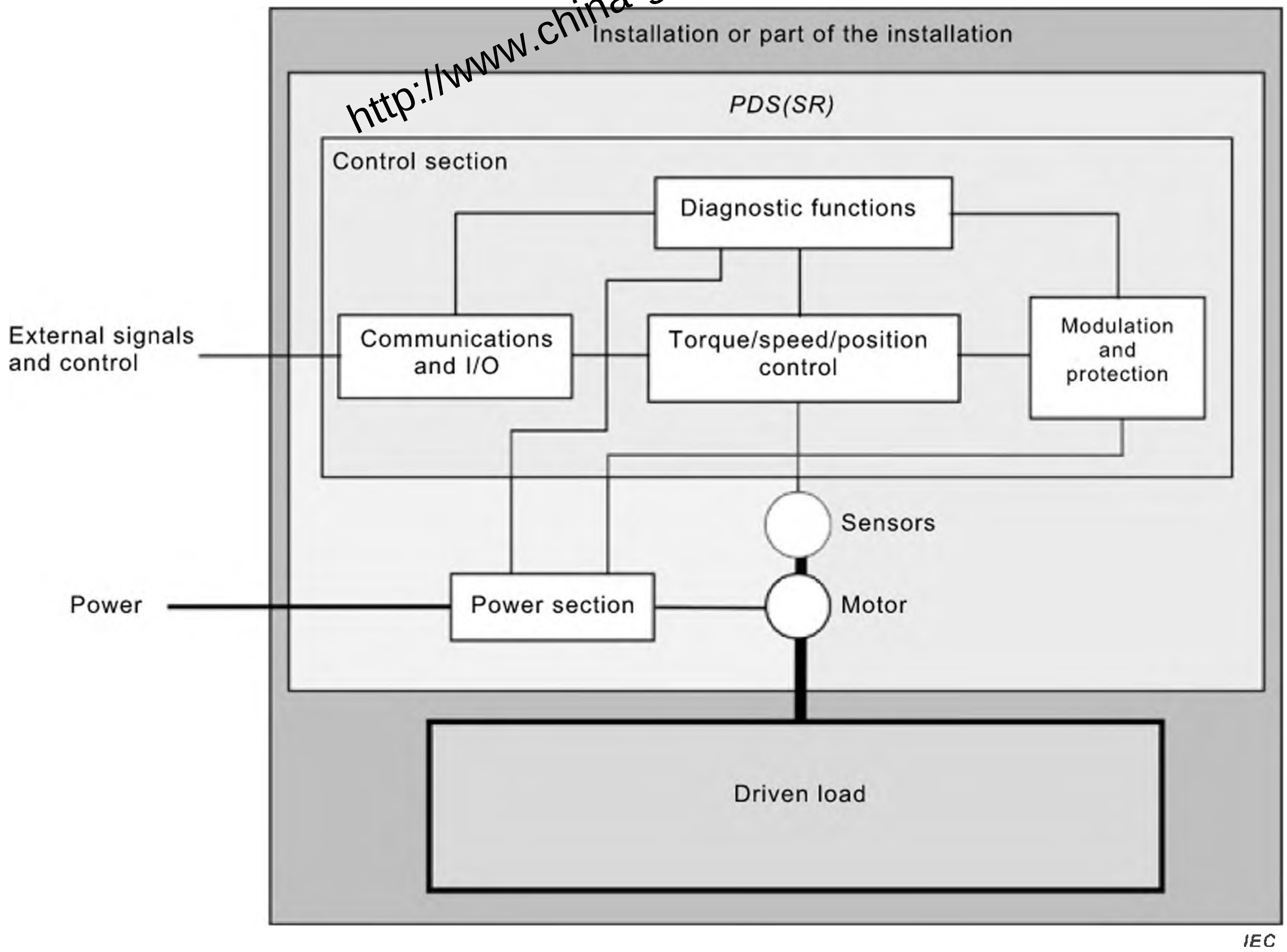


Figure 1 – Installation and functional parts of a *PDS(SR)*

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-functions*

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 *subsystems*, 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 *subsystems* 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 systems* 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-functions* include the words "safe" or "safely" to indicate that these functions may be used in a safety-related application on the grounds of a judgement (i.e. risk analysis) of that specific application, resulting in safety-relevant functions and their integrity to be performed by the *PDS(SR)*.

