INTERNATIONAL STANDARD

IEC 61800-5-2

First edition
2007-07

Adjustable speed electrical power drive systems –

Part 5-2:
Safety requirements –
Functional

Reference number
IEC 61800-5-2:2007(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

IEC 61800-5-2

First edition
2007-07

Adjustable speed electrical power drive systems –

Part 5-2:
Safety requirements –
Functional

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XB

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-2: Safety requirements – Functional

FOREWORD

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

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

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

FDIS	Report on voting
22G/179/FDIS	22G/182/RVD

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

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

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

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

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

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

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

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

Examples of industrial applications are:

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

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

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

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

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

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

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

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-2: Safety requirements – Functional

1 Scope and object

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

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

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

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

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

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

This part of IEC 61800 does not specify requirements for:

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

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

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

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

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

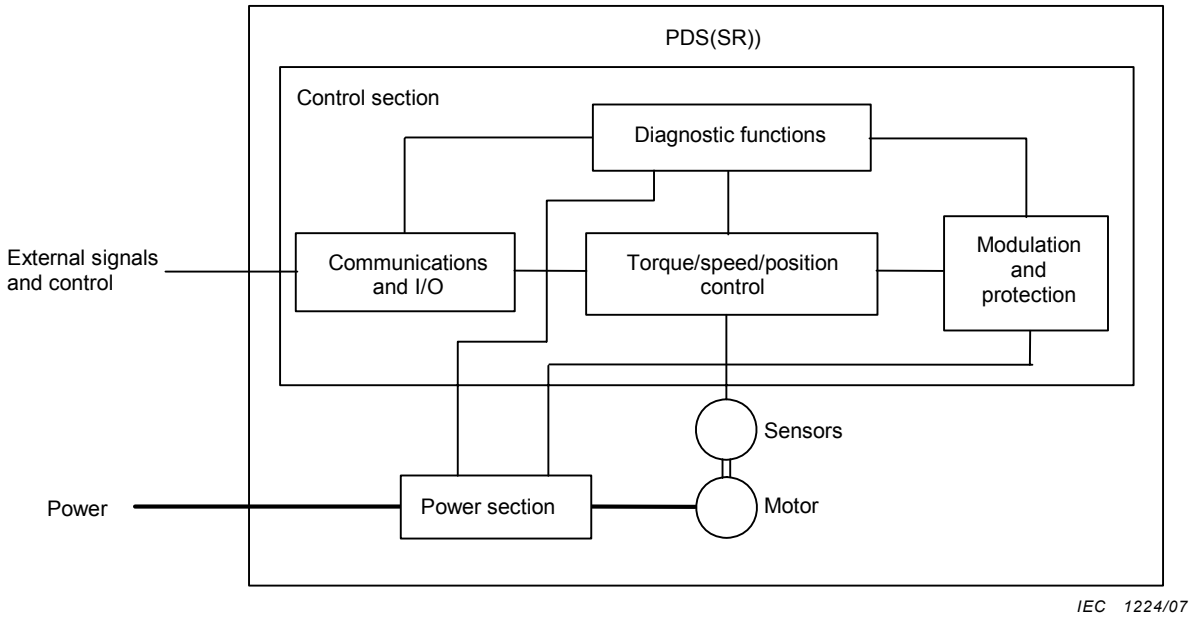


Figure 1 – Functional elements of a PDS(SR)

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

Table 1 – Alphabetical list of definitions

Term	Definition number	Term	Definition number
common cause failure	0	safe failure	3.17
dangerous failure	3.2	safe failure fraction (SFF)	3.18
diagnostic coverage (DC)	3.3	safety function(s) (of a PDS(SR))	3.19
diagnostic test(s)	3.4	safety integrity	3.20
fault reaction function	3.5	safety integrity level (SIL)	3.21
functional safety	3.6	safety-related system	3.22
hazard	3.7	safety requirements specification (SRS)	3.23
installation	3.8	SIL capability	0
mission time	3.10	subsystem	3.25
mode of operation	3.11	systematic failure	3.26
PDS(SR)	3.14	systematic safety integrity	0
PFH	3.15	validation	3.25
proof test	3.16	verification	3.26

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

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

[IEC 61508-4:1998; definition 3.6.10]

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

[IEC 61508-4:1998; definition 3.6.7]

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

[IEC 61508-4:1998; definition 3.8.6]

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

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

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

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

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

[IEC 61508-4:1998; definition 3.1.9]

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

3.7
hazard
potential source of harm

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.12
PFH
probability of a dangerous random hardware failure per hour

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

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

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

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

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

(IEC 61508-4:1998; definition 3.6.8)

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

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

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

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

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

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

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

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

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

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

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

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

3.19
safety-related system
designated system that both

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

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

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

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

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

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

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

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

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

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

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

(IEC 61508-4:1998; definition 3.6.6)

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

(IEC 61508-4:1998; definition 3.5.4)

NOTE Systematic safety integrity cannot usually be quantified.

