AS IEC 61800.5.2:2024
IEC 61800-5-2:2016

Australian STANDARD®

STANDARDS Australia

Adjustable speed electrical power drive systems

Part 5.2: Safety requirements — Functional

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

AS IEC 61800.5.2:2024

This Australian Standard® was prepared by EL-027, Power Electronics. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 12 June 2024.

This Standard was published on 28 June 2024.

The following are represented on Committee EL-027:

Australian Industry Group
Bureau of Steel Manufacturers of Australia
Department of Defence (Australian Government)
Energy Networks Australia
Engineers Australia
University of Newcastle

This Standard was issued in draft form for comment as DR AS IEC 61800.5.2:2024.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76139 698 4

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

AS IEC 61800.5.2:2024
IEC 61800-5-2:2016

Adjustable speed electrical power drive systems

Part 5.2: Safety requirements — Functional

Originated as AS IEC 61800.5.2—2013.
Second edition AS IEC 61800.5.2:2024.

© IEC Geneva Switzerland 2024 — All rights reserved
© Standards Australia Limited 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of either the IEC or the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth). If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please see the contact details on the back cover or the contact us page of the website for further information.

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

Preface

This Standard was prepared by the Standards Australia Committee EL-027, Power Electronics, to supersede AS 61800.5.2:2013.

The objective of this document is to specify requirements and make 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 AS IEC 61800.2:2024. This document, which is a product standard, sets out safety-related considerations of PDS(SR)s in terms of the framework of IEC 61508, and introduces requirements for PDS(SR)s as subsystems of a safety-related system. It is intended to facilitate the realization of the electrical/ electronic/programmable electronic (E/E/PE) parts of a PDS(SR) in relation to the safety performance of safety sub-function(s) of a PDS.

This document is identical with, and has been reproduced from, IEC 61800-5-2:2016, *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional.*

As this document has been reproduced from an international document, the following apply:

(a) In the source text “this part of IEC 61800” should read “this document”.

(b) A full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

AVA Documents
Document Sharing Hub

© Standards Australia Limited 2024

Full document details: AS IEC 61800.5.2-2024

Contents

Preface ii
FOREWORD vi
INTRODUCTION ix
1 Scope 1
2 Normative references 2
3 Terms and definitions 4
4 Designated safety sub-functions 10
4.1 General 10
4.2 Safety sub-functions 11
4.2.1 General 11
4.2.2 Limit values 11
4.2.3 Stopping functions 12
4.2.4 Monitoring functions 13
4.2.5 Output functions – Safe brake control (SBC) 15
5 Management of functional safety 15
5.1 Objective 15
5.2 Requirements for the management of functional safety 15
5.3 PDS(SR) development lifecycle 15
5.4 Planning of PDS(SR) functional safety management 16
5.5 Safety requirements specification (SRS) for a PDS(SR) 18
5.5.1 General 18
5.5.2 Safety sub-functions requirements specification 19
5.5.3 Safety integrity requirements specification 20
5.6 PDS(SR) safety system architecture specification 20
5.6.1 General 20
5.6.2 Requirements for safety system architecture specification 21
6 Requirements for design and development of a PDS(SR) 22
6.1 General requirements 22
6.1.1 Change in operational status 22
6.1.2 Design standards 22
6.1.3 Realisation 22
6.1.4 Safety integrity and fault detection 22
6.1.5 Safety and non-safety sub-functions 23
6.1.6 SIL for multiple safety sub-functions within one PDS(SR) 23
6.1.7 Integrated circuits with on-chip redundancy 23
6.1.8 Software requirements 24
6.1.9 Design documentation 24
6.2 PDS(SR) design requirements 24
6.2.1 Basic and well-tried safety principles 24
6.2.2 Requirements for the estimation of the probability of dangerous random hardware failures per hour (PFH) 24
6.2.3 Architectural constraints 27
6.2.4 Estimation of safe failure fraction (SFF) 29
6.2.5 Requirements for systematic safety integrity of a PDS(SR) and PDS(SR) subsystems 29
6.2.6 Design requirements for electromagnetic (EM) immunity of a PDS(SR) 32
6.2.7 Design requirements for thermal immunity of a PDS(SR) 32
6.2.8 Design requirements for mechanical immunity of a PDS(SR) 32
6.3 Behaviour on detection of fault 32
6.3.1 Fault detection 32
6.3.2 Fault tolerance greater than zero 33
6.3.3 Fault tolerance zero 33

