

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Entraînements électriques de puissance à vitesse variable –
Partie 5-2: Exigences de sécurité – Fonctionnelle**



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.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.



IEC 61800-5-2

Edition 2.0 2016-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Entraînements électriques de puissance à vitesse variable –
Partie 5-2: Exigences de sécurité – Fonctionnelle**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.110; 29.200

ISBN 978-2-8322-3302-3

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references.....	10
3 Terms and definitions	12
4 Designated <i>safety sub-functions</i>	18
4.1 General.....	18
4.2 <i>Safety sub-functions</i>	19
4.2.1 General	19
4.2.2 Limit values	20
4.2.3 Stopping functions	20
4.2.4 Monitoring functions.....	21
4.2.5 Output functions – Safe brake control (SBC).....	23
5 Management of <i>functional safety</i>	23
5.1 Objective	23
5.2 Requirements for the management of <i>functional safety</i>	23
5.3 <i>PDS(SR)</i> development lifecycle	23
5.4 Planning of <i>PDS(SR) functional safety</i> management	24
5.5 Safety requirements specification (<i>SRS</i>) for a <i>PDS(SR)</i>	26
5.5.1 General	26
5.5.2 <i>Safety sub-functions</i> requirements specification.....	26
5.5.3 <i>Safety integrity</i> requirements specification.....	27
5.6 <i>PDS(SR)</i> safety system architecture specification	28
5.6.1 General	28
5.6.2 Requirements for safety system architecture specification.....	28
6 Requirements for design and development of a <i>PDS(SR)</i>	29
6.1 General requirements.....	29
6.1.1 Change in operational status	29
6.1.2 Design standards	29
6.1.3 Realisation.....	29
6.1.4 <i>Safety integrity</i> and fault detection.....	29
6.1.5 Safety and non- <i>safety sub-functions</i>	30
6.1.6 <i>SIL</i> for multiple <i>safety sub-functions</i> within one <i>PDS(SR)</i>	30
6.1.7 Integrated circuits with on-chip redundancy	31
6.1.8 Software requirements	31
6.1.9 Design documentation.....	31
6.2 <i>PDS(SR)</i> design requirements	31
6.2.1 Basic and well-tried safety principles	31
6.2.2 Requirements for the estimation of the probability of dangerous random hardware failures per hour (<i>PFH</i>).....	31
6.2.3 Architectural constraints	34
6.2.4 Estimation of <i>safe failure fraction (SFF)</i>	35
6.2.5 Requirements for <i>systematic safety integrity</i> of a <i>PDS(SR)</i> and <i>PDS(SR) subsystems</i>	36
6.2.6 Design requirements for electromagnetic (EM) immunity of a <i>PDS(SR)</i>	39
6.2.7 Design requirements for thermal immunity of a <i>PDS(SR)</i>	39

6.2.8	Design requirements for mechanical immunity of a <i>PDS(SR)</i>	39
6.3	Behaviour on detection of fault	39
6.3.1	Fault detection	39
6.3.2	Fault tolerance greater than zero.....	39
6.3.3	Fault tolerance zero	39
6.4	Additional requirements for data communications.....	39
6.5	<i>PDS(SR)</i> integration and testing requirements	40
6.5.1	Hardware integration.....	40
6.5.2	Software integration	40
6.5.3	Modifications during integration	40
6.5.4	Applicable integration tests	40
6.5.5	Test documentation.....	40
7	Information for use	41
7.1	General.....	41
7.2	Information and instructions for safe application of a <i>PDS(SR)</i>	41
8	<i>Verification and validation</i>	42
8.1	General.....	42
8.2	<i>Verification</i>	43
8.3	<i>Validation</i>	43
8.4	Documentation.....	43
9	Test requirements.....	43
9.1	Planning of tests	43
9.2	Functional testing.....	43
9.3	Electromagnetic (EM) immunity testing	44
9.3.1	General	44
9.3.2	Intended EM environment.....	44
9.3.3	Performance criterion (fail safe state – FS).....	44
9.4	Thermal immunity testing	44
9.4.1	General	44
9.4.2	Functional thermal test.....	45
9.4.3	Component thermal test	45
9.5	Mechanical immunity testing.....	45
9.5.1	General	45
9.5.2	Vibration test	45
9.5.3	Shock test.....	45
9.5.4	Performance criterion for mechanical immunity tests (fail safe state – FS).....	45
9.6	Test documentation.....	45
10	Modification.....	46
10.1	Objective	46
10.2	Requirements.....	46
10.2.1	General	46
10.2.2	Modification request.....	46
10.2.3	Impact analysis	46
10.2.4	Authorization.....	46
10.2.5	Documentation.....	46
Annex A (informative)	Sequential task table.....	47
Annex B (informative)	Example for estimation of <i>PFH</i>	51

