IEC 61800-5-2

Edition 2.0 2016-04
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

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

IEC 60000:2016-01 RLV(en)

Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

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

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

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

Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

IEC 61800-5-2

Edition 2.0 2016-04
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 29.200

ISBN 978-2-8322-3353-5

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

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

CONTENTS

FOREWORD 7
INTRODUCTION 10
1 Scope ~~and object~~ 11
2 Normative references 12
3 Terms and definitions 14
4 Designated *safety sub-functions* 22
4.1 General 22
4.2 *Safety sub-functions* 23
4.2.1 General 23
4.2.2 Limit values 23
4.2.3 Stopping functions 23
4.2.4 ~~Other safety~~ Monitoring functions 25
4.2.5 Output functions – Safe brake control (SBC) 26
5 Management of *functional safety* 26
5.1 Objective 26
5.2 Requirements for the management of *functional safety* 27
5.3 *PDS(SR)* development lifecycle 27
5.4 ~~Functional safety~~ Planning of PDS(SR) functional safety management 28
5.5 Safety requirements specification (*SRS*) for a *PDS(SR)* 30
5.5.1 General 30
5.5.2 *Safety ~~functionality~~ sub-functions* requirements specification 30
5.5.3 *Safety integrity* requirements specification 31
5.6 *PDS(SR)* safety system architecture specification 32
5.6.1 General 32
5.6.2 Requirements for safety system architecture specification 32
6 Requirements for design and development of a *PDS(SR)* 33
6.1 General requirements 33
6.1.1 Change in operational status 33
6.1.2 Design standards 33
6.1.3 Realisation 33
6.1.4 *Safety integrity* and fault detection 33
6.1.5 Safety and non-*safety sub-functions* 34
6.1.6 *SIL ~~to be used~~* for multiple *safety sub-functions* within one PDS(SR) 34
6.1.7 Integrated circuits with on-chip redundancy 35
6.1.8 Software requirements 35
~~6.1.8 Review of requirements ..... 35~~
6.1.9 Design documentation 35
6.2 *PDS(SR)* design requirements 36
6.2.1 Basic and well-tried safety principles 36
6.2.2 Requirements for the estimation of the probability of dangerous random hardware failures per hour (*PFH*) 36
6.2.3 Architectural constraints 38
6.2.4 Estimation of *safe failure fraction (SFF)* 41
~~6.2.5 Electromagnetic (EM) immunity requirement of a PDS(SR) ..... 41~~
6.2.5 Requirements for *systematic safety integrity* of a *PDS(SR)* and *PDS(SR) subsystems* 41

AVA Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

6.2.6 Design requirements for electromagnetic (EM) immunity of a *PDS(SR)*.....45
6.2.7 Design requirements for thermal immunity of a *PDS(SR)*.....45
6.2.8 Design requirements for mechanical immunity of a *PDS(SR)*.....45
6.3 Behaviour on detection of fault.....45
6.3.1 Fault detection.....45
6.3.2 Fault tolerance greater than zero.....46
6.3.3 Fault tolerance zero.....46
6.4 Additional requirements for data communications.....46
6.5 *PDS(SR)* integration and testing requirements.....47
6.5.1 Hardware integration.....47
6.5.2 Software integration.....47
6.5.3 Modifications during integration.....47
6.5.4 Applicable integration tests.....47
6.5.5 Test documentation.....48
7 Information for use.....48
7.1 General.....48
7.2 Information and instructions for safe application of a *PDS(SR)*.....48
8 *Verification* and *validation*.....50
8.1 General.....50
8.2 *Verification*.....50
8.3 *Validation*.....50
8.4 Documentation.....50
9 Test requirements.....51
9.1 Planning of tests.....51
9.2 Functional testing.....51
9.3 Electromagnetic (EM) immunity testing.....51
9.3.1 General.....51
9.3.2 Intended EM environment.....51
9.3.3 Performance criterion (fail safe state – FS).....52
9.4 Thermal immunity testing.....52
9.4.1 General.....52
9.4.2 Functional thermal test.....52
9.4.3 Component thermal test.....52
9.5 Mechanical immunity testing.....52
9.5.1 General.....52
9.5.2 Vibration test.....53
9.5.3 Shock test.....53
9.5.4 Performance criterion for mechanical immunity tests (fail safe state – FS).....53
9.6 Test documentation.....53
10 Modification.....53
10.1 Objective.....53
10.2 Requirements.....53
10.2.1 General.....53
10.2.2 Modification request.....54
10.2.3 Impact analysis.....54
10.2.4 Authorization.....54
10.2.5 Documentation.....54

AVA Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

Annex A (informative) Sequential task table 55
Annex B (informative) Example for ~~determination~~ estimation of *PFH* 60
B.1 General 60
B.2 Example *PDS(SR)* structure 60
B.2.1 General 60
B.2.2 *Subsystem* A/B 61
B.2.3 *Subsystem* PS/VM 61
B.3 Example PDS(SR) PFH value determination 62
B.3.1 *Subsystem* "A/B" (main *subsystem*) 62
B.3.2 *Subsystem* "PS/VM" 67
B.3.3 *PFH* value of the *safety sub-function* STO of *PDS(SR)* 71
B.4 Reduction of DC and SFF depending on test interval 71
Annex C (informative) Available failure rate databases 73
C.1 Databases 73
C.2 Helpful standards concerning component failure 74
Annex D (informative) Fault lists and fault exclusions 75
D.1 General 75
D.2 Remarks applicable to fault exclusions 75
D.2.1 Validity of exclusions 75
D.2.2 Tin whisker growth 75
D.2.3 Short-circuits on PWB-mounted parts 75
D.3 Fault models 76
D.3.1 Conductors/cables 76
D.3.2 Printed wiring boards/assemblies 76
D.3.3 Terminal block 77
D.3.4 Multi-pin connector 77
D.3.5 Electromechanical devices 78
D.3.6 Transformers 82
D.3.7 Inductances 82
D.3.8 Resistors 82
D.3.9 Resistor Networks 82
D.3.10 Potentiometers 82
D.3.11 Capacitors 82
D.3.12 Discrete semiconductors 82
D.3.13 Signal Isolation components 82
D.3.14 Non-programmable integrated circuits 83
D.3.15 Programmable and/or complex integrated circuits 84
D.3.16 Motion and position feedback sensors 84
Annex E (normative) Electromagnetic (EM) immunity requirement for *PDS(SR)* 89
E.1 General 89
E.2 Immunity requirements – low frequency disturbances 89
E.3 Immunity requirements – high frequency disturbances 92
Annex F (informative) Estimation of PFD_{avg} value for low demand with given PFH value 96
F.1 General 96
F.2 Estimation of PFD_{avg} value for low demand with given PFH value 96
Bibliography 97

