

Adjustable speed electrical power drive systems —

Part 5-2: Safety requirements — Functional

The European Standard EN 61800-5-2:2007 has the status of a
British Standard

ICS 13.110; 29.200

National foreword

This British Standard is the UK implementation of EN 61800-5-2:2007. It is identical to IEC 61800-5-2:2007.

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

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

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

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2007

© BSI 2007

ISBN 978 0 580 55410 0

Amendments issued since publication

Amd. No.	Date	Comments

**Adjustable speed electrical power drive systems -
Part 5-2: Safety requirements -
Functional
(IEC 61800-5-2:2007)**

Entraînements électriques de puissance
à vitesse variable -
Partie 5-2: Exigences de sécurité -
Fonctionnalité
(CEI 61800-5-2:2007)

Elektrische Leistungsantriebssysteme
mit einstellbarer Drehzahl -
Teil 5-2: Anforderungen an die Sicherheit -
Funktionale Sicherheit
(IEC 61800-5-2:2007)

This European Standard was approved by CENELEC on 2007-10-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of document 22G/179/FDIS, future edition 1 of IEC 61800-5-2, prepared by SC 22G, Adjustable speed electric drive systems incorporating semiconductor power converters, of IEC TC 22, Power electronic systems and equipment, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61800-5-2 on 2007-10-01.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2008-07-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2010-10-01

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EC Directives 98/37/EC and 2006/42/EC. See Annex ZZ.

Annexes ZA and ZZ have been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61800-5-2:2007 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION.....	6
1 Scope and object.....	7
2 Normative references	8
3 Terms and definitions	9
4 Designated safety functions.....	14
4.1 General.....	14
4.2 Safety functions	15
4.2.1 Limit values	15
4.2.2 Stopping functions.....	15
4.2.3 Other safety functions.....	16
5 Management of functional safety	17
5.1 Objective	17
5.2 PDS(SR) development lifecycle	17
5.3 Functional safety planning.....	18
5.4 Safety requirements specification (SRS) for a PDS(SR)	20
5.4.1 General	20
5.4.2 Safety functionality requirements specification	20
5.4.3 Safety integrity requirements specification.....	21
6 Requirements for design and development of a PDS(SR)	21
6.1 General requirements.....	21
6.1.1 Change in operational status	21
6.1.2 Design standards.....	21
6.1.3 Realisation	22
6.1.4 Safety integrity and fault detection.....	22
6.1.5 Safety and non-safety functions.....	22
6.1.6 SIL to be used	22
6.1.7 Software requirements.....	22
6.1.8 Review of requirements	22
6.1.9 Design documentation	23
6.2 PDS(SR) design requirements.....	23
6.2.1 Requirements for probability of dangerous random hardware failures per hour (PFH)	23
6.2.2 Architectural constraints	25
6.2.3 Estimation of safe failure fraction (SFF).....	27
6.2.4 Requirements for systematic safety integrity of a PDS(SR) and PDS(SR) subsystems	27
6.2.5 Electromagnetic (EM) immunity requirement of a PDS(SR).....	30
6.3 Behaviour on detection of fault	30
6.3.1 Fault detection.....	30
6.3.2 Fault tolerance greater than zero.....	31
6.3.3 Fault tolerance zero.....	31
6.4 Additional requirements for data communications.....	31
6.5 PDS(SR) integration and testing requirements	32
6.5.1 Hardware integration	32

6.5.2	Software integration	32
6.5.3	Modifications during integration	32
6.5.4	Applicable integration tests	32
6.5.5	Test documentation	33
7	Information for use	33
7.1	Information and instructions for safe application of a PDS(SR)	33
8	Verification and validation	34
8.1	General	34
8.2	Verification	35
8.3	Validation	35
8.4	Documentation	35
9	Test requirements	35
9.1	Planning of tests	35
9.2	Test documentation	35
10	Modification	36
10.1	Objective	36
10.2	Requirements	36
10.2.1	Modification request	36
10.2.2	Impact analysis	36
10.2.3	Authorization	36
10.2.4	Documentation	36
Annex A (informative)	Sequential task table	37
Annex B (informative)	Example for determination of <i>PFH</i>	40
Annex C (informative)	Available failure rate databases	51
Annex D (informative)	Fault lists and fault exclusions	53
Annex ZA (normative)	Normative references to international publications with their corresponding European publications	65
Annex ZZ (informative)	Coverage of Essential Requirements of EC Directives	67
Annex ZZA (informative)	Coverage of Essential Requirements of Directive 98/37/EC	67
Annex ZZB (informative)	Coverage of Essential Requirements of Directive 2006/42/EC	67
Bibliography		63
Figure 1	– Functional elements of a PDS(SR)	8
Figure 2	– PDS(SR) development lifecycle	18
Figure 3	– Architectures for data communication (a) White channel; b) Black channel)	32
Figure B.1	– Example PDS(SR)	40
Figure B.2	– Subsystems of the PDS(SR)	41
Figure B.3	– Function blocks of subsystem A/B	42
Figure B.4	– Reliability model (Markov) of subsystem A/B	45
Figure B.5	– Function blocks of subsystem PS/VM	47
Figure B.6	– Reliability model (Markov) of subsystem PS/VM	49