B.1	General.....	51
B.2	Example <i>PDS(SR)</i> structure	51
B.2.1	General	51
B.2.2	<i>Subsystem A/B</i>	52
B.2.3	<i>Subsystem PS/VM</i>	52
B.3	Example <i>PDS(SR)</i> PFH value determination	53
B.3.1	<i>Subsystem “A/B” (main subsystem)</i>	53
B.3.2	<i>Subsystem “PS/VM”</i>	58
B.3.3	PFH value of the <i>safety sub-function STO</i> of <i>PDS(SR)</i>	61
B.4	Reduction of DC and SFF depending on test interval	62
Annex C (informative)	Available failure rate databases	63
C.1	Databases	63
C.2	Helpful standards concerning component failure	63
Annex D (informative)	Fault lists and fault exclusions	65
D.1	General.....	65
D.2	Remarks applicable to fault exclusions	65
D.2.1	Validity of exclusions.....	65
D.2.2	Tin whisker growth	65
D.2.3	Short-circuits on PWB-mounted parts	65
D.3	Fault models	66
D.3.1	Conductors/cables	66
D.3.2	Printed wiring boards/assemblies	66
D.3.3	Terminal block	66
D.3.4	Multi-pin connector.....	67
D.3.5	Electromechanical devices	67
D.3.6	Transformers	68
D.3.7	Inductances	68
D.3.8	Resistors	68
D.3.9	Resistor Networks.....	68
D.3.10	Potentiometers.....	68
D.3.11	Capacitors	68
D.3.12	Discrete semiconductors	68
D.3.13	Signal Isolation components.....	69
D.3.14	Non-programmable integrated circuits	69
D.3.15	Programmable and/or complex integrated circuits	69
D.3.16	Motion and position feedback sensors	70
Annex E (normative)	Electromagnetic (EM) immunity requirement for <i>PDS(SR)</i>	74
E.1	General.....	74
E.2	Immunity requirements – low frequency disturbances.....	74
E.3	Immunity requirements – high frequency disturbances	77
Annex F (informative)	Estimation of PFD_{avg} value for low demand with given PFH value	81
F.1	General.....	81
F.2	Estimation of PFD_{avg} value for low demand with given PFH value	81
Bibliography	82
Figure 1	– Installation and functional parts of a <i>PDS(SR)</i>	10
Figure 2	– <i>Safety function</i> consisting of <i>safety sub-functions</i>	19