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

Figure 1 – Installation and functional ~~elements~~ parts of a *PDS(SR)* 12
Figure 2 – *Safety function* consisting of *safety sub-functions* 23
~~Figure 3 – Architectures for data communication (a) White channel; b) Black channel) .....~~
Figure 3 – *PDS(SR)* development lifecycle 27
Figure B.1 – Example *PDS(SR)* 60
Figure B.2 – *Subsystems* of the *PDS(SR)* 61
Figure B.3 – Function blocks of *subsystem* A/B 62
Figure B.4 – Reliability model (Markov) of *subsystem* A/B 65
Figure B.5 – Function blocks of *subsystem* PS/VM 68
Figure B.6 – Reliability model (Markov) of *subsystem* PS/VM 70

Table 1 – Alphabetical list of terms and definitions 13
Table 2 – Example for determining the *SIL* from hardware and software independence 32
Table 3 – *Safety integrity levels*: target failure measures for a *PDS(SR)* *safety sub-function* 33
Table 4 – ~~Hardware safety integrity: architectural constraints on type A safety-related subsystems~~ Maximum allowable safety integrity level for a *safety sub-function* carried out by a type A safety-related *subsystem* 36
Table 5 – ~~Hardware safety integrity: architectural constraints on type B safety-related subsystems~~ Maximum allowable safety integrity level for a *safety sub-function* carried out by a type B safety-related *subsystem* 37
Table A.1 – Design and development procedure for *PDS(SR)* 50
Table B.1 – Determination of DC factor of subsystem A/B 59
Table B.2 – *PFH* value calculation results for *subsystem* A/B 62
Table B.3 – Determination of DC factor of *subsystem* A/B 63
Table B.4 – *PFH* value calculation results for *subsystem* PS/VM 66
~~Table D.1 – Conductors/cables .....~~
Table D.1 – Printed wiring boards/assemblies 71
Table D.2 – Terminal block 72
Table D.3 – Multi-pin connector 72
Table D.4 – Electromechanical devices (for example relay, contactor relays) 73
Table D.5 – Signal Isolation components 76
~~Table D.6 – Transformers .....~~
~~Table D.7 – Inductances .....~~
~~Table D.8 – Resistors .....~~
~~Table D.9 – Resistor networks .....~~
~~Table D.10 – Potentiometers .....~~
~~Table D.11 – Capacitors .....~~
~~Table D.12 – Discrete semiconductors (for example diodes, Zener diodes, transistors, triacs, GTO thyristors, IGBTs, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs]) .....~~
~~Table D.13 – Optocouplers .....~~
Table D.6 – Non-programmable integrated circuits 77
Table D.7 – Programmable and/or complex integrated circuits 78
Table D.8 – Motion and position feedback sensors 79

AVA Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

Table E.1 – Minimum immunity requirements for voltage deviations, dips and short interruptions 84
Table E.2 – *PDS(SR)* minimum immunity requirements for voltage deviations, dips and short interruptions on main power ports with a rated voltage above 1 000 V 85
Table E.3 – Immunity requirements – high frequency disturbances 86
Table E.4 – General frequency ranges for mobile transmitters and ISM for radiated tests 88
Table E.5 – General frequency ranges for mobile transmitters and ISM for conducted tests 89

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-2: Safety requirements – Functional

FOREWORD

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

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

Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

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

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

a) rational added in the scope why low demand mode is not covered by this standard
b) definition added for: "*category*" and "*safety function*"
c) "Other sub-functions" sorted into "Monitoring sub-functions" and "Output functions"
d) deleted "proof test" throughout the document because for *PDS(SR)* a proof test is not applicable
e) replaced the term "safety function" by "*safety sub-function*" throughout the document
f) Updated references to IEC 61508 series Ed.2010
g) Added the principle rules of ISO 13849-1 and reference to tables of ISO 13849-2
h) 6.1.6 Text replaced by Table 2
i) 6.1.7 Integrated circuits with on-chip redundancy matched to changed requirement in IEC 61508-2: 2010, Annex E
j) 6.2.8 Design requirements for thermal immunity of a *PDS(SR)*
k) 6.2.9 Design requirements for mechanical immunity of a *PDS(SR)*
l) 6.1.6 *SIL* for multiple *safety sub-functions* within one *PDS(SR)*
m) 6.1.7 Integrated circuits with on-chip redundancy
n) 6.2.1 Basic and well-tried safety principles
o) 6.2.2.1.4 *Diagnostic test* interval when the hardware fault tolerance is greater than zero
p) 6.2.5.2.7 *PDS(SR)* parameterization
q) 9 Test requirements
r) 9.3 Electromagnetic (EM) immunity testing
s) 9.4 Thermal immunity testing
t) 9.5 Mechanical immunity testing
u) Annex A Sequential task table
v) Annex D, D.3.16, Motion and position feedback sensors updated
w) Annex E Electromagnetic immunity (EM) requirement for *PDS(SR)*
x) Annex F Estimation of PFD_{avg} value for low demand with given PFH value

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

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

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

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

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

AVA Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

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

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

Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

INTRODUCTION

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

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

Examples of industrial applications are:

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

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

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

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

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

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

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

AVA Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-2: Safety requirements – Functional

1 Scope ~~and object~~

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

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

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

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

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

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

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

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

This part of IEC 61800 does not specify requirements for:

- the *hazard* and risk analysis of a particular application;
- the identification of *safety sub-function*s for that application;
- the initial allocation of *SIL*s to those *safety sub-function*s;
- the driven equipment except for interface arrangements;
- secondary *hazard*s (for example from failure in a production or manufacturing process);
- the electrical, thermal and energy safety considerations, which are covered in +IEC 61800-5-1;

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

- the *PDS(SR)* manufacturing process;
- the validity of signals and commands to the *PDS(SR)*.
- security aspects (e.g. cyber security or *PDS(SR)* security of access)

NOTE 3 The functional safety requirements of a *PDS(SR)* are dependent on the application, and ~~must~~ can be considered as a part of the overall risk assessment of the *installation*. Where the supplier of the *PDS(SR)* is not ~~also~~ responsible for the driven equipment, the *installation* designer is responsible for the risk assessment, and for specifying the functional and safety integrity requirements of the *PDS(SR)*.

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

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

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

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

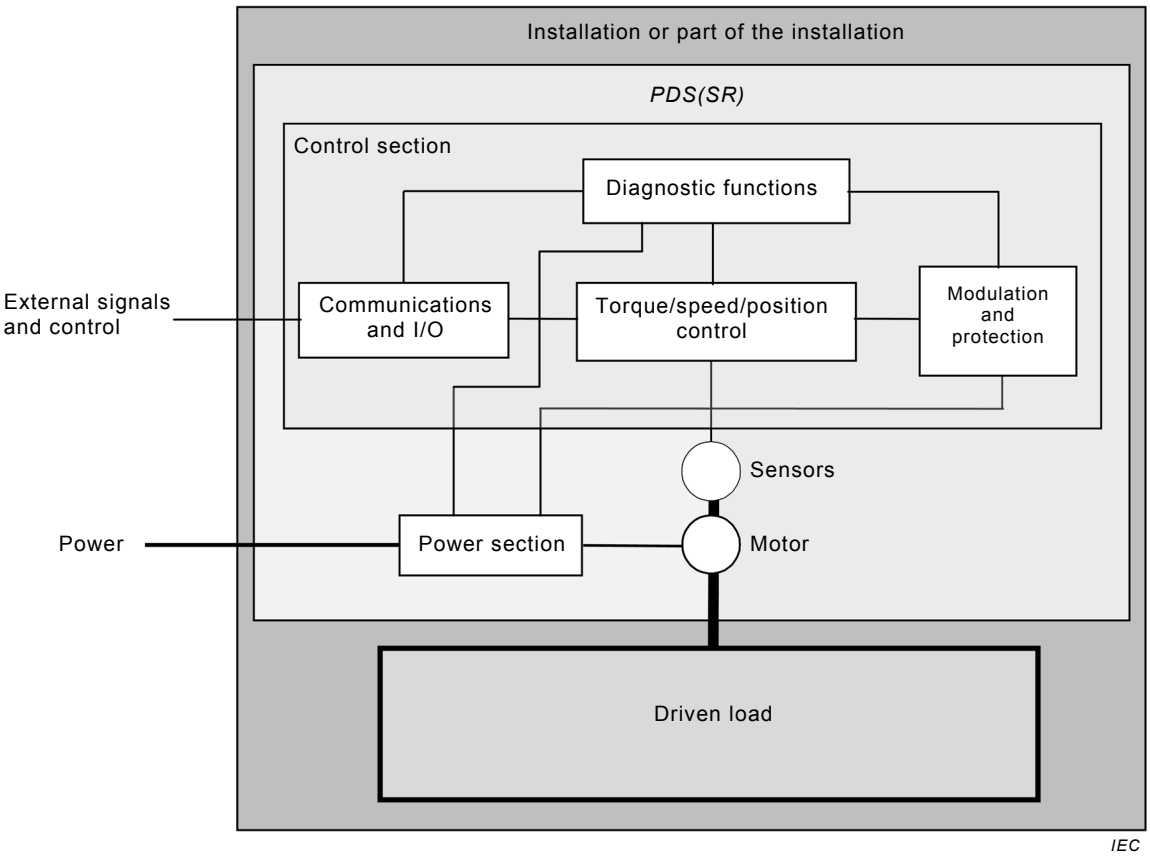


Figure 1 – Installation and functional ~~elements~~ parts of a *PDS(SR)*

2 Normative references

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEC 61508-3:~~1998~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

AVA Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

IEC 61508-6:~~2000~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:~~2000~~ 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

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

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

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

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

IEC 61800-5-1:~~2003~~ 2007, *Adjustable speed electrical power drive systems – Part 5-1: Safety requirements – Electrical, thermal and energy*

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

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

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

3 Terms and definitions

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

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

Table 1 – Alphabetical list of terms and definitions

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.7
diagnostic test~~(s)~~
test~~(s)~~ intended to detect faults or failures and produce a specified output ~~information or activity~~ when a fault or failure is detected

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

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

3.11
functional safety
part of the overall safety relating to the ~~EUC (equipment under control) and the EUC control system which depends on the correct functioning of the E/E/PE (electrical/electronic/programmable electronic) safety related systems, other technology safety related systems and external risk reduction facilities~~ *PDS(SR)* which depends on the correct functioning of the *safety-related parts of the PDS(SR)* and on external risk reduction measures

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

[SOURCE: IEC 61508-4:~~1998~~ 2010, 3.1.12, modified – "EUC and the EUC control system" replaced by "*PDS(SR)";* "E/E/PE safety-related systems and other" replaced by "*safety-related parts of the PDS(SR)* and on external"]

3.12
hazard
potential source of harm

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

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

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

3.13
installation
PDS(SR), equipment ~~or equipments including at least~~ driven by the *PDS(SR)* and ~~the driven~~ possibly other equipment (see Figure 1)

Note 1 to entry: The word "*installation*" is also used in this international standard to denote the process of installing a *PDS(SR)*. In these cases, the word ~~does not appear in italics~~ "act of installing" will be used in this standard.