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

(IEC 61508-4:1998; definition 3.8.2)

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

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

(IEC 61508-4:1998; definition 3.8.1)

4 Designated safety functions

4.1 General

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

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

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

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

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

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

– the fault reaction function:

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

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

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

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

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

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

4.2 Safety functions

4.2.1 Limit values

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

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

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

4.2.2 Stopping functions

4.2.2.1 General

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

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

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

4.2.2.2 Safe torque off (STO)

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

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

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

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

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

4.2.2.3 Safe stop 1 (SS1)

The PDS(SR) either

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

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

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

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

4.2.2.4 Safe stop 2 (SS2)

The PDS(SR) either

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

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

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

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

4.2.3 Other safety functions

4.2.3.1 Safe operating stop (SOS)

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

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

4.2.3.2 Safely-limited acceleration (SLA)

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

4.2.3.3 Safe acceleration range (SAR)

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

4.2.3.4 Safely-limited speed (SLS)

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

4.2.3.5 Safe speed range (SSR)

The SSR function keeps the motor speed within specified limits.

4.2.3.6 Safely-limited torque (SLT)

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

4.2.3.7 Safe torque range (STR)

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

4.2.3.8 Safely-limited position (SLP)

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

4.2.3.9 Safely-limited increment (SLI)

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

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

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

4.2.3.10 Safe direction (SDI)

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

4.2.3.11 Safe motor temperature (SMT)

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

4.2.3.12 Safe brake control (SBC)

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

4.2.3.13 Safe cam (SCA)

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

4.2.3.14 Safe speed monitor (SSM)

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

5 Management of functional safety

5.1 Objective

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

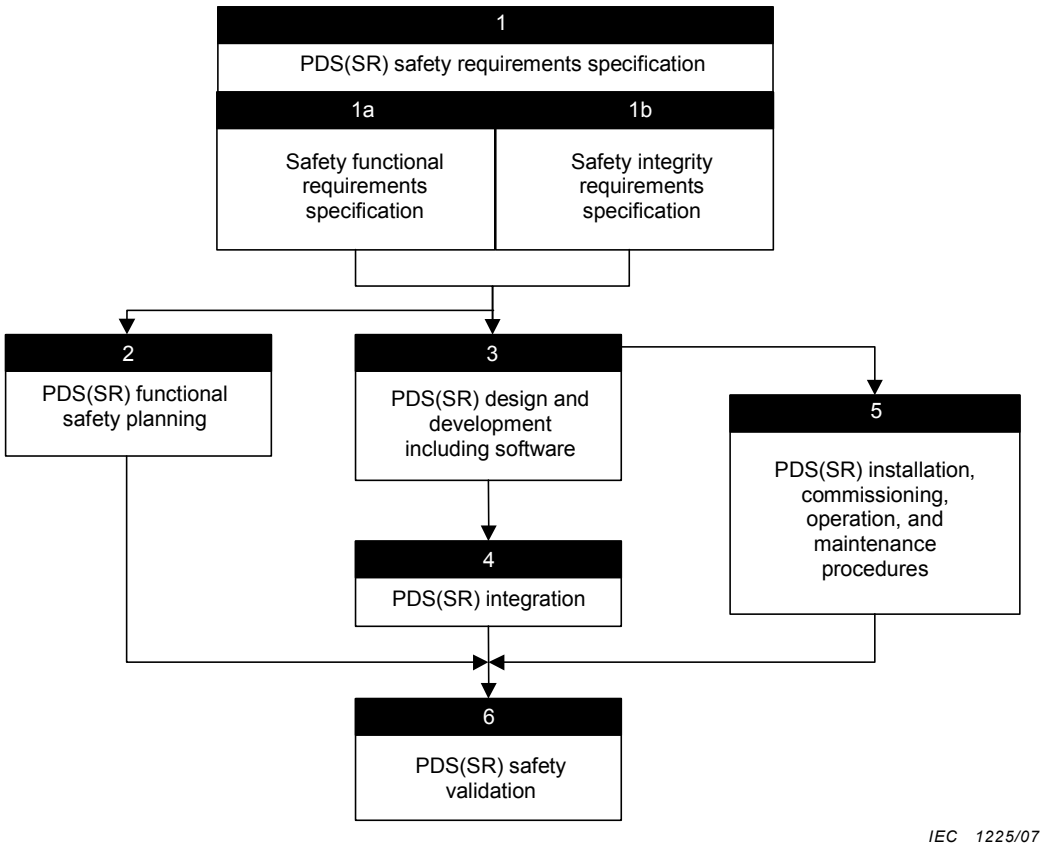
NOTE This clause is solely aimed at the achievement of the functional safety of the PDS(SR) and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

5.2 PDS(SR) development lifecycle

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

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

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



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

Figure 2 – PDS(SR) development lifecycle

5.3 Functional safety planning

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

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

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

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

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

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

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

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

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

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

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

5.4.1 General

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

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

These shall be written so that they are:

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

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

5.4.2 Safety functionality requirements specification

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

The safety functionality requirements specification shall describe, as appropriate:

a) all safety functions to be performed;

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

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

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

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

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

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

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

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

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

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

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

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

5.4.3 Safety integrity requirements specification

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

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

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

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

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

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

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

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

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

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

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

6.1 General requirements

6.1.1 Change in operational status

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

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

6.1.2 Design standards

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

6.1.3 Realisation

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

6.1.4 Safety integrity and fault detection

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

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

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

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

6.1.5 Safety and non-safety functions

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

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

6.1.6 SIL to be used

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

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

6.1.7 Software requirements

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

6.1.8 Review of requirements

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

a) safety functions;

b) safety integrity requirements;

c) equipment and operator interfaces.

6.1.9 Design documentation

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

6.2 PDS(SR) design requirements

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

6.2.1.1 General requirements

6.2.1.1.1 PFH for each safety function

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

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

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

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

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

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

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

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

– fault tree analysis (see IEC 61025);

– Markov models (see IEC 61165);

– reliability block diagrams (see IEC 61078).

See also IEC 60300-3-1.

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

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

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

6.2.1.1.2 Estimation of PFH

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

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

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

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

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

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

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

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

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

g) the repair times for detected failures;

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

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

6.2.1.1.3 Failure rate data

Component failure rate data shall be obtained from:

– a recognised source; or

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

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

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

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

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

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

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

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

6.2.1.1.4 *Diagnostic test* interval

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

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

6.2.1.1.5 Test interval when hardware fault tolerance zero

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

6.2.2 Architectural constraints

6.2.2.1 Limitations of SIL

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

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

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

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

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

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

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

6.2.2.2 Type A and Type B subsystems

6.2.2.2.1 Type A

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

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

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

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

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

6.2.2.2.2 Type B

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

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

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

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

6.2.2.3 Architectural constraints

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

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

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

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

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

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

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

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

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

6.2.3 Estimation of safe failure fraction (SFF)

6.2.3.1 Methods of analysis

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

6.2.3.2 Basis of data

The estimation of SFF shall be based upon either:

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

– component failure data from a recognised source.

See also 6.2.1.1.3.

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

6.2.3.3 Safety relays

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

6.2.3.4 Calculation of SFF

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

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

6.2.4.1 Requirements for the avoidance of failures

6.2.4.1.1 General

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

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

6.2.4.1.2 Choice of design methods

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

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

6.2.4.1.3 Design measures

The following design measures shall be applied.

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

6.2.4.1.4 Test planning

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

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

Documentation of the test planning shall include:

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

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

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

6.2.4.1.5 Design maintenance requirements

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

6.2.4.2 Requirements for the control of systematic faults

6.2.4.2.1 Design features

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

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

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

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

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

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

6.2.4.2.2 Testability and maintainability

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

6.2.4.2.3 Human constraints

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

6.2.4.2.4 Protection against unintentional modification

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

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

6.2.4.2.5 Input acknowledgement and operator mistakes

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

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

6.2.4.2.6 Loss of electrical supply

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

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

6.2.5.1 General

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

6.2.5.2 Intended environment

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

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

6.2.5.3 Performance criterion

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

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

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

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

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

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

6.2.5.4 Introduction of hazards

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

6.2.5.5 Verification

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

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

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

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

6.3 Behaviour on detection of fault

6.3.1 Fault detection

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

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

6.3.2 Fault tolerance greater than zero

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

a) a fault reaction function, or

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

6.3.3 Fault tolerance zero

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

6.4 Additional requirements for data communications

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

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

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

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

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

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

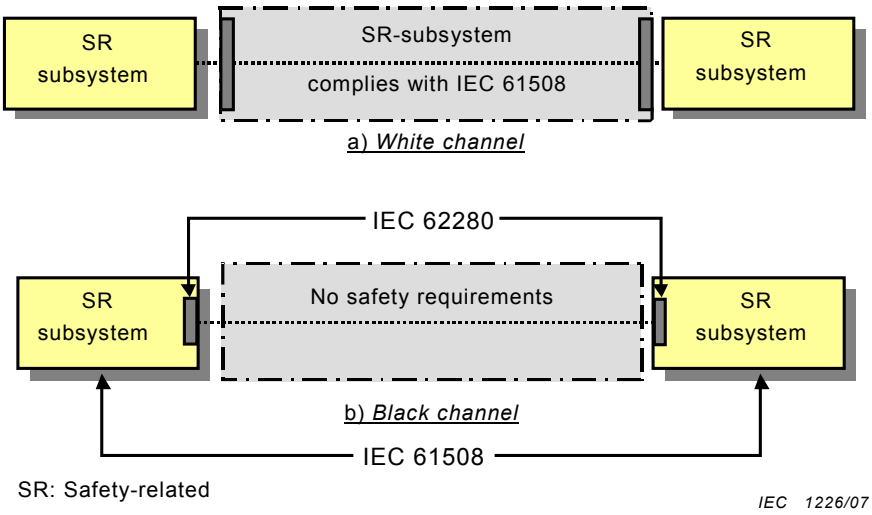


Figure 3 – Architectures for data communication: a) White channel; b) Black channel)