AVA Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024

6.4 Additional requirements for data communications 33
6.5 PDS(SR) integration and testing requirements 33
6.5.1 Hardware integration 33
6.5.2 Software integration 33
6.5.3 Modifications during integration 33
6.5.4 Applicable integration tests 33
6.5.5 Test documentation 34

7 Information for use 34
7.1 General 34
7.2 Information and instructions for safe application of a PDS(SR) 34

8 Verification and validation 36
8.1 General 36
8.2 Verification 36
8.3 Validation 36
8.4 Documentation 37

9 Test requirements 37
9.1 Planning of tests 37
9.2 Functional testing 37
9.3 Electromagnetic (EM) immunity testing 37
9.3.1 General 37
9.3.2 Intended EM environment 38
9.3.3 Performance criterion (fail safe state – FS) 38
9.4 Thermal immunity testing 38
9.4.1 General 38
9.4.2 Functional thermal test 38
9.4.3 Component thermal test 38
9.5 Mechanical immunity testing 39
9.5.1 General 39
9.5.2 Vibration test 39
9.5.3 Shock test 39
9.5.4 Performance criterion for mechanical immunity tests (fail safe state – FS) 39
9.6 Test documentation 39

10 Modification 39
10.1 Objective 39
10.2 Requirements 40
10.2.1 General 40
10.2.2 Modification request 40
10.2.3 Impact analysis 40
10.2.4 Authorization 40
10.2.5 Documentation 40

Annex A (informative) **Sequential task table 41**

Annex B (informative) **Example for estimation of PFH 46**

Annex C (informative) **Available failure rate databases 59**

Annex D (informative) **Fault lists and fault exclusions 61**

Annex E (normative) **Electromagnetic (EM) immunity requirement for PDS(SR) 71**

Annex F (informative) **Estimation of PFD_{avg} value for low demand with given PFH value 76**

Bibliography 77

List of Figures

Figure 1 — Installation and functional parts of a PDS(SR) 2
Figure 2 — Safety function consisting of safety sub-functions 11

AVA Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024

Figure 3 — PDS(SR) development lifecycle 16
Figure B.1 — Example PDS(SR) 46
Figure B.2 — Subsystems of the PDS(SR) 47
Figure B.3 — Function blocks of subsystem A/B 49
Figure B.4 — Reliability model (Markov) of subsystem A/B 52
Figure B.5 — Function blocks of subsystem PS/VM 54
Figure B.6 — Reliability model (Markov) of subsystem PS/VM 56

List of Tables

Table 1 — Alphabetical list of terms and definitions 4
Table 2 — Example for determining the SIL from hardware and software independence 23
Table 3 — Safety integrity levels: target failure measures for a PDS(SR)safety sub-function 24
Table 4 — Maximum allowable safety integrity level for a safety sub-function carried out by a type A safety-related subsystem 28
Table 5 — Maximum allowable safety integrity level for a safety sub-function carried out by a type B safety-related subsystem 28
Table A.1 — Design and development procedure for PDS(SR) 41
Table B.1 — Determination of DC factor of subsystem A/B 50
Table B.2 — PFH value calculation results for subsystem A/B 53
Table B.3 — Determination of DC factor of subsystem A/B 54
Table B.4 — PFH value calculation results for subsystem PS/VM 57
Table D.1 — Printed wiring boards/assemblies 62
Table D.2 — Terminal block 63
Table D.3 — Multi-pin connector 63
Table D.4 — Electromechanical devices (for example relay, contactor relays) 64
Table D.5 — Signal Isolation components 65
Table D.6 — Non-programmable integrated circuits 66
Table D.7 — Programmable and/or complex integrated circuits 66
Table D.8 — Motion and position feedback sensors 67
Table E.1 — Minimum immunity requirements for voltage deviations, dips and short interruptions 71
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 72
Table E.3 — Immunity requirements – high frequency disturbances 73
Table E.4 — General frequency ranges for mobile transmitters and ISM for radiated tests 74
Table E.5 — General frequency ranges for mobile transmitters and ISM for conducted tests 75

Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

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

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

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

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

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

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

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

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

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

b) definition added for: "*category*" and "*safety function*"

© Standards Australia Limited 2024

AVA Documents Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

c) "Other sub-functions" sorted into "Monitoring sub-functions" and "Output functions"