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

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

Note 3 to entry: The low demand *mode of operation* is not generally considered to be relevant for *PDS(SR)* applications. Therefore, in this standard, *PDS(SR)s* are ~~only~~ mainly considered to operate in the high demand mode or continuous mode.

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

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

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

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

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

Note 1 to entry: in IEC 62061~~:2005~~, the abbreviation PFH_D is used.

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

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

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

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

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

3.18
Performance Level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a *safety sub-function* under foreseeable conditions

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

3.19
safe failure
~~failure which does not have the potential to put the safety related system in a hazardous or fail-to-function state~~
failure of a component and/or *subsystem* and/or system that plays a part in implementing the *safety sub-function* that:

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

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

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

3.20
safe failure fraction
SFF
~~ratio of the average rate of safe failures plus detected dangerous failures of a PDS(SR) subsystem to the total average failure rate of that subsystem~~
property of a safety related component and *subsystems* that is defined by the ratio of the sum of the average failure rates of safe and dangerous detected failures to the sum of safe and all dangerous failures.

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

3.23
***safety sub-function(s)*, <of a *PDS(SR)*>**
function(s) with a specified safety performance, to be implemented in whole or in part by a *PDS(SR)*, which is(are) intended to maintain the ~~safe condition~~ safety of the *installation* or prevent *hazardous* conditions arising at the *installation*

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

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

Note 1 to entry: The higher the level of *safety integrity* of the *PDS(SR)*(s), the lower the probability that the *PDS(SR)*(s) will fail to carry out the required *safety sub-function*.

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

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

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

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

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

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

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

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

3.26
safety-related system
designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the ~~EUC~~ equipment or machinery driven by the *PDS(SR)*; and
- is intended to achieve, on its own or with other ~~E/E/PE safety-related systems, other technology safety-related systems or external~~ risk reduction ~~facilities~~ measures, the necessary safety integrity for the required safety functions

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

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

3.28
SIL capability
maximum *SIL* that can be claimed to have been achieved by the design of a *PDS(SR)* in terms of the *systematic safety integrity* and the architectural constraints on hardware *safety integrity*.

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

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

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

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

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

3.30
systematic failure
failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

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

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

4 Designated *safety sub-functions*

4.1 General

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

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

Each *safety sub-function* may ~~require~~ include safe inputs and/or outputs ~~signalling~~ in order to accomplish necessary communication with (or activation of) other functions, *subsystem*s or systems (which may or may not be safety-related). ~~The integrity of the interfaces shall be included in the determination of the SIL of the associated safety function.~~

Some of the *safety sub-function*s perform monitoring tasks only; some perform safety relevant control or other actions. Therefore, a distinction ~~must~~ shall be made between:

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

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

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

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

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

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

Timing requirements for the actions required following detection of a fault are specified in the *safety requirements specification* (see 5.5).

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

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

AVA Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

4.2 *Safety sub-functions*

4.2.1 General

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

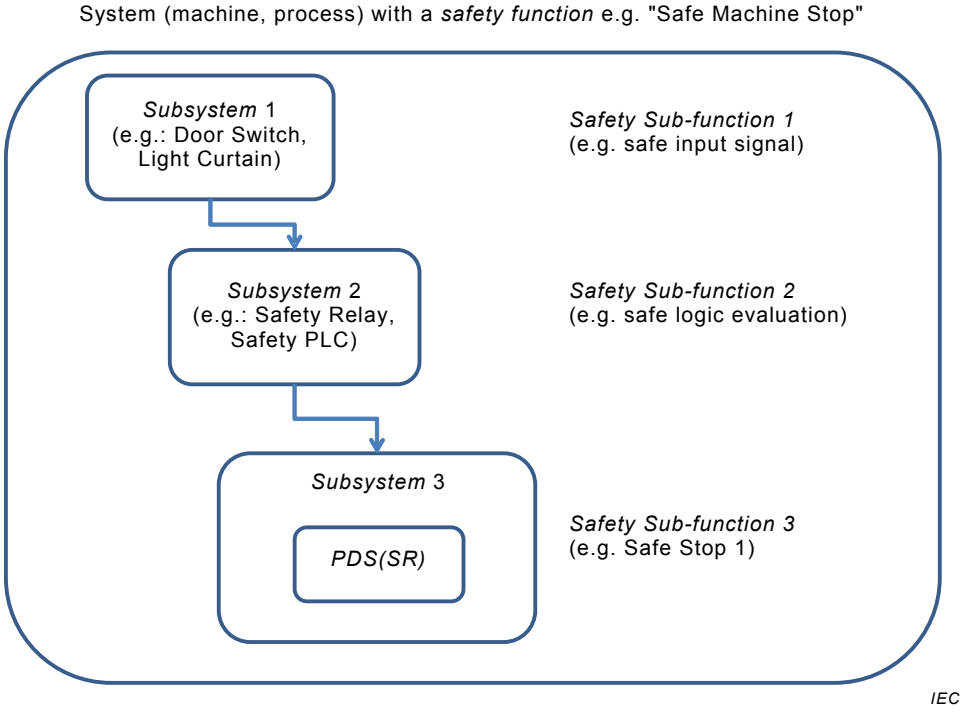


Figure 2 – *Safety function* consisting of *safety sub-functions*

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

4.2.2 Limit values

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

NOTE Specification of any limit value ~~should~~ can take into account possible exceeding of the limit value in case of violation of the limit. For example, specification of the position limit value(s) in 4.2.4.9 ~~should~~ can take into account the maximum allowable over travel distance(s).

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

4.2.3 Stopping functions

4.2.3.1 General

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

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

4.2.3.2 Safe torque off (STO)

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

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

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

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

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

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

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

4.2.3.3 Safe stop 1 (SS1)

This function is specified as either

a) Safe Stop 1 deceleration controlled

SS1-d

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

b) Safe Stop 1 ramp monitored

SS1-r

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

c) Safe Stop 1 time controlled

SS1-t

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

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

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

4.2.3.4 Safe stop 2 (SS2)

This function is specified as either

a) Safe Stop 2 deceleration controlled

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

SS2-d

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

b) Safe Stop 2 ramp monitored

SS2-r

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

c) Safe Stop 2 time controlled

SS2-t

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

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

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

4.2.4 ~~Other safety~~ Monitoring functions

4.2.4.1 General

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

4.2.4.2 Safe operating stop (SOS)

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

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

4.2.4.3 Safely-limited acceleration (SLA)

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

4.2.4.4 Safe acceleration range (SAR)

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

4.2.4.5 Safely-limited speed (SLS)

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

4.2.4.6 Safe speed range (SSR)

This function keeps the motor speed within specified limits.