6.5 PDS(SR) integration and testing requirements

6.5.1 Hardware integration

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

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

6.5.2 Software integration

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

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

6.5.3 Modifications during integration

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

6.5.4 Applicable integration tests

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

6.5.5 Test documentation

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

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

7 Information for use

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

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

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

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

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

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

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

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

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

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

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

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

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

8 Verification and validation

8.1 General

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

8.2 Verification

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

8.3 Validation

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

8.4 Documentation

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

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

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

c) the tools and equipment used;

d) the results of each verification and validation.

9 Test requirements

9.1 Planning of tests

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

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

a) the functional testing of each safety function;

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

c) the acceptance criteria.

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

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

9.2 Test documentation

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

a) the version of the test plan used;

b) the criteria for acceptance of tests;

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

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

e) the conditions of the test;

f) the test personnel;

g) the detailed results of each test;

h) any discrepancy between expected and actual results;

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

10 Modification

10.1 Objective

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

10.2 Requirements

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

10.2.1 Modification request

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

a) the reasons for the change;

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

10.2.2 Impact analysis

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

10.2.3 Authorization

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

10.2.4 Documentation

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

a) the detailed specification of the modification;

b) the results of the impact analysis;

c) all approvals for changes;

d) the test cases for components including revalidation data;

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

f) the deviation from previous operations and conditions;

g) the necessary changes to information for use;

h) all applicable development steps according to 5.2.

Annex A
(informative)

Sequential task table

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

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

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

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

	Tasks	References
1	**General requirements**	
	All relevant documents should be under the control of an appropriate document control scheme Description of project management Certification quality management system	IEC 61508-1:1998, §5 IEC 61508-2:2000, §7.3, 7.7, 7.8, 7.9 IEC 61508-3:1998, §6, 7.3, 7.4.2.1, 7.7, 7.8, 7.9
2	**Specification of PDS(SR) safety requirements**	Phase 1 of PDS(SR) safety lifecycle (see 5.2 of this standard)
	Development of a safety requirements specification (SRS) including safety functions requirements and safety integrity requirements	See 5.4 of this standard IEC 61508-1:1998, §7.6 IEC 61508-2:2000, §7.2, Tables B.1, B.6 IEC 61508-2:2000, §7.4.4-6, Annex A IEC 61508-3:1998, §7.2,Tables A.1, B.7 IEC 61508-3:1998, §7.4.2/4, Tables A.3, B.1 IEC 61508-7:2000, Table C.1 Examples in IEC 61508-5, Examples in IEC 61508-6:2000, Annex A
3	**Verification of PDS(SR) safety requirements specification**	
	a) Reviews of the safety requirements specification b) Check by independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:2000 and IEC 61508-3:1998, §7.9
4	**Concept**	Phase 3 of PDS(SR) safety lifecycle (see 5.2 of this standard)
	a) Hardware design on an architectural level, including • 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*	a) See Clause 6 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

	Tasks	References
	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.	b) IEC 61508-2:2000, §7.2.3.1(h) IEC 61508-3:1998, §7.2.2.8, 7.2.2.10, 7.4.2/3, Tables A.2, B.1, B.7, B.9 IEC 61508-7:2000, Table C.1
	c) Recommendation Pre-estimation of the probability of failure of safety functions due to random hardware failures on a level of functional block diagrams	c) IEC 61508-1:1998, Table 2 IEC 61508-2:2000, §7.4.3, Tables 3, A.1, Annex C IEC 61508-3:1998, Table B.4 (FMEA) Examples in IEC 61508-6:2000, Annexes C and D
5	**Verification of concept**	
	a) Reviews of system design b) Check by independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:2000 and IEC 61508-3:1998, §7.9
6	**Validation planning**	Phase 2 of PDS(SR) safety lifecycle (see 5.2 of this standard)
	a) Detailed planning of the validation of safety related PDS(SR). b) The validation plan should be generated in parallel to Phase 9.3 Design and Development.	a) See 8.3 of this standard b) IEC 61508-2:2000, §7.3, Table B.5 IEC 61508-3:1998, §7.3, Tables A.7, B.3, B.5
7	**Verification of validation plan**	
	a) Reviews of the validation plan b) Check by independent person or department where required	a) See 8.2 of this standard b) IEC 61508-2:2000 and IEC 61508-3:1998, §7.9
8	**Design and development**	Phase 3 of PDS(SR) safety lifecycle (see 5.2 of this standard)
		See Clause 6 of this standard
	a) Hardware design	a) IEC 61508-2:2000, §7.4, Annex A, Table B.2, B.3, B.6
	b) Software design	b) IEC 61508-3:1998, §7.4.5, 7.4.6, Table A.4
	c) Reliability Prediction (calculation of the probability of failure of safety functions due to random hardware failures) including: • type of PDS(SR) • SFF • functional block diagram • reliability model • data basis of the model (device lists) • PFH calculation • mission time • repair interval, proof test interval (if relevant)	c) IEC 61508-1:1998, Table 2 IEC 61508-2:2000, §7.4.3, 7.4.7, Table 3, A.1, Annex C IEC 61508-3:1998, Table B.4 (FMEA) Examples in IEC 61508-6:2000, Annexes C and D