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

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

f) Updated references to IEC 61508 series Ed.2010

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

h) 6.1.6 Text replaced by Table 2

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

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

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

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

m) 6.1.7 Integrated circuits with on-chip redundancy

n) 6.2.1 Basic and well-tried safety principles

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

p) 6.2.5.2.7 *PDS(SR)* parameterization

q) 9 Test requirements

r) 9.3 Electromagnetic (EM) immunity testing

s) 9.4 Thermal immunity testing

t) 9.5 Mechanical immunity testing

u) Annex A Sequential task table

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

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

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

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

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

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

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

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

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

- reconfirmed,

Documents Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

- 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.**

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

INTRODUCTION

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

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

Examples of industrial applications are:

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

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

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

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

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

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

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

NOTES

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

Australian Standard®

Adjustable speed electrical power drive systems

Part 5.2: Safety requirements — Functional

1 Scope

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

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

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

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

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

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

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

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

This part of IEC 61800 does not specify requirements for:

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

Documents
Document Sharing Hub
© Standards Australia Limited 2024

Full document details: AS IEC 61800.5.2-2024

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

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

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

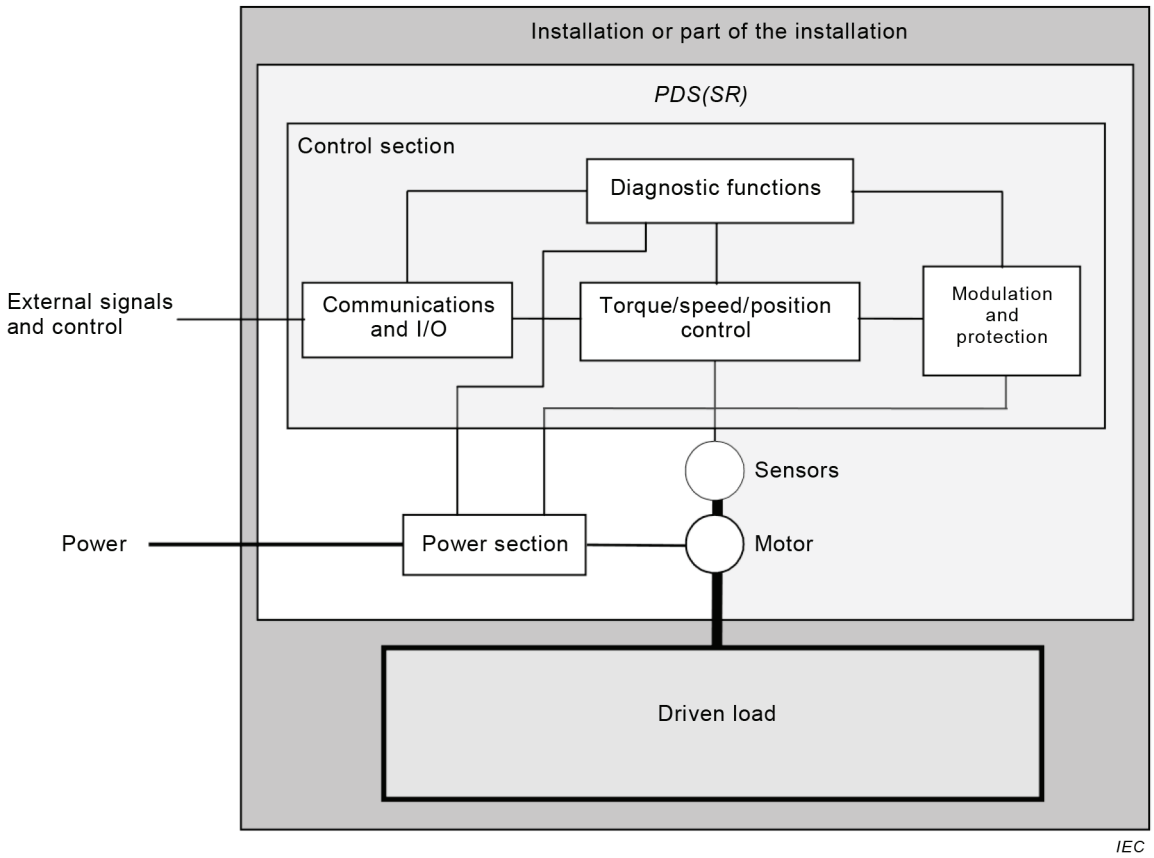


Figure 1 — Installation and functional parts of a *PDS(SR)*

2 Normative references

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

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

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

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

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

IEC 61000-4-3:2006/AMD1:2007

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

IEC 61000-4-3:2006/AMD2:2010

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEC 61800-3:2004/AMD1:2011

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

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

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

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

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

3 Terms and definitions

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

Table 1 — Alphabetical list of terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