4.2.4.7 Safely-limited torque (SLT)

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

4.2.4.8 Safe torque range (STR)

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

4.2.4.9 Safely-limited position (SLP)

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

4.2.4.10 Safely-limited increment (SLI)

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

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

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

4.2.4.11 Safe direction (SDI)

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

4.2.4.12 Safe motor temperature (SMT)

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

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

~~**4.2.3.12 Safe brake control (SBC)**~~

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

4.2.4.13 Safe cam (SCA)

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

4.2.4.14 Safe speed monitor (SSM)

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

4.2.5 Output functions – Safe brake control (SBC)

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

5 Management of *functional safety*

5.1 Objective

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

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

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

5.2 Requirements for the management of *functional safety*

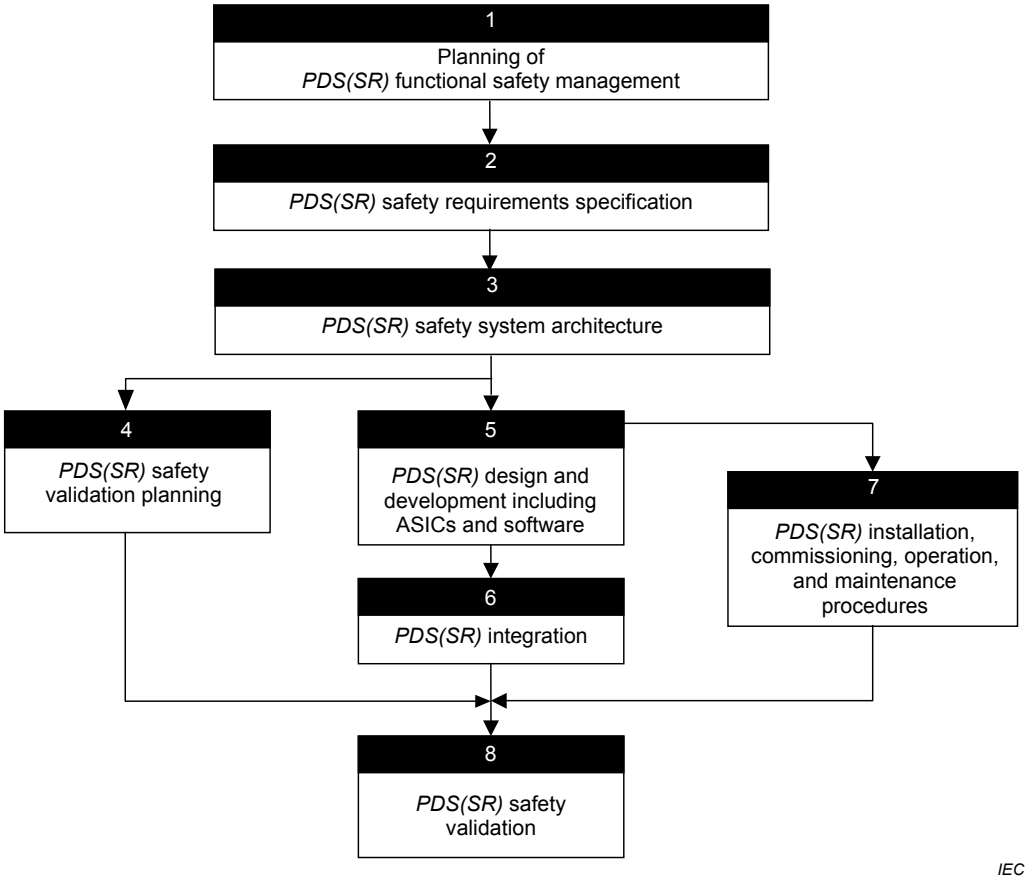
The requirements of Clause 6 of IEC 61508-1:2010 apply.

5.3 *PDS(SR)* development lifecycle

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

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

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



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

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

Figure 3 – *PDS(SR)* development lifecycle

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

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

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

~~– the integration and functional test techniques, regression testing, and responsible personnel;~~

– the design change management (both hardware and software).

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

– the personnel responsible for *verification*;

– the selection of *verification* strategies, techniques and tools;

– the selection and documentation of *verification* activities;

– the selection and utilization of test equipment;

– the evaluation of *verification* results gained from *verification* equipment and from tests.

e) A *validation* plan for the *safety sub-function*(s) comprising the following:

– the personnel responsible for *validation* testing;

– the identification of the relevant modes of operation of the *PDS(SR)*;

~~– the technical strategy for validation, for example analytical methods or statistical tests;~~

~~– the acceptance criteria;~~

– the procedures to be applied to validate that each *safety sub-function* of the *PDS(SR)* is correctly implemented, and the pass/fail criteria for accomplishing the tests;

– the procedures to be applied to validate that each *safety sub-function* of the *PDS(SR)* is of the required *safety integrity*, and the pass/fail criteria for accomplishing the tests;

– the required environment in which the testing is to take place including all necessary tools and equipment (also plan which tools and equipment should be calibrated);

– test evaluation procedures (with justifications);

– the test procedures and performance criteria to be applied to validate the specified electromagnetic immunity limits;

– the action to be taken in the event of failure to meet any of the acceptance criteria~~.~~

~~e) Planning for installation and commissioning comprising the following (where applicable):~~

~~– the special instructions for installation and sequence of installation;~~

~~– the personnel responsible for installation and commissioning;~~

~~– the commissioning activities and tests related to functional safety;~~

~~– the reporting methodology for commissioning tests and results;~~

~~– the mechanism for resolution of test failures and issues~~.