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

Annex B
(informative)

Example for determination of *PFH*

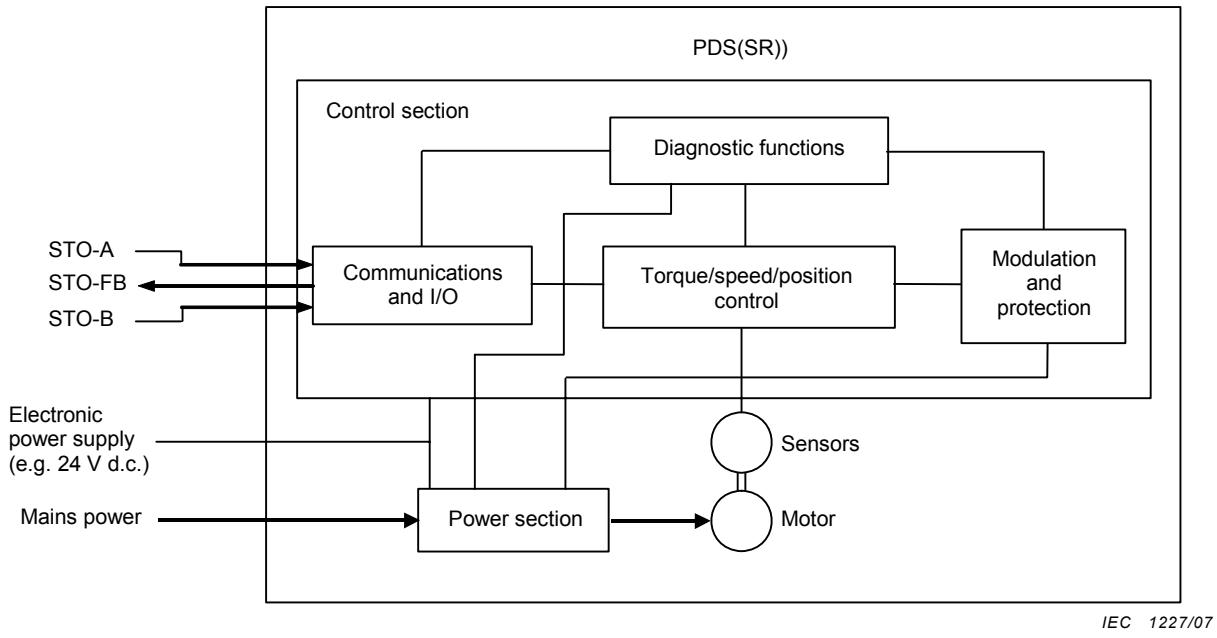
B.1 General

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

B.2 Example PDS(SR) structure

B.2.1 General

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



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

Figure B.1 – Example PDS(SR)

The example requirements are:

– SIL 2;

– continuous mode of operation.

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

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

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

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

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

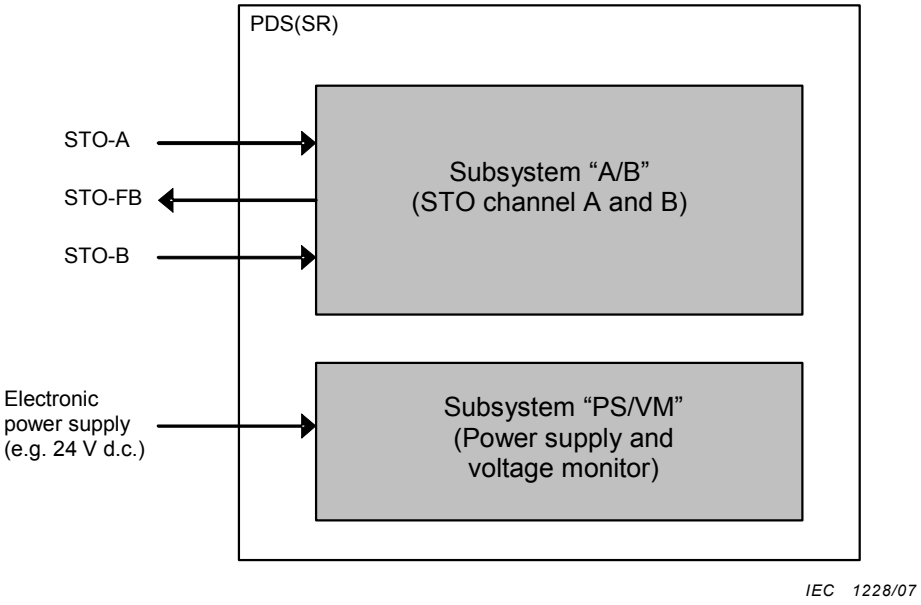


Figure B.2 – Subsystems of the PDS(SR)

B.2.2 Subsystem A/B

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

— type B (complex hardware);

— hardware fault tolerance of 1 (two channel implementation).