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*:

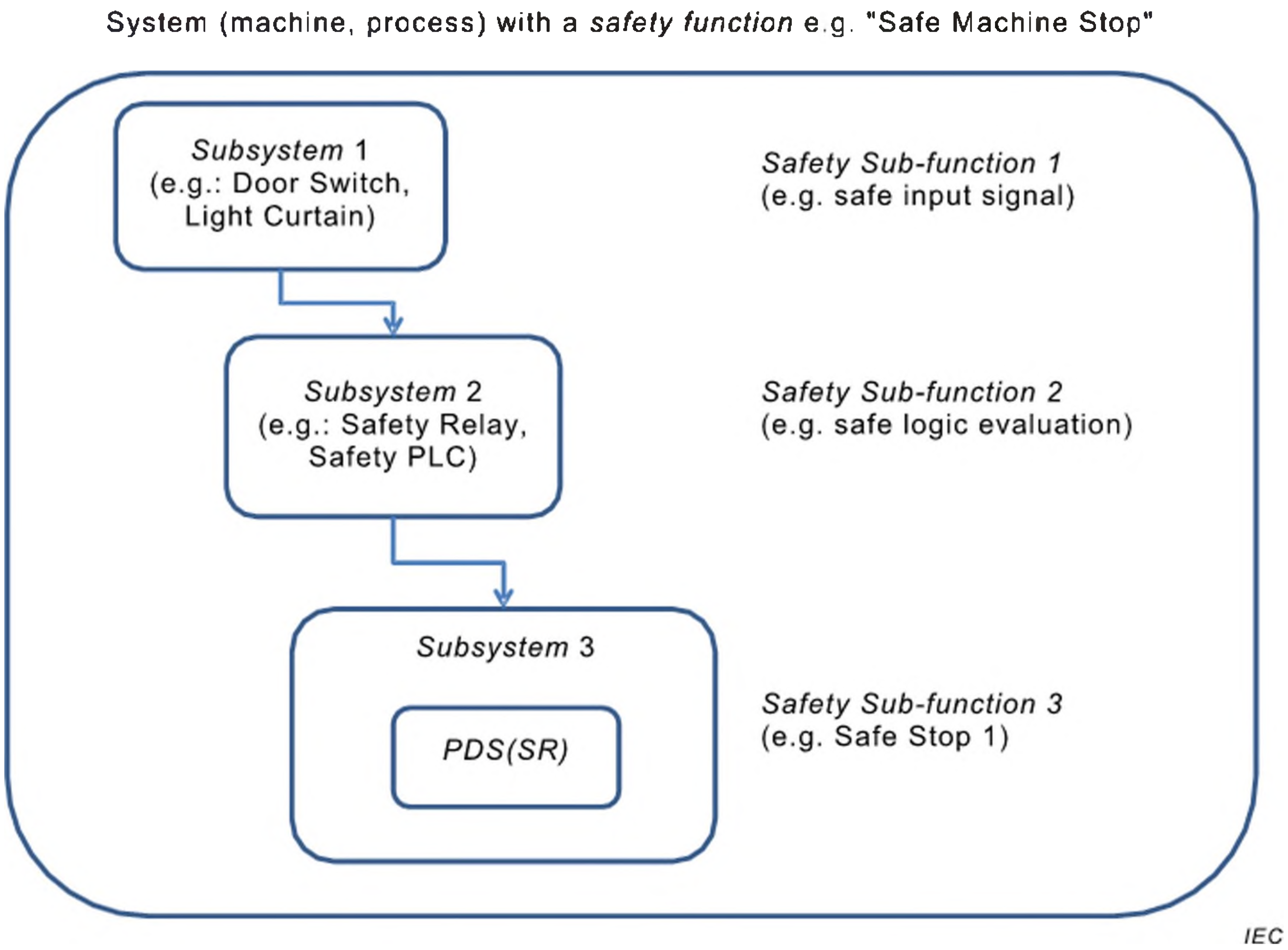


Figure 2 – *Safety function* consisting of *safety sub-functions*

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*

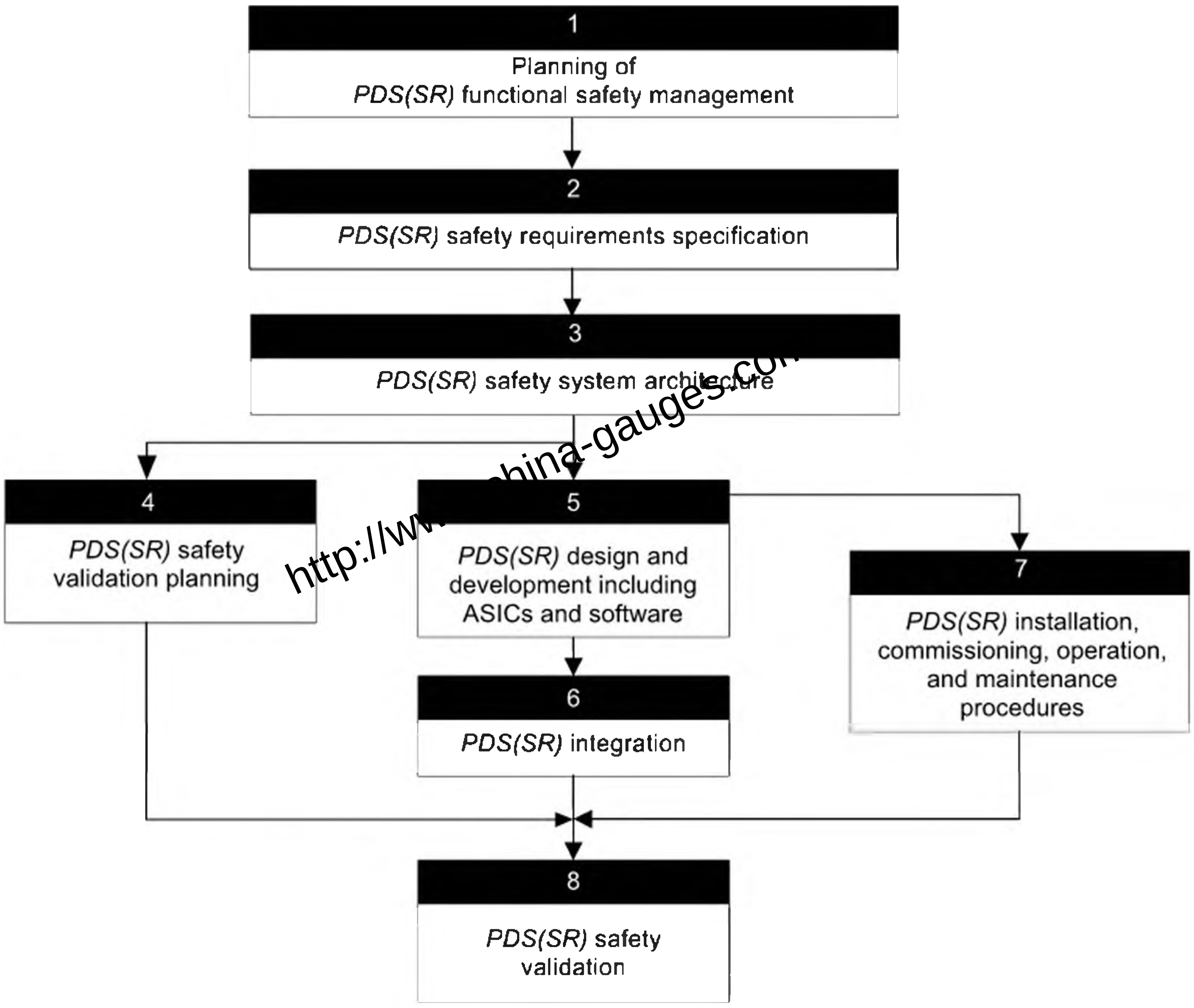
The requirements of Clause 6 of IEC 61508-1:2010 apply.

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.



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 *subsystem*s (for example *safety sub-function* logic, input/output circuitry, power supply, software). The representation of the *PDS(SR)* in form of *subsystem*s 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 *subsystem*s 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 failures*;

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 failures*, 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 *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.

6.2.5 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 *subsystems* with compatible operating characteristics.

c) Withstanding specified environmental conditions:
   – design the *PDS(SR)* so that it is capable of safe operation in all specified environments, for example temperature, humidity, vibration, EM phenomena, pollution degree, overvoltage category, altitude.

6.2.5.1.4 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-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 *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, 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)*;
- 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 failures*;
- any information valid hardware and software versions and the combinations permitted for the *safety sub-functions;* the fact that *safety sub-functions* cannot prevent any failure of non-*safety sub-functions* 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-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.

9 Test requirements

9.1 Planning of tests

Testing of the *safety sub-function*s 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-functions* 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-functions* 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-functions* 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*