Figure 3 – <i>PDS(SR)</i> development lifecycle	24
Figure B.1 – Example <i>PDS(SR)</i>	51
Figure B.2 – <i>Subsystems</i> of the <i>PDS(SR)</i>	52
Figure B.3 – Function blocks of <i>subsystem A/B</i>	53
Figure B.4 – Reliability model (Markov) of <i>subsystem A/B</i>	56
Figure B.5 – Function blocks of <i>subsystem PS/VM</i>	58
Figure B.6 – Reliability model (Markov) of <i>subsystem PS/VM</i>	60
Table 1 – Alphabetical list of terms and definitions	12
Table 2 – Example for determining the <i>SIL</i> from hardware and software independence	30
Table 3 – <i>Safety integrity levels</i> : target failure measures for a <i>PDS(SR)</i> <i>safety sub-function</i>	32
Table 4 – Maximum allowable safety integrity level for a <i>safety sub-function</i> carried out by a type A safety-related <i>subsystem</i>	35
Table 5 – Maximum allowable safety integrity level for a <i>safety sub-function</i> carried out by a type B safety-related <i>subsystem</i>	35
Table A.1 – Design and development procedure for <i>PDS(SR)</i>	47
Table B.1 – Determination of DC factor of <i>subsystem A/B</i>	55
Table B.2 – <i>PFH</i> value calculation results for <i>subsystem A/B</i>	58
Table B.3 – Determination of DC factor of <i>subsystem A/B</i>	59
Table B.4 – <i>PFH</i> value calculation results for <i>subsystem PS/VM</i>	61
Table D.1 – Printed wiring boards/assemblies	66
Table D.2 – Terminal block	67
Table D.3 – Multi-pin connector.....	67
Table D.4 – Electromechanical devices (for example relay, contactor relays)	68
Table D.5 – Signal Isolation components.....	69
Table D.6 – Non-programmable integrated circuits	69
Table D.7 – Programmable and/or complex integrated circuits	70
Table D.8 – Motion and position feedback sensors	71
Table E.1 – Minimum immunity requirements for voltage deviations, dips and short interruptions	75
Table E.2 – <i>PDS(SR)</i> minimum immunity requirements for voltage deviations, dips and short interruptions on main power ports with a rated voltage above 1 000 V	76
Table E.3 – Immunity requirements – high frequency disturbances.....	77
Table E.4 – General frequency ranges for mobile transmitters and ISM for radiated tests.....	79
Table E.5 – General frequency ranges for mobile transmitters and ISM for conducted tests.....	80

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ADJUSTABLE SPEED ELECTRICAL
POWER DRIVE SYSTEMS –****Part 5-2: Safety requirements – Functional**

FOREWORD

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

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

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

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

- a) rational added in the scope why low demand mode is not covered by this standard
- b) definition added for: “*category*” and “*safety function*”
- c) “Other sub-functions” sorted into “Monitoring sub-functions” and “Output functions”
- d) deleted “proof test” throughout the document because for *PDS(SR)* a proof test is not applicable

- e) replaced the term “safety function” by “*safety sub-function*” throughout the document
- f) Updated references to IEC 61508 series Ed.2010
- g) Added the principle rules of ISO 13849-1 and reference to tables of ISO 13849-2
- h) 6.1.6 Text replaced by Table 2
- i) 6.1.7 Integrated circuits with on-chip redundancy matched to changed requirement in IEC 61508-2: 2010, Annex E
- j) 6.2.8 Design requirements for thermal immunity of a *PDS(SR)*
- k) 6.2.9 Design requirements for mechanical immunity of a *PDS(SR)*
- l) 6.1.6 *SIL* for multiple *safety sub-functions* within one *PDS(SR)*
- m) 6.1.7 Integrated circuits with on-chip redundancy
- n) 6.2.1 Basic and well-tried safety principles
- o) 6.2.2.1.4 *Diagnostic test* interval when the hardware fault tolerance is greater than zero
- p) 6.2.5.2.7 *PDS(SR)* parameterization
- q) 9 Test requirements
- r) 9.3 Electromagnetic (EM) immunity testing
- s) 9.4 Thermal immunity testing
- t) 9.5 Mechanical immunity testing
- u) Annex A Sequential task table
- v) Annex D, D.3.16, Motion and position feedback sensors updated
- w) Annex E Electromagnetic immunity (EM) requirement for *PDS(SR)*
- x) Annex F Estimation of PFD_{avg} value for low demand with given PFH value

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

Examples of industrial applications are:

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

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

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

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

There are many situations where control systems that incorporate a *PDS(SR)* are employed, for example as part of safety measures that have been provided to achieve risk reduction. A typical case is guard interlocking in order to exclude personnel from *hazards* 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-functions* and to enable the appropriate design of the *PDS(SR)* and verification that it meets the required performance.

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

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-2: Safety requirements – Functional

1 Scope

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-functions* 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 *subsystems* of a safety-related system. It is intended to facilitate the realisation of the electrical/ electronic/ programmable electronic (E/E/PE) parts of a *PDS(SR)* in relation to the safety performance of *safety sub-function(s)* of a PDS.

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

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

This part of IEC 61800 does not specify requirements for:

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