Table 1 – Alphabetical list of definitions	10
Table 2 – Safety integrity levels: target failure measures for a PDS(SR) safety function	23
Table 3 – Hardware safety integrity: architectural constraints on type A safety-related subsystems.....	26
Table 4 – Hardware safety integrity: architectural constraints on type B safety-related subsystems.....	27
Table B.1 – Determination of DC factor of subsystem A/B.....	44
Table B.2 – PFH value calculation results for subsystem A/B.....	46
Table B.3 – Determination of DC factor of subsystem A/B.....	47
Table B.4 – PFH value calculation results for subsystem PS/VM.....	50
Table D.1 – Conductors/cables	54
Table D.2 – Printed wiring boards/assemblies.....	54
Table D.3 – Terminal block	55
Table D.4 – Multi-pin connector	55
Table D.5 – Electromechanical devices (for example relay, contactor relays).....	56
Table D.6 – Transformers	56
Table D.7 – Inductances	57
Table D.8 – Resistors	57
Table D.9 – Resistor networks	57
Table D.10 – Potentiometers.....	58
Table D.11 – Capacitors	58
Table D.12 – Discrete semiconductors (for example diodes, Zener diodes, transistors, triacs, GTO thyristors, IGBTs, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs]).....	58
Table D.13 – Optocouplers	59
Table D.14 – Non-programmable integrated circuits.....	59
Table D.15 – Programmable and/or complex integrated circuits	60
Table D.16 – Motion and position feedback sensors	61

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.

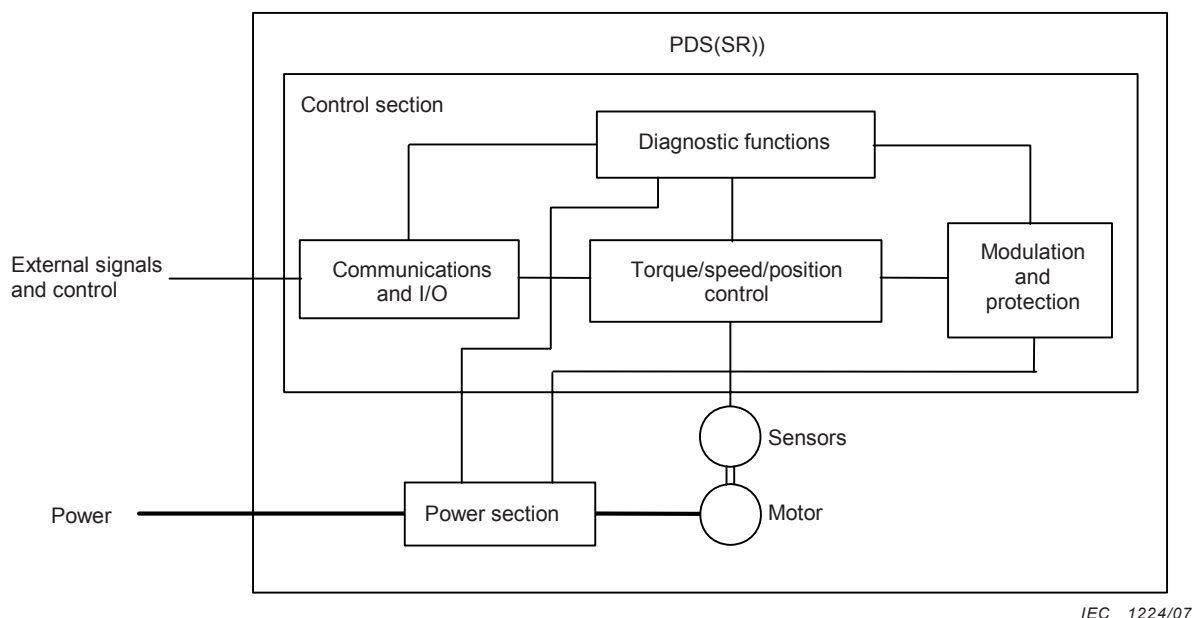


Figure 1 – Functional elements of a PDS(SR)

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 failures* of a PDS(SR) subsystem to the total average failure rate of that subsystem

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

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

3.16**safety function(s) (of a PDS(SR))**

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

3.17**safety integrity**

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

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

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

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

3.18**safety integrity level****SIL**

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

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

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

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

3.19

safety-related system

designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and
- is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

3.20

safety requirements specification

SRS

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

3.21

SIL capability

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

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

3.22

subsystem

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

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

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

3.23

systematic failure

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

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

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

(IEC 61508-4:1998; definition 3.6.6)

3.24

systematic safety integrity

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

(IEC 61508-4:1998; definition 3.5.4)

NOTE Systematic safety integrity cannot usually be quantified.

3.25

validation

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

(IEC 61508-4:1998; definition 3.8.2)

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

3.26

verification

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

(IEC 61508-4:1998; definition 3.8.1)

4 Designated safety functions

4.1 General

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

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

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

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

- the reaction on violation of limits (only relevant for monitoring functions):
the reaction function when a violation of limits is detected during the correct operation of the safety function; and
- the fault reaction function:
the reaction function when diagnostics detect a fault within the safety function.

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

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

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

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

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

4.2 Safety functions

4.2.1 Limit values

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

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

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

4.2.2 Stopping functions

4.2.2.1 General

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

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

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

4.2.2.2 Safe torque off (STO)

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

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

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

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

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

4.2.2.3 Safe stop 1 (SS1)

The PDS(SR) either

- a) initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the STO function (see 4.2.2.2) when the motor speed is below a specified limit; or
- b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit; or
- c) initiates the motor deceleration and initiates the STO function after an application specific time delay.

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

4.2.2.4 Safe stop 2 (SS2)

The PDS(SR) either

- a) initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function (see 4.2.3.1) when the motor speed is below a specified limit; or
- b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit; or
- c) initiates the motor deceleration and initiates the safe operating stop function after an application specific time delay.

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

4.2.3 Other safety functions

4.2.3.1 Safe operating stop (SOS)

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

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

4.2.3.2 Safely-limited acceleration (SLA)

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

4.2.3.3 Safe acceleration range (SAR)

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

4.2.3.4 Safely-limited speed (SLS)

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

4.2.3.5 Safe speed range (SSR)

The SSR function keeps the motor speed within specified limits.

4.2.3.6 Safely-limited torque (SLT)

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

4.2.3.7 Safe torque range (STR)

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

4.2.3.8 Safely-limited position (SLP)

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

4.2.3.9 Safely-limited increment (SLI)

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

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

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

4.2.3.10 Safe direction (SDI)

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

4.2.3.11 Safe motor temperature (SMT)

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

4.2.3.12 Safe brake control (SBC)

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

4.2.3.13 Safe cam (SCA)

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

4.2.3.14 Safe speed monitor (SSM)

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

5 Management of functional safety

5.1 Objective

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

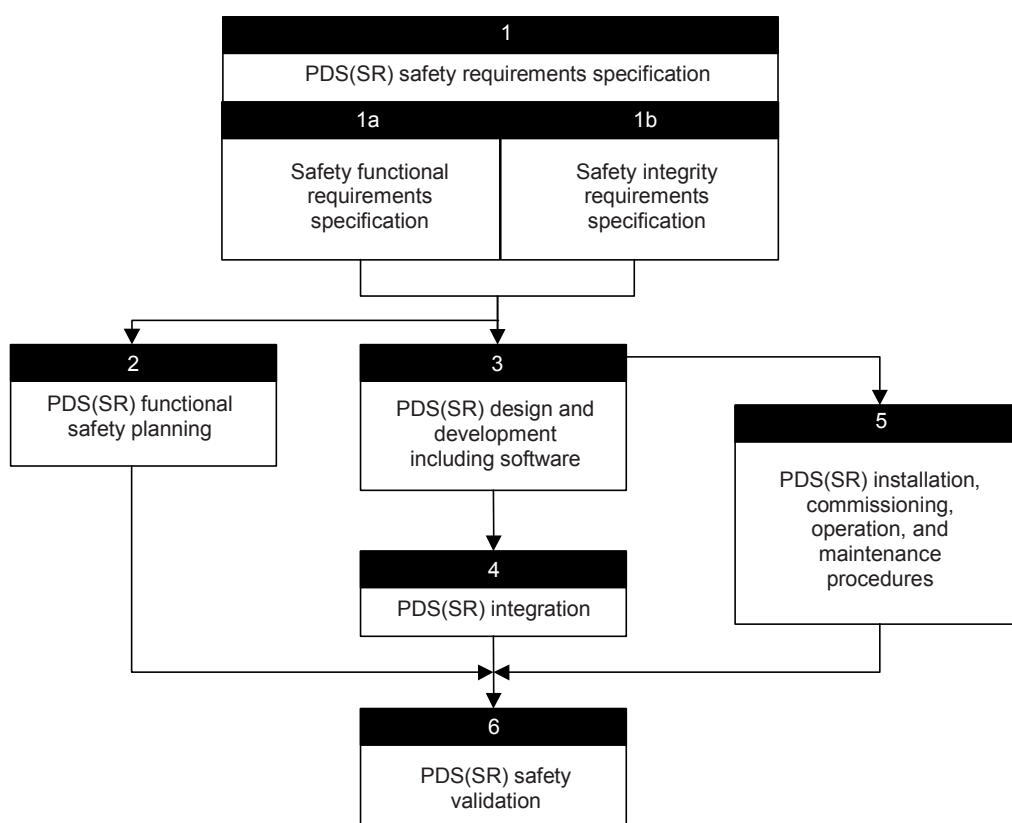
NOTE This clause is solely aimed at the achievement of the functional safety of the PDS(SR) and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

5.2 PDS(SR) development lifecycle

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

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

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



IEC 1225/07

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;