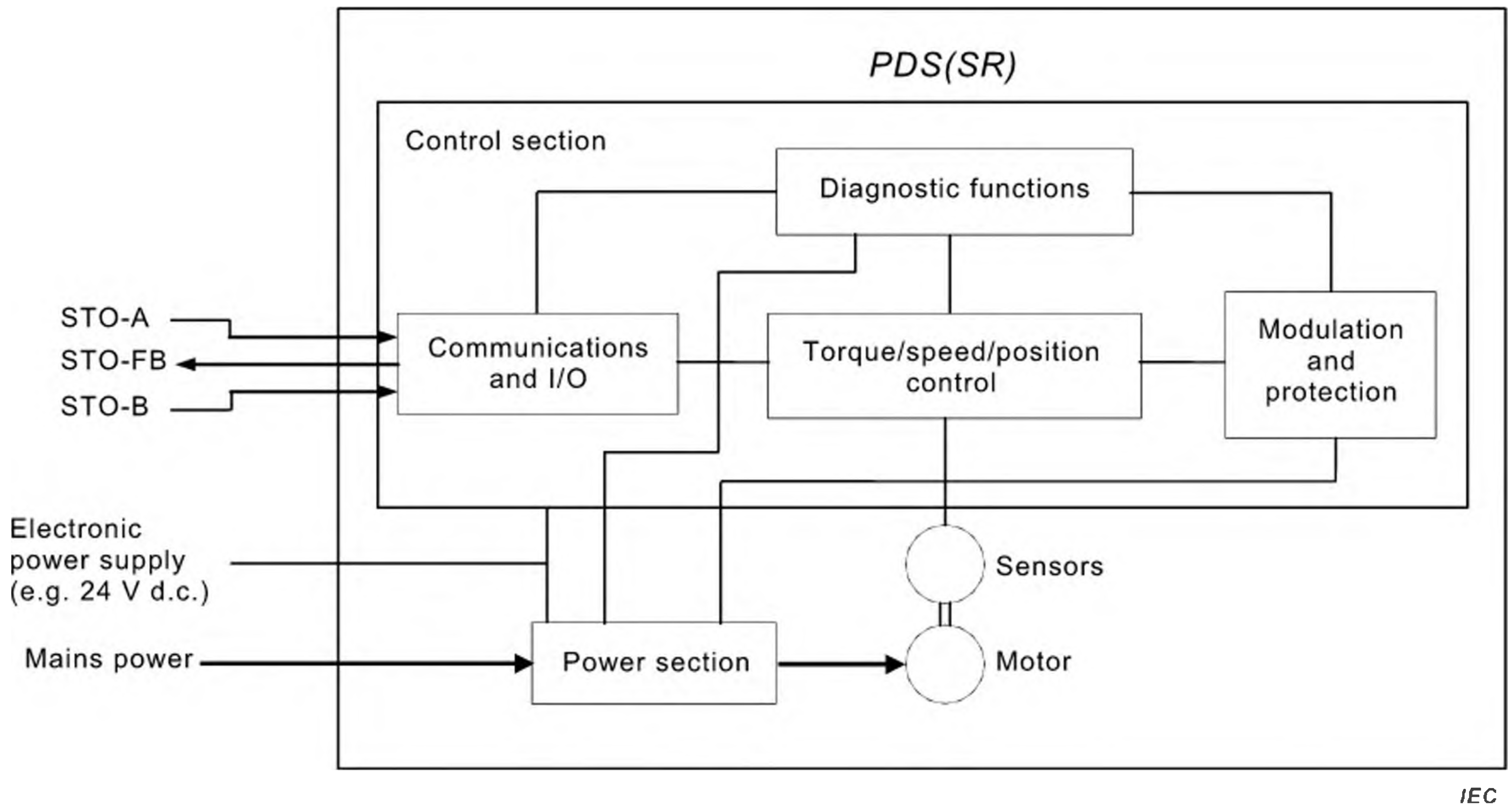
B.1 General

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*.

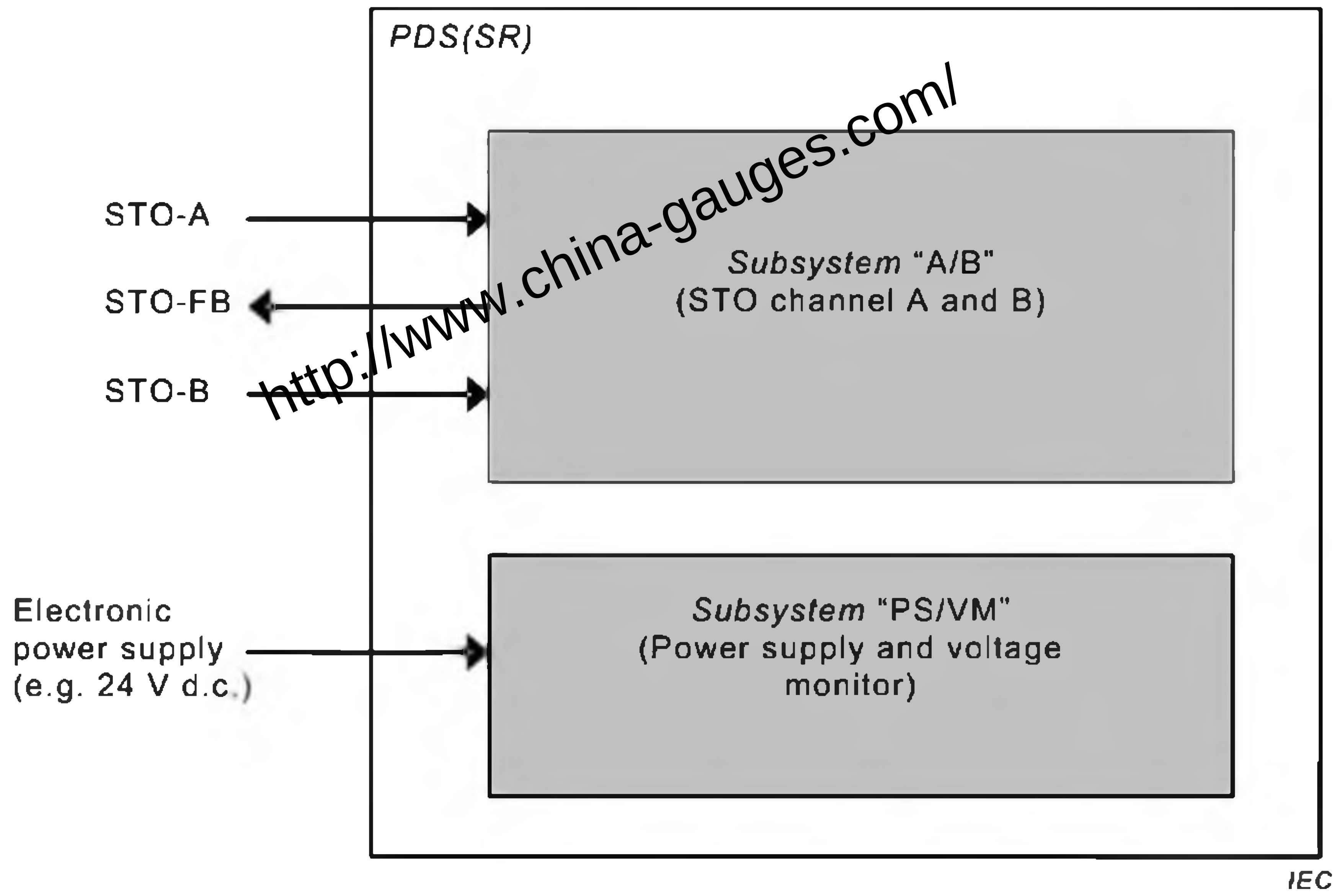
Within the *PDS(SR)*, the *safety sub-function* STO is implemented together with the non-safety-related functionality of the *PDS(SR)* using only a few *safety sub-function* exclusive components.