© Standards Australia Limited 2024

Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

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

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

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

3.12
hazard
potential source of harm

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

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

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

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

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

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

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

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

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

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

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

3.16
PDS(SR)
adjustable speed electrical power drive system providing *safety sub-function*s

© Standards Australia Limited 2024

Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024

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

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

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

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

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

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

3.19
safe failure
failure of a component and/or *subsystem* and/or system that plays a part in implementing the *safety sub-function* that:

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

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

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

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

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

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

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

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

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

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

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

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

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

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

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

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

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

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

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

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

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

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

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

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

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

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

3.26
safety-related system
designated system that both

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

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

© Standards Australia Limited 2024

Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024

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

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

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

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

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

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

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

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

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

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

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

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

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

3.31
systematic safety integrity
part of the *safety integrity* of *safety-related system*s relating to *systematic 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 61508-4:2010; 3.5.6]

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

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

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

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

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

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

4 Designated *safety sub-functions*

4.1 General

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

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

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

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

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

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

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

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

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

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

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

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

© Standards Australia Limited 2024

Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024

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

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

4.2 *Safety sub-functions*

4.2.1 General

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

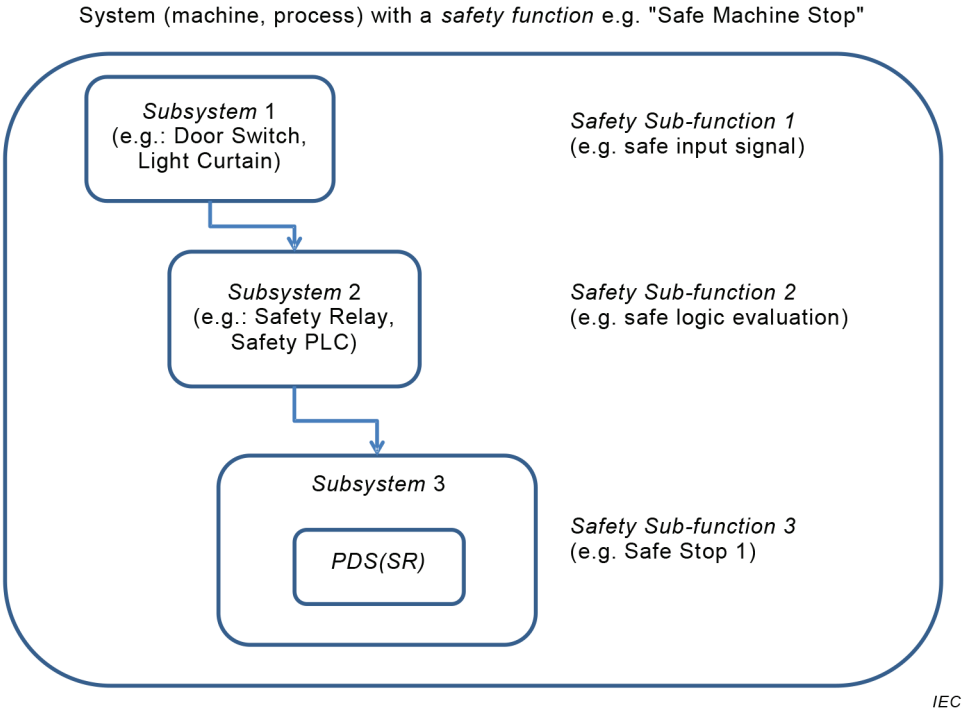


Figure 2 — *Safety function* consisting of *safety sub-functions*

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

4.2.2 Limit values

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

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

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

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

4.2.3 Stopping functions

4.2.3.1 General

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

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

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

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

4.2.3.2 Safe torque off (STO)

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

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

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

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

NOTE 3 Electronic means and some contactors are not adequate for protection against electric shock.

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

4.2.3.3 Safe stop 1 (SS1)

This function is specified as either

a) Safe Stop 1 deceleration controlled

SS1-d

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

b) Safe Stop 1 ramp monitored

SS1-r

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

c) Safe Stop 1 time controlled

SS1-t

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

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

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

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

4.2.3.4 Safe stop 2 (SS2)

This function is specified as either

a) Safe Stop 2 deceleration controlled

SS2-d

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

b) Safe Stop 2 ramp monitored

SS2-r

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

c) Safe Stop 2 time controlled

SS2-t

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

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

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

4.2.4 Monitoring functions

4.2.4.1 General

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

4.2.4.2 Safe operating stop (SOS)

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

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

4.2.4.3 Safely-limited acceleration (SLA)

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

4.2.4.4 Safe acceleration range (SAR)

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

Documents Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024

4.2.4.5 Safely-limited speed (SLS)

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

4.2.4.6 Safe speed range (SSR)

This function keeps the motor speed within specified limits.