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

B.2.3 Subsystem PS/VM

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

— type B (complex hardware);

— hardware fault tolerance of 0 (single channel implementation).

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

B.3 Example PDS(SR) PFH value determination

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

B.3.1.1 Function block division

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

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

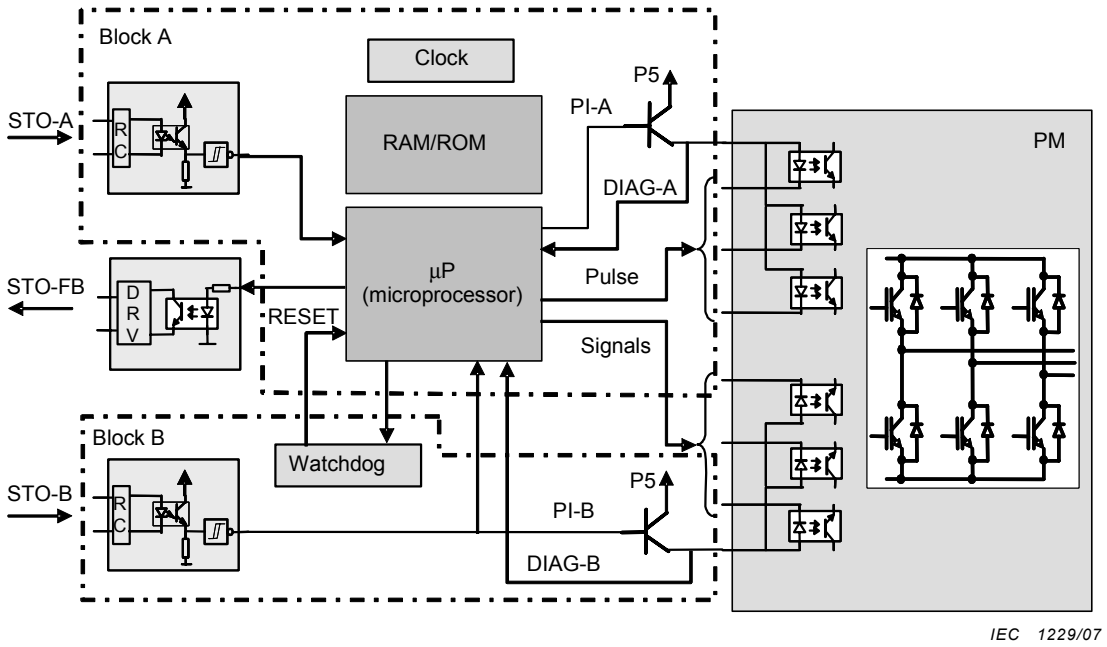


Figure B.3 – Function blocks of subsystem A/B

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

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

B.3.1.2 Determination of failure rates of function blocks

B.3.1.2.1 Function block analysis

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

B.3.1.2.2 Component FMEA

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

In addition, the FMEA identifies the proportion of the *dangerous failure* rate of each component which is detected by the available diagnosis functionality. For complex components, the portion of detected *dangerous failure*s has to be defined using the tables in IEC 61508-2. This proportioning defines the failure rates λ_{DD} (dangerous detectable) and λ_{DU} (dangerous undetectable) 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 Annex C of IEC 61508-6:2000, may be selected.

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

This method will also lead to the failure rates λ_S, λ_{DD} and λ_{DU} of the function block.

B.3.1.3 Safe failure fraction

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

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

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

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

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

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

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

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

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

Block A:	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 item g) of Clause C.1 of IEC 61508-2:2000, is:

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

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

= 494 FIT / 520 FIT;

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

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

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

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

B.3.1.5 Reliability model (Markov)