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:

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

where $PFH_{A/B}$ and $PFH_{PS/VM}$ 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

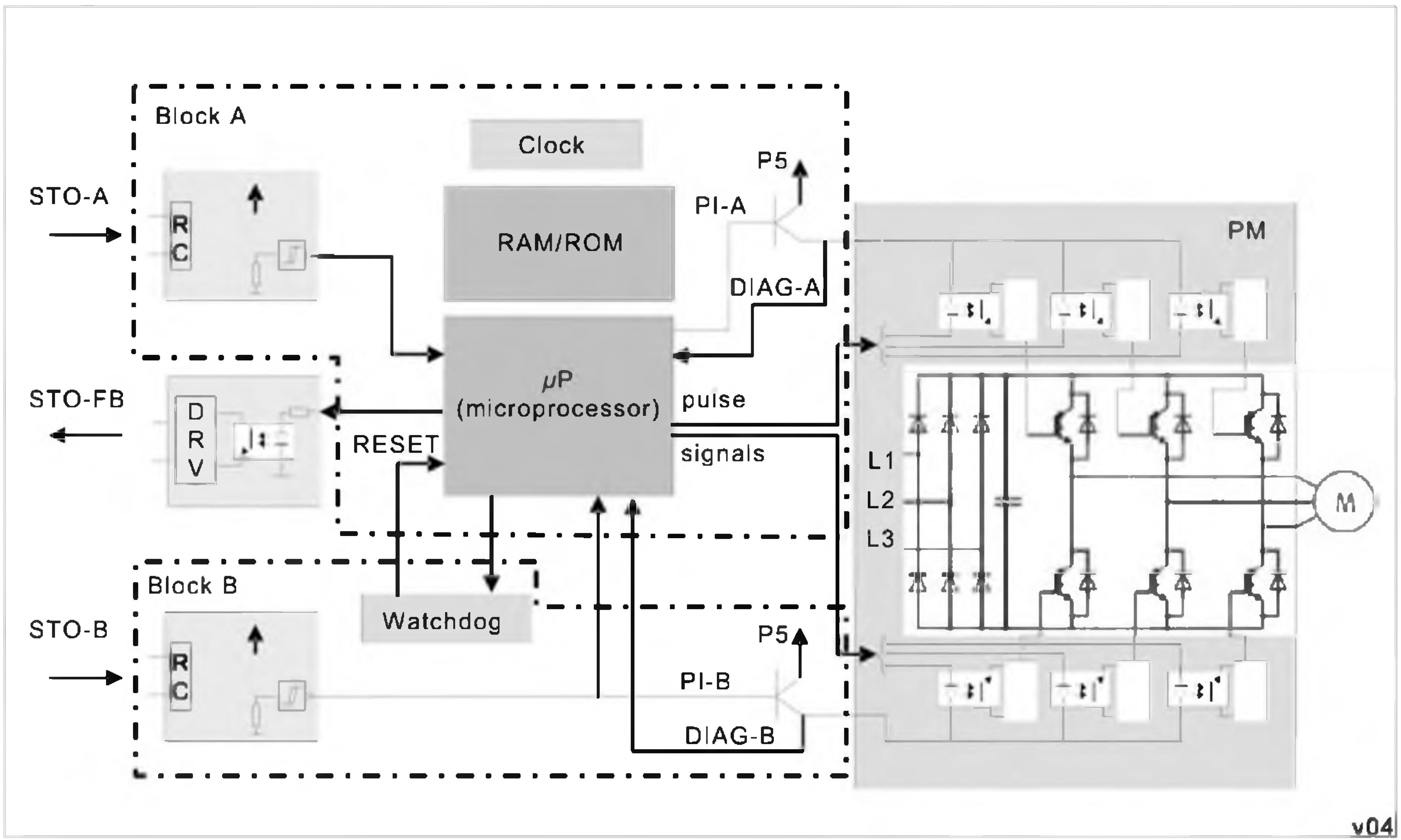
B.3.1 *Subsystem* "A/B" (main *subsystem*)

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 failures*. 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 failures* 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 failures* and a 50 % portion of *dangerous failures*. 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 failures* 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 61508-2:2010, Clause C.1, item h, is:

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

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

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).