4.2.4.7 Safely-limited torque (SLT)

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

4.2.4.8 Safe torque range (STR)

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

4.2.4.9 Safely-limited position (SLP)

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

4.2.4.10 Safely-limited increment (SLI)

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

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

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

4.2.4.11 Safe direction (SDI)

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

4.2.4.12 Safe motor temperature (SMT)

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

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

4.2.4.13 Safe cam (SCA)

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

4.2.4.14 Safe speed monitor (SSM)

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

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 61800.5.2-2024

4.2.5 Output functions – Safe brake control (SBC)

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

5 Management of *functional safety*

5.1 Objective

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

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

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

5.2 Requirements for the management of *functional safety*

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

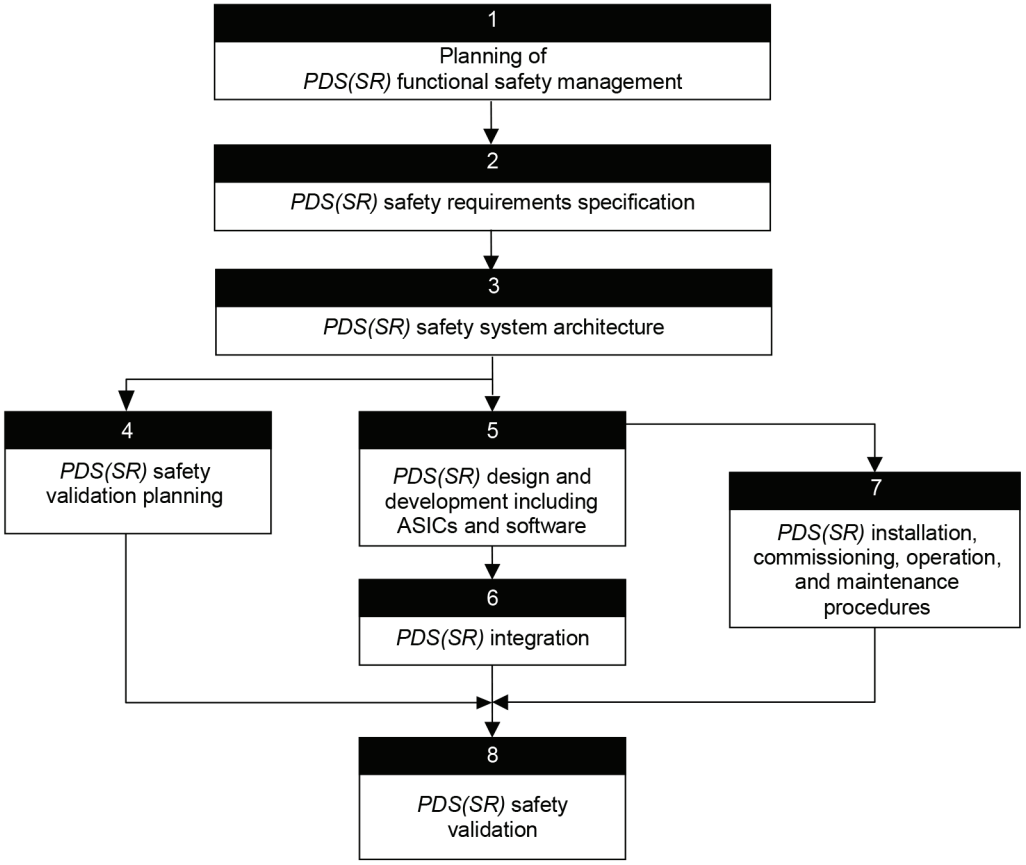
5.3 *PDS(SR)* development lifecycle

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

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

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

Documents Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 61800.5.2-2024



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

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

Figure 3 — *PDS(SR)* development lifecycle

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

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

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

a) Generation of the *safety requirements specification* (see 5.5), including factors such as:

- the personnel responsible for generation and maintenance of the *safety requirements specification*;
- the choice of methods for the avoidance of mistakes during generation of the *safety requirements specification* (see IEC 61508-2:2010, Annex B);
- the consideration of requirements from guidelines and standards for specific target applications of the *PDS(SR)*;

© Standards Australia Limited 2024

Documents
Document Sharing Hub
Full document details: AS IEC 61800.5.2-2024