INTERNATIONAL STANDARD

IEC 61800-5-2

First edition
2007-07

Adjustable speed electrical power drive systems –

Part 5-2: Safety requirements – Functional

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

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

About the IEC

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

About IEC publications

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

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

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 It also gives information on projects, withdrawn and replaced publications.

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

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

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

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

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

INTERNATIONAL STANDARD

IEC 61800-5-2

First edition
2007-07

Adjustable speed electrical power drive systems –

Part 5-2: Safety requirements – Functional

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XB

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-2: Safety requirements – Functional

FOREWORD

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

Examples of industrial applications are:

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

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

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

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

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

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

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

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-2: Safety requirements – Functional

1 Scope and object

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

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

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

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

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

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

This part of IEC 61800 does not specify requirements for:

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

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

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

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

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

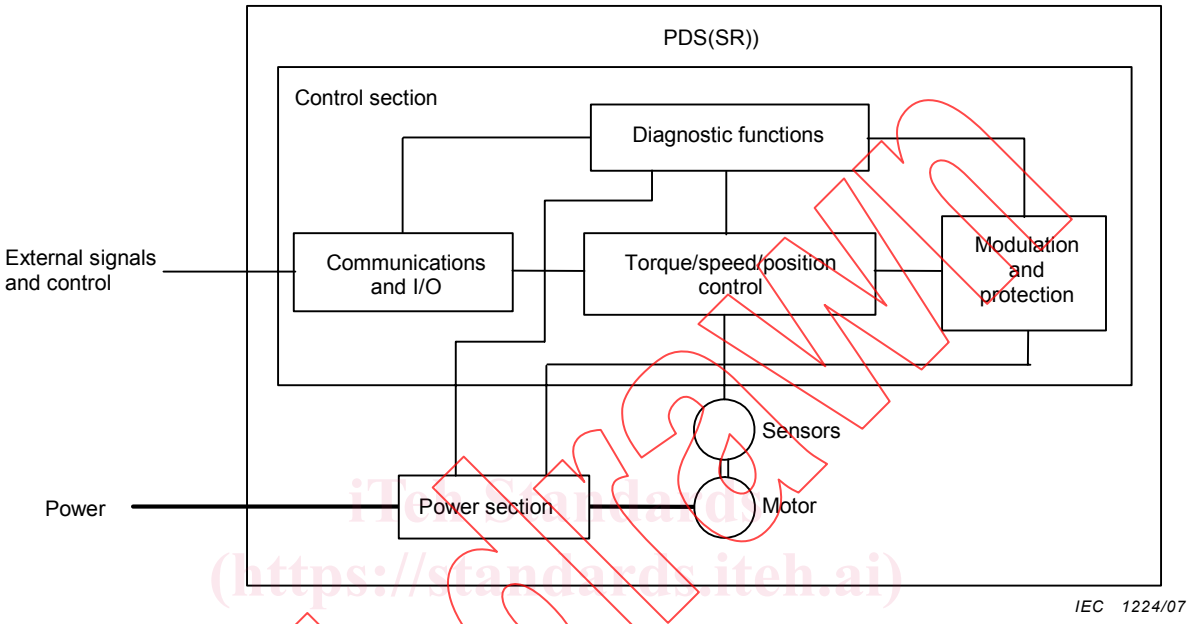

Figure 1 – Functional elements of a PDS(SR)

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

Table 1 – Alphabetical list of definitions

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

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

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

[IEC 61508-4:1998; definition 3.6.10]

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

[IEC 61508-4:1998; definition 3.6.7]

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

[IEC 61508-4:1998; definition 3.8.6]

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

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

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

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

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

[IEC 61508-4:1998; definition 3.1.9]

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

3.7
hazard
potential source of harm

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

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

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

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

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

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

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

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

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

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

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

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

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

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