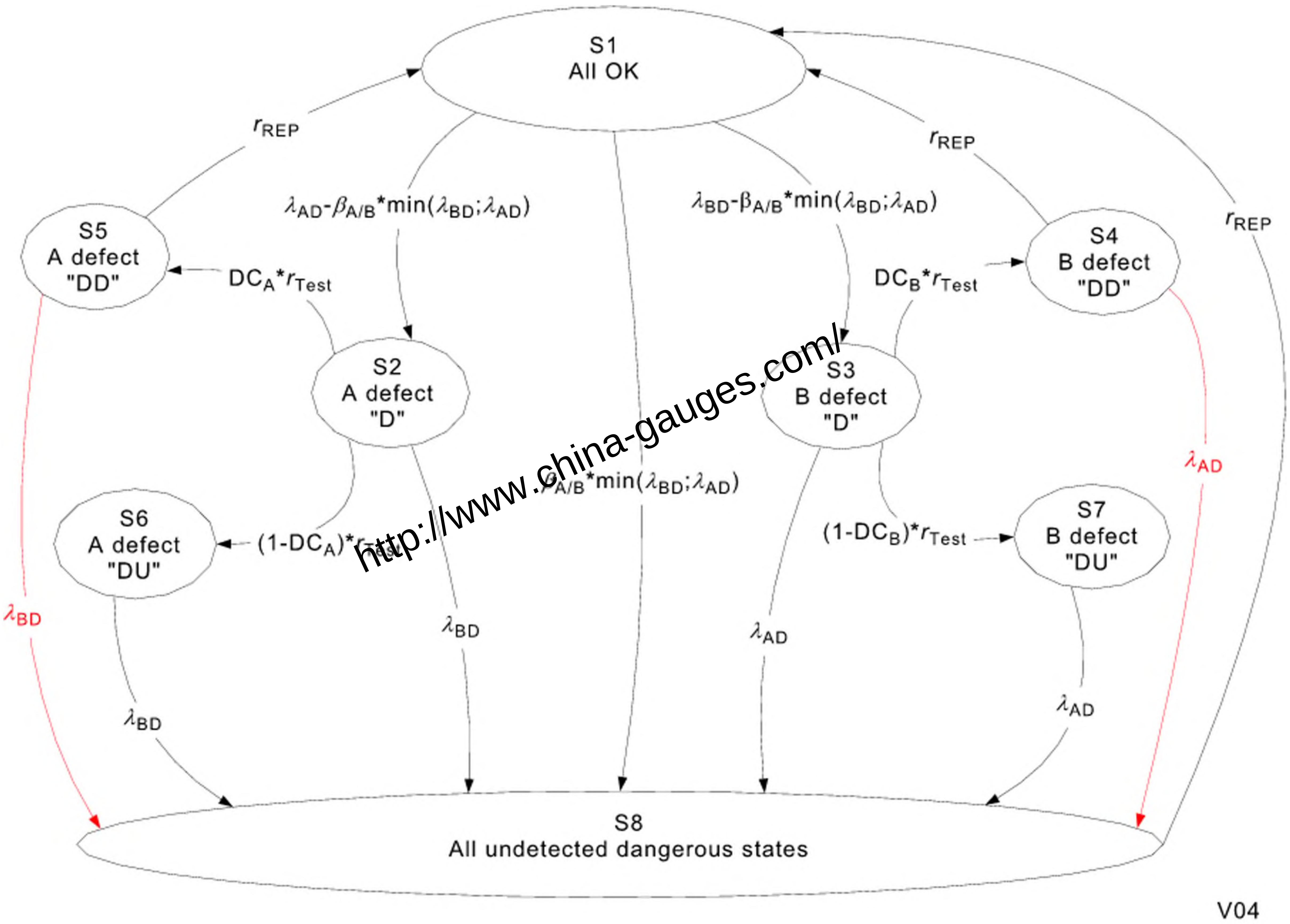
B.3.1.4 *Common cause failure* factor $\beta_{A/B}$

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 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 "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 [$p_i(t)$] 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.

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

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

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

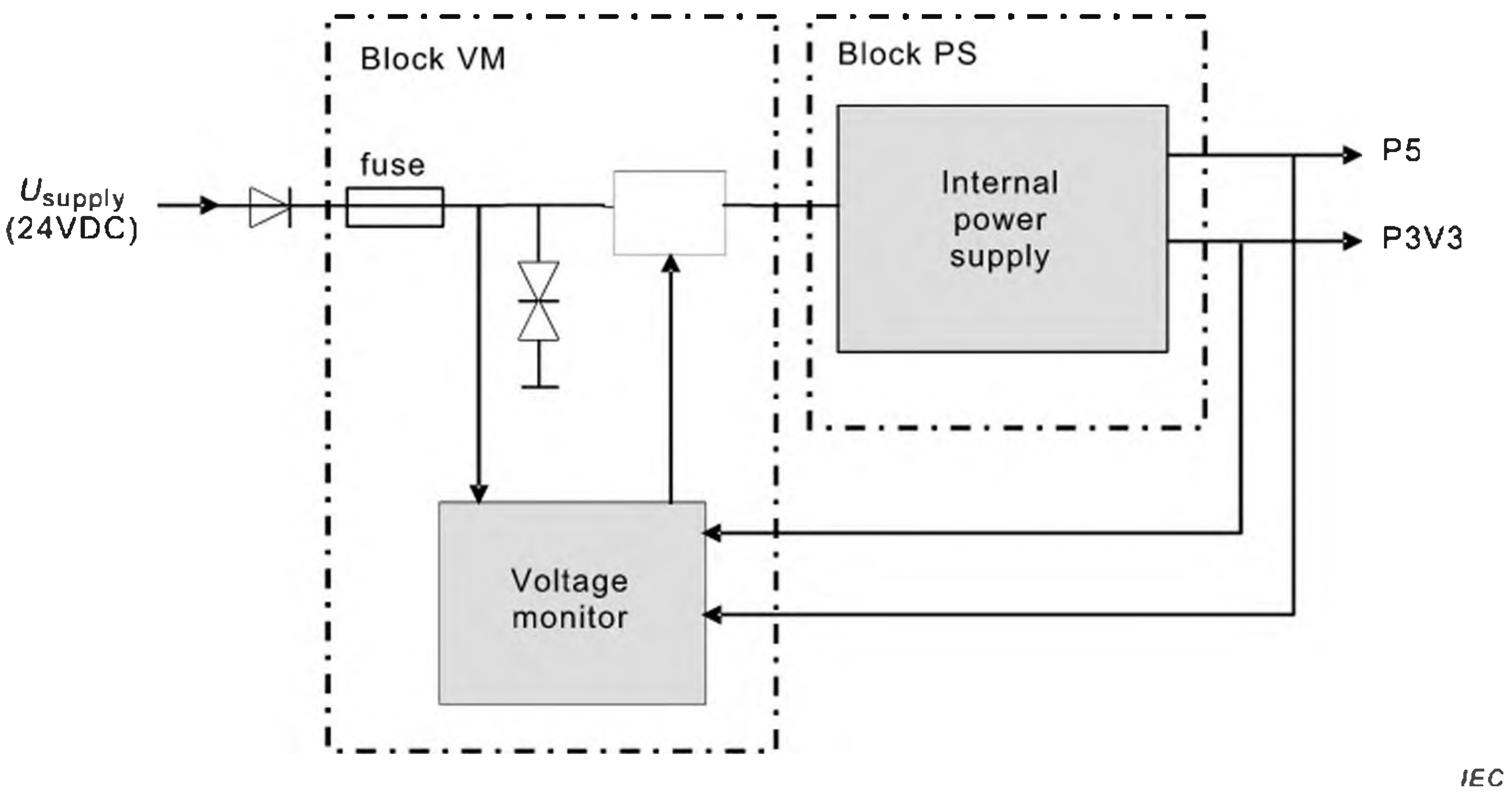
$\beta_{A/B}$	r_{Rep}	r_{Test}	T_M years	$PFH_{A/B}$
2 %	1/8 h	1/8 h	10	$7{,}67 \times 10^{-10}$ /h
2 %	1/8 h	**1/24 h**	10	$7{,}68 \times 10^{-10}$ /h
2 %	1/8 h	**1/168 h**	10	$7{,}70 \times 10^{-10}$ /h
2 %	1/8 h	**1/672 h**	10	$7{,}76 \times 10^{-10}$ /h
2 %	1/8 h	**1/8760 h**	10	$8{,}76 \times 10^{-10}$ /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 failures* 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).

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}	$DC_{PS} * \lambda_{PSD}$	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):

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

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

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

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

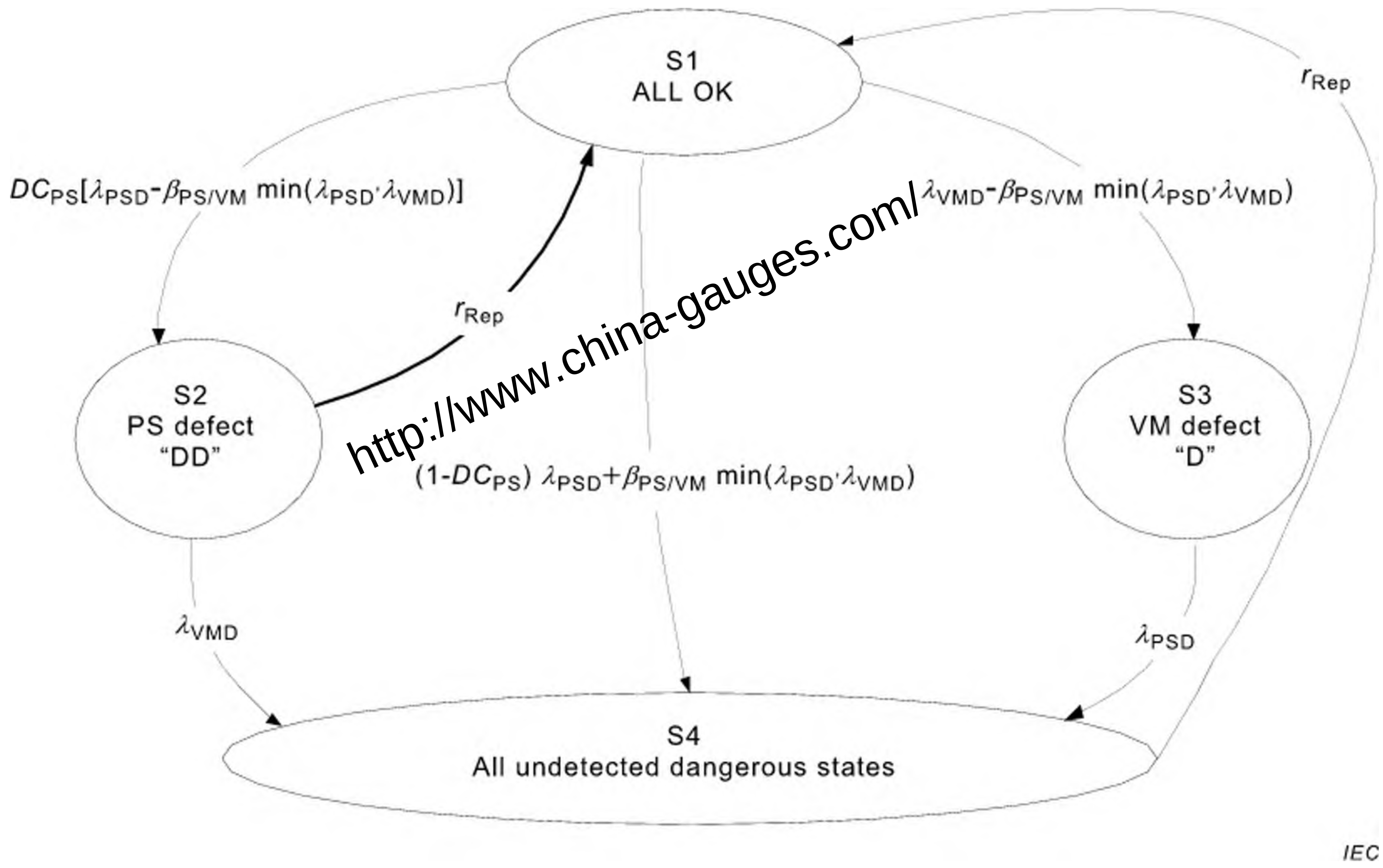
B.3.2.4 *Common cause failure* factor $\beta_{PS/VM}$

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.



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 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 "*hazardous* 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.

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

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

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

$\beta_{PS/VM}$	r_{Rep}	T_M years	$PFH_{PS/VM}$
2 %	1/8 h	10	$4,39 \times 10^{-9}$ /h
2 %	1/8 h	**20**	$5,03 \times 10^{-9}$ /h
3 %	1/8 h	20	$6,25 \times 10^{-9}$ /h
5 %	1/8 h	20	$8,70 \times 10^{-9}$ /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:

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

$PFH_{STO/PDS(SR)}$ (T_M = 10 years) = $(7,67 \times 10^{-10}/h + 4,39 \times 10^{-9}/h) = 5,16 \times 10^{-9}/h$;

$PFH_{STO/PDS(SR)}$ (T_M = 20 years) = $(8,34 \times 10^{-10}/h + 5,03 \times 10^{-9}/h) = 5,86 \times 10^{-9}/h$.

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

Increasing the test interval will lead to a lower resulting *diagnostic coverage* ($DC_{resulting}$) 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' (= $DC_{resulting}$) depending on DC and DI

DC' = $DC_{resulting}$ = DC(1-DI/TM);

SFF' (= $SFF_{resulting}$) according IEC 61508:

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

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) <u>For form-locked connections:</u> 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 ≥ 2 against fatigue fracture. or 2) Overdimensioning with a safety factor S ≥ 5 against fatigue fracture – Verification is performed by calculation. b) <u>For force-locked connections:</u> 1) Overdimensioning with a safety factor S ≥ 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 ≥ 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_{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 60664-1:2007, *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

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.