f) Planning for safety-related user documentation including:

– the personnel responsible for user documentation;

– a list of significant safety-related information which ~~must~~ shall be provided;

– the review process to insure the accuracy of documentation

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

– the scope of the functional safety assessment;

~~– the personnel responsible for the functional assessment;~~

– the organisations involved;

– the resources required ~~to complete the functional safety assessment activity~~;

– those to perform the *functional safety* assessment;

– the level of independence of ~~the assessment team~~ those performing the *functional safety* assessment;

– the competence of each person involved in the *functional safety* assessment;

– the outputs from the *functional safety* assessment;

AVA Documents
Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

– how the *functional safety* assessment relates to, and shall be integrated with, other *functional safety* assessments where appropriate;

– the requirement to perform an impact analysis to determine which parts of the assessment are to be repeated in case of a modification (see also IEC 61508-1:2010, 7.16.2)

~~– the stages at which the functional safety assessment activities are to be carried out (for example, after the safety requirements specification has been developed, after the safety-related control system has been designed);~~

~~– the information that shall be generated as a result of the functional safety assessment activity;~~

~~– the means by which the functional safety assessment shall be revalidated after modifications to the PDS(SR).~~

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

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

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

5.5.1 General

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

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

– a *safety integrity* requirements specification (see 5.5.3).

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

– clear, precise~~, uniquivocal~~, unambiguous, feasible, verifiable, testable and maintainable;

– written to aid the comprehension by those who are likely to utilise the information at any stage of the *PDS(SR)* safety lifecycle;

– expressed in natural or formal language and/or logic, sequence or cause and effect diagrams that define the necessary *safety sub-functions* with each *safety sub-function* being individually defined.

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

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

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

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

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

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

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

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.5.3 *Safety integrity* requirements specification

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

a) for each safety-related function (or group of simultaneously used safety-related functions), ~~both a~~ *SIL capability* (or *SIL*) and ~~a maximum probability~~ an upper limit of ~~dangerous random hardware failure~~ *PFH* value.

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

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

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

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

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

b) the required *mission time*;

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

NOTE 6 This information ~~may~~ can have been obtained in order to satisfy the requirements of IEC 61800-1, IEC 61800-2 or IEC 61800-4 and in this case need not be documented again.

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

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

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

5.6 *PDS(SR)* safety system architecture specification

5.6.1 General

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

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

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

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

– clear, precise, unambiguous, feasible, verifiable, testable and maintainable;

– written to aid the comprehension by those who are likely to utilise the information at any stage of the *PDS(SR)* safety lifecycle;

– traceable to the *PDS(SR) safety requirements specification*.

5.6.2 Requirements for safety system architecture specification

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

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

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

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

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

d) accuracy and stability requirements for measurements and controls;

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

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

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

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

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

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

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

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

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

6.1 General requirements

6.1.1 Change in operational status

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

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

6.1.2 Design standards

The *PDS(SR)* shall be designed in accordance with IEC 61800-5-1 and~~, as necessary,~~ other applicable parts of the IEC 61800 series, listed in the normative references.

6.1.3 Realisation

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

6.1.4 *Safety integrity* and fault detection

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

a) the requirements for hardware *safety integrity* comprising:
   - the architectural constraints on hardware *safety integrity* (see 6.2.3), and
   - the requirements for the ~~probability of dangerous random hardware failures per hour~~ *PFH* value (see 6.2.2 or 6.2.3);

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

– the requirements for the avoidance of failures (see 6.2.5.1), and the requirements for the control of systematic faults (see 6.2.5.2), or

– evidence that components used are 'proven-in-use'. In this case the components shall fulfil the relevant requirements of IEC 61508-2:2010

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

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

6.1.5 Safety and non-*safety sub-functions*

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

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

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

6.1.6 *SIL* ~~to be used~~ for multiple *safety sub-functions* within one *PDS(SR)*

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

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

As an example see Table 2:

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

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

6.1.7 Integrated circuits with on-chip redundancy

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

6.1.8 Software requirements

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

~~**6.1.8 Review of requirements**~~

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

~~a) safety functions;~~

~~b) safety integrity requirements;~~

~~c) equipment and operator interfaces.~~

6.1.9 Design documentation

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

6.2 *PDS(SR)* design requirements

6.2.1 Basic and well-tried safety principles

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

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

– For mechanical parts (e.g. encoders), these principles correspond to ISO 13849-2:2012, Table A.1 and Table A.2

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

6.2.2.1 General requirements

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

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

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

~~NOTE 1~~ The target failure measure, expressed in terms of the *PFH*, is determined by the *SIL* of the *safety sub-function* (see IEC 61508-1:~~1998~~ 2010, Table 3), unless there is a requirement in the *PDS(SR) safety integrity* requirements specification (see 5.5.3) for the *safety sub-function* to meet a specific target failure measure, rather than a specific *SIL*.

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

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

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

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

NOTE 2 A number of modelling methods are available and the most appropriate method is a matter for the analyst and will depend on the circumstances. Available methods include:

– fault tree analysis (see IEC 61025);

– Markov models (see IEC 61165);

– reliability block diagrams (see IEC 61078);

– parts count (see IEC 61709:2011);

– procedure description (see IEC 61508-6:2010);

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

See also IEC 60300-3-1.

NOTE 3 The mean time to restoration (see IEC 60050~~-191-13-08~~ 192-07-23) that is considered in the reliability model will need to take into account the diagnostic~~ and proof test~~ intervals, the repair time and any other delays prior to restoration, and the *mission time*.

NOTE 4 Failures due to common cause effects and data communication processes~~ may~~ can result from effects other than actual failures of hardware components (for example decoding errors). However, such failures are considered, for the purposes of this standard, as random hardware failures (see IEC 61508-6:2000, Annex D).

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

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

6.2.2.1.2 Estimation of *PFH*

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

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

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

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

d) the susceptibility of the *PDS(SR)* to *common cause failures* (see IEC 61508-6:~~2000~~ 2010, Annex D);

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

~~NOTE 1~~ and when establishing the diagnostic test interval, the intervals between all of the tests which contribute to the diagnostic coverage will need to be considered;

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

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

f) the repair times for detected failures;

NOTE 1 The repair time will constitute one part of the mean time to restoration (see~~ IEV 191-13-08~~ IEC 60050-192:2015, 192-07-23), which will also include the time taken to detect a failure and any time period during which repair is not possible (see Annex B of IEC 61508-6:~~2000~~ 2010 for an example of how the mean time to restoration can be used to calculate the probability of failure). For situations where the repair can only be carried out during a specific period of time, for example while the~~ EUC~~ equipment or machinery driven by the *PDS(SR)* is shut down and in a safe state, it is particularly important that full account is taken of the time period when no repair can be carried out, especially when this is relatively large.

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

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

6.2.2.1.3 Failure rate data

Component failure rate data shall be obtained from:

– a recognised source; or

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

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

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

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

NOTE 2 Although a constant failure rate is assumed by most probabilistic estimation methods, this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time), the results of most probabilistic calculation methods are therefore meaningless. Thus, any probabilistic estimation ~~should~~ can include a specification of the components' useful lifetimes. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolytic capacitors can be very sensitive). ~~Experience has shown that the useful lifetime often lies within a range of 8 years to 12 years. It can, however, be significantly less if components are operated near to their specification limits.~~

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

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

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

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

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

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

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

– one test per year for *SIL* 2, PL d / category 3;

– one test per three months for *SIL* 3, PL e / category 3;

– one test per day for *SIL* 3, PL e / category 4.

PL and category according to ISO 13849-1.

6.2.2.1.5 Diagnostic test interval when the hardware fault tolerance is zero

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

6.2.3 Architectural constraints

6.2.3.1 Limitations of *SIL*

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

subsystem carrying out a *safety sub-function* and hence every part of the *PDS(SR)*; 6.2.3.2.2 and 6.2.3.2.3 specify which one of Table 4 or Table 5 applies to any particular *subsystem*. With respect to these requirements,

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

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

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

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

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

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

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

6.2.3.2 Type A and Type B *subsystem*s

6.2.3.2.1 General

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

6.2.3.2.2 Type A

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

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

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

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

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

6.2.3.2.3 Type B

A *subsystem* shall be regarded as type B if, for the components required to achieve the *safety sub-function*, one or more of the criteria of 6.2.3.2.2 ~~is~~ are not satisfied.

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

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

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

6.2.3.3 Architectural constraints

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

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

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

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

[a] See 6.2.4 for details of how to estimate *safe failure* fraction.

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

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

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

[a] See 6.2.4 for details of how to estimate *safe failure* fraction.

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

Exception:

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

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

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

6.2.4 Estimation of *safe failure fraction (SFF)*

6.2.4.1 Methods of analysis

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

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

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

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

Basis of data is given in 6.2.2.1.3.

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

~~**6.2.3.2 Basis of data**~~

~~The estimation of SFF shall be based upon either:~~

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

~~– component failure data from a recognised source.~~

~~See also 6.2.1.1.3.~~

~~**6.2.3.3 Safety relays**~~

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

~~**6.2.3.4 Calculation of SFF**~~

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

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

6.2.5.1 Requirements for the avoidance of failures

6.2.5.1.1 General

Techniques and measures shall be used which minimize the introduction of faults during the design and development of the hardware of the *PDS(SR)* according to IEC 61508-2:2010, Table B.2.

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

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

6.2.5.1.2 Choice of design methods

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

a) transparency, modularity and other features which minimize complexity and enhance understandability of the design;

b) clear and precise specification of
   – functionality,
   – *subsystem* interfaces,
   – sequencing and time-related information,
   – concurrency and synchronisation;

c) clear and precise documentation and communication of information;

d) *verification* and *validation*.

6.2.5.1.3 Design measures

The following design measures shall be applied.

a) Proper design of the *PDS(SR)* and/or *subsystem*s including
   – the use of components within manufacturers specifications, for example temperature, loading, power supply, power rating, and timing parameters;
   – the derating of design parameters to improve reliability where necessary to achieve target failure rates;
   – the proper combination and assembly of *subsystem*s, for example cabling, wiring and any interconnections;
   – the use of reviews and inspections for early detection of design defects.

b) Compatibility:
   – use *subsystem*s with compatible operating characteristics.

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

6.2.5.1.4 Test planning

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

a) *subsystem* testing;

b) integration testing;

c) *validation* testing;

d) configuration testing (see 7.2).

Documentation of the test planning shall include:

e) types of tests to be performed and procedures to be followed;

f) test environment, tools, configuration and programs;

g) pass/fail criteria.

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

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

6.2.5.1.5 Design maintenance requirements

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

6.2.5.2 Requirements for the control of systematic faults

6.2.5.2.1 General

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

6.2.5.2.2 Design features

For controlling systematic faults, the design shall ~~possess~~ provide features that make the *PDS(SR)* and its *subsystem*s tolerant against:

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

b) environmental stresses~~, including electromagnetic disturbances, by applying Clause A.3 and Table A.17 of IEC 61508-2:2000~~ according IEC 61800-2:2015, Table 6 as applicable for the environment specified for the *PDS(SR)*;

c) electromagnetic disturbances, see 6.2.6;

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

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

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

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

6.2.5.2.3 Testability and maintainability

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

6.2.5.2.4 Human constraints

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

6.2.5.2.5 Protection against unintentional modification

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

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

6.2.5.2.6 Input acknowledgement and operator mistakes

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

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

AVA Documents Document Sharing Hub

Full document details: IEC 61800-5-2 2016 RLV

6.2.5.2.7 *PDS(SR)* parameterization

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

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

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

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

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

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

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

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

6.2.5.2.8 Loss of electrical supply

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

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

~~**6.2.5.1 General**~~

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

~~**6.2.5.2 Intended environment**~~

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

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

~~**6.2.5.3 Performance criterion**~~

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

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

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

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

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

~~6.2.5.4 Introduction of hazards~~

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

~~6.2.5.5 Verification~~

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

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

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

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

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

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

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

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

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

The thermal immunity test requirements are described in 9.4.

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

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

The mechanical immunity test requirements are described in 9.5.

6.3 Behaviour on detection of fault

6.3.1 Fault detection

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

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

6.3.2 Fault tolerance greater than zero

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

a) a *fault reaction function*, or

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

6.3.3 Fault tolerance zero

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

6.4 Additional requirements for data communications

When data communication is used in the implementation of a *safety sub-function* within a *PDS(SR)* then the probability of undetected failure of the communication process shall be estimated~~ taking into account transmission errors, repetitions, deletion, insertion, resequencing, corruption, delay and masquerade~~. This probability shall be taken into account when estimating the *PFH* of the *safety sub-function* due to random failures (see 6.2.1.1.2). This does not cover all data communication within a *PDS(SR)*. For example data communication within one printed wiring board is not covered by this requirement.

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

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

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

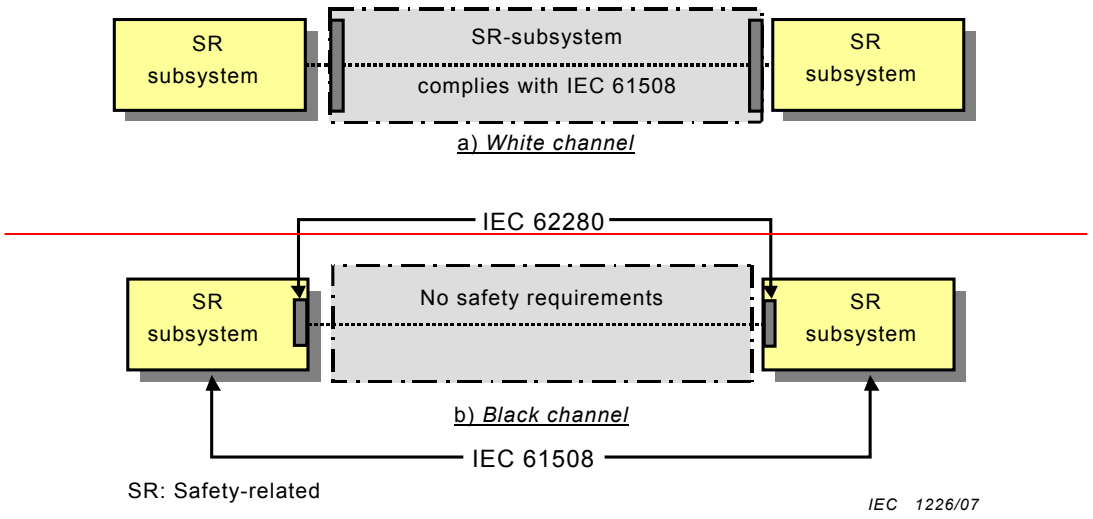
~~The measures necessary to ensure the required failure measure of the communication process shall be implemented according to the requirements of IEC 61508-2 and of IEC 61508-3. This allows two possible approaches:~~

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

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

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

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV



~~**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 *subsystem*s and components into the *PDS(SR)*, the *PDS(SR)* shall be tested according to the specified integration tests. These tests are specified on the *verification* plan and shall show that all modules interact correctly to perform their intended function and not perform unintended functions.

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

6.5.2 Software integration

The integration of safety-related software part/module into the *PDS(SR)* shall be carried out according to IEC 61508-3:2010. It shall include tests that are specified on the software *verification* plan to ensure the compatibility of the software with the hardware such that the functional and safety performance requirements are satisfied.

NOTE This does not imply testing of all input combinations. Testing all equivalence classes (see IEC 61508-7:~~2000~~ 2010, B.5.2) ~~may~~ can suffice. Static analysis (see IEC 61508-7:~~2000~~ 2010, B.6.4), dynamic analysis (see IEC 61508-7:~~2000~~ 2010, B.6.5) or failure analysis (see IEC 61508-7:~~2000~~ 2010, B.6.6) ~~may~~ can reduce the number of test cases to an acceptable level.

6.5.3 Modifications during integration

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

6.5.4 Applicable integration tests

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

AVA Documents Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV

6.5.5 Test documentation

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

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

7 Information for use

7.1 General

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

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

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

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

a) A functional specification of each *safety sub-function* and interface which is available for use in the implementation of *safety sub-function*s. This shall comprise:
   – a detailed description of the *safety sub-function* (including the reaction(s) to a violation of limits);
   – the *fault reaction function*;
   – the response time of each safety-related function and of the associated *fault reaction function*s;
   – the condition(s) (for example, operating mode) in which the *safety sub-function* is intended to be active or disabled;
   – the priority of those ~~functions~~ *safety sub-function* that are simultaneously active and can conflict with each other.
b) The *safety integrity* information for each *safety sub-function*, including:
   – the *SIL* or *SIL* capability; (includes systematic capability, see IEC61508-2);
   – the PFH value for each *safety sub-function*;
   – resulting PFH-value for a group of simultaneously activated *safety sub-function*s;
   – PL and category according to ISO 13849-1 when applicable.
c) A definition of the environmental and operating conditions (including electromagnetic) under which the *PDS(SR)* is intended to be used (see also IEC 61800-1, IEC 61800-2, IEC 61800-3, IEC 61800-4 and IEC 61800-5-1). This shall take into account storage, transport, ~~installation~~ act of installing, commissioning, testing, operation and maintenance.

   NOTE As an example for an EMC related information for use: "Warning: handheld radio transmitters held closer than 20 cm to *PDS(SR)* can disturb the *safety sub-function*s of the *PDS(SR)*" or similar (see E.2, footnote p)
d) An indication of any constraints on the *PDS(SR)* for:
   – the environment which should be observed in order to maintain the validity of the estimated failure rates;
   – the *mission time* of the *PDS(SR)* ~~and proof test interval(s), as appropriate~~;

Documents
Document Sharing Hub
Full document details: IEC 61800-5-2 2016 RLV