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

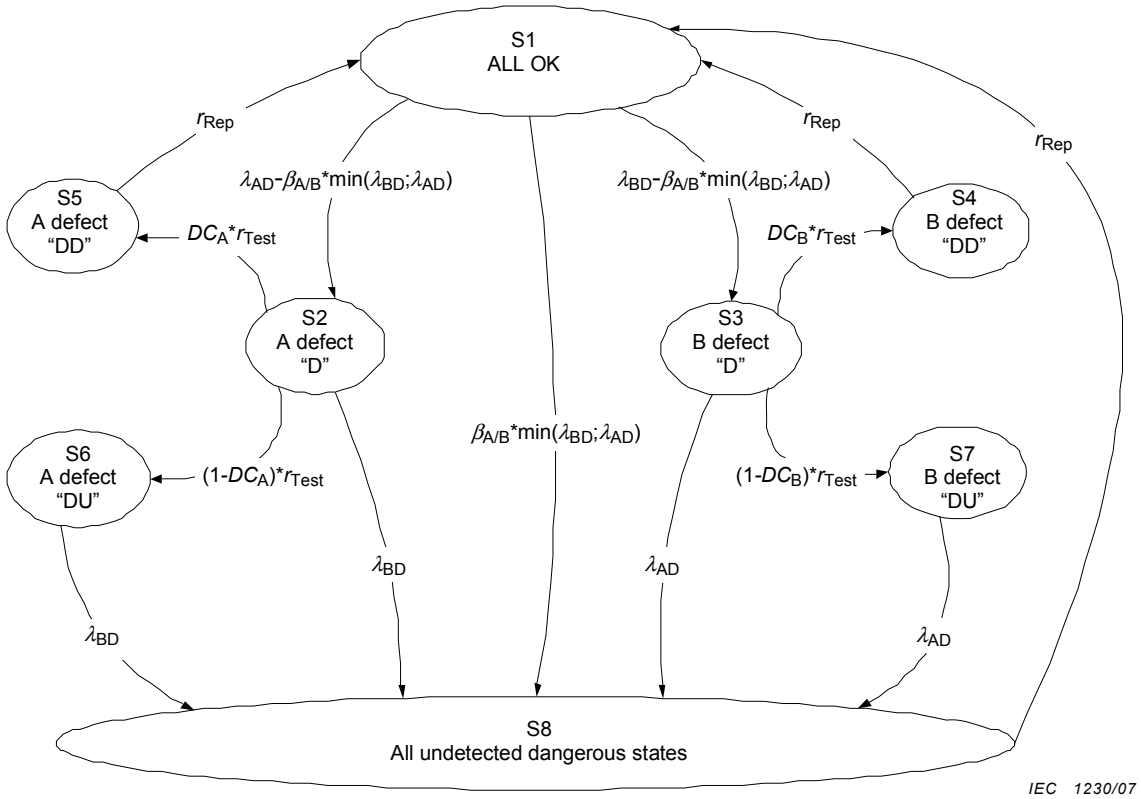


Figure B.4 – Reliability model (Markov) of subsystem A/B

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

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

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

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

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

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

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

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

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

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

B.3.1.6 PFH value calculation

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 [Si] of the Markov model has to be calculated. The starting probability value of all states except state S1 is equal to zero. The starting probability value of state S1 is equal to one. The calculation has to be done up to the mission time T_M.

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

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

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

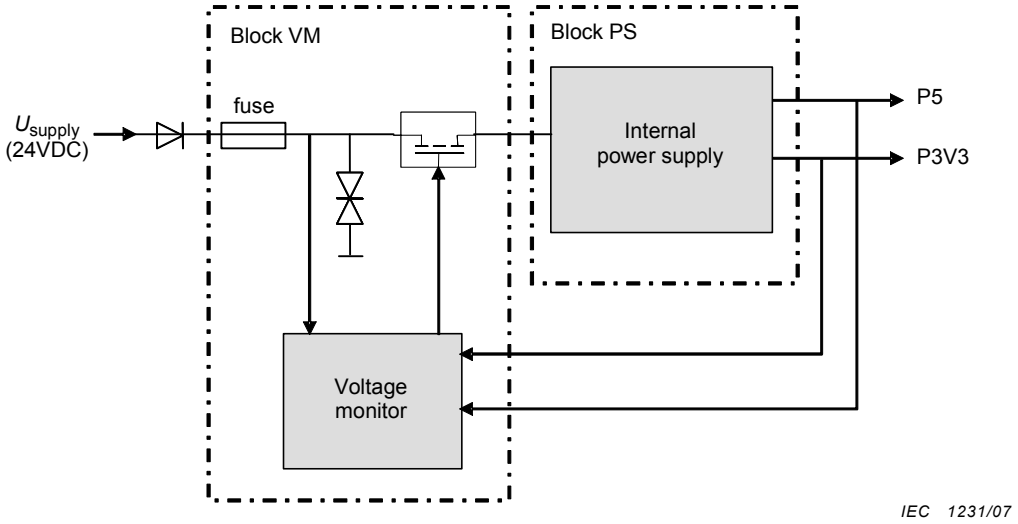
$\beta_{A/B}$	r_{Rep}	r_{Test}	T_M (years)	$PFH_{A/B}$
2 %	1/8 h	1/8 h	10	6.84×10^{-10} /h
2 %	1/8 h	**1/24 h**	10	6.84×10^{-10} /h
2 %	1/8 h	**1/168 h**	10	6.86×10^{-10} /h
2 %	1/8 h	**1/672 h**	10	6.91×10^{-10} /h
2 %	1/8 h	**1/8760 h**	10	7.72×10^{-10} /h
2 %	**1/8760 h**	1/8 h	10	6.83×10^{-10} /h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

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

B.3.2 Subsystem "PS/VM"

B.3.2.1 Function block division

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



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

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

B.3.2.2 Failure rates of function blocks

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

B.3.2.3 Safe failure fraction

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

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

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

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

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

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

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

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

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

Block PS:	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 item g) of Clause C.1 of IEC 61508-2:2000 (see NOTE):

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

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

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

NOTE The monitor block does not contribute to the SFF.

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

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

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

B.3.2.5 Reliability model (Markov)

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

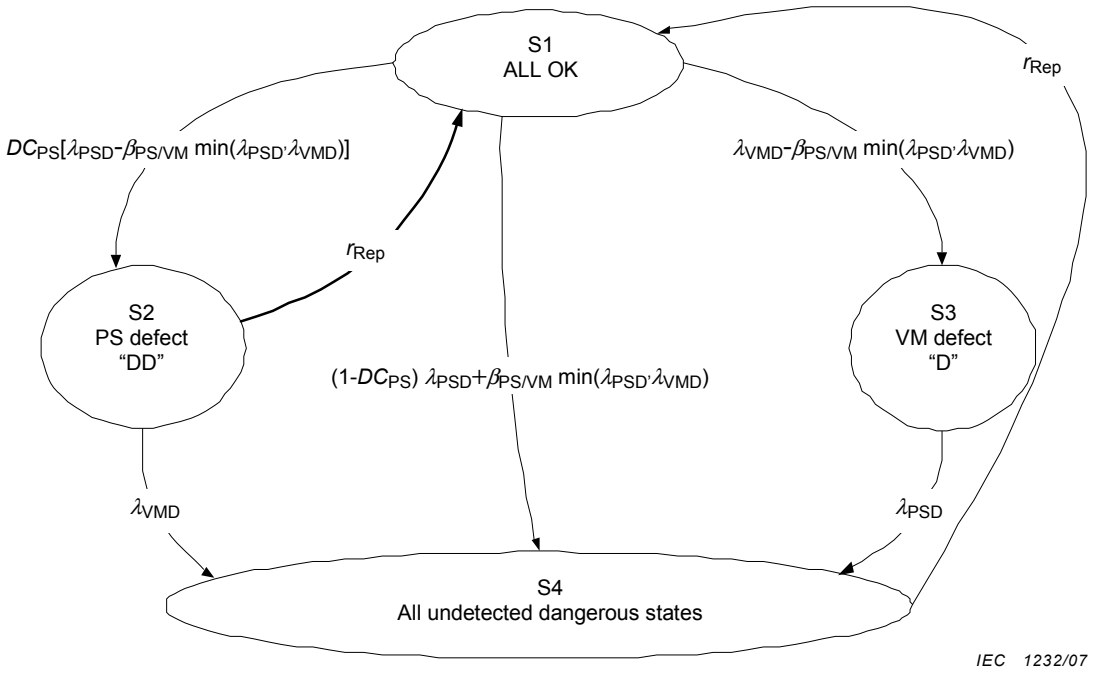


Figure B.6 – Reliability model (Markov) of subsystem PS/VM

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

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

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

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

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

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

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

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

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

B.3.2.6 PFH value calculation

λ values, DC and β factors are given in B.3.2.3 and B.3.2.4:

Additional determinations:

— r_{Rep} = 1/8 h (repair rate)

— T_M = 10 years or 20 years; (mission time).

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

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

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

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

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

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

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

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

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

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

Annex C
(informative)

Available failure rate databases

C.1 Databases

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

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

C.2 Helpful standards concerning component failure

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

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

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

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

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

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

Annex D
(informative)

Fault lists and fault exclusions

D.1 General

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

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

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

D.2 Remarks applicable to fault exclusions

D.2.1 Validity of exclusions

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

D.2.2 Tin whisker growth

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

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

NOTE 2 The following publications may be helpful for evaluation:

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

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

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

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

D.2.3 Short-circuits on PWB-mounted parts

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

D.3 Fault models

Table D.1 – Conductors/cables

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

Table D.2 – Printed wiring boards/assemblies

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

Table D.3 – Terminal block

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

Table D.4 – Multi-pin connector

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

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

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

Table D.6 – Transformers

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

Table D.7 – Inductances

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

Table D.8 – Resistors

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

Table D.9 – Resistor networks

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

Table D.10 – Potentiometers

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

Table D.11 – Capacitors

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

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

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

Table D.13 – Optocouplers

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

Table D.14 – Non-programmable integrated circuits

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

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

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

Table D.16 – Motion and position feedback sensors

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

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

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

Bibliography

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

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

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

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

IEC 61025, *Fault tree analysis (FTA)*

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

IEC 61165, *Application of Markov techniques*

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

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

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

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

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

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

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

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

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

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

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

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

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

ISBN 2-8318-9227-9

ICS 29.200; 13.110

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND