

Australian Standard[®]

**Adjustable speed electrical power drive
systems**

**Part 5.2: Safety requirements—
Functional**

STANDARDS
Australia



This Australian Standard® was prepared by Committee EL-027, Power Electronics. It was approved on behalf of the Council of Standards Australia on 4 February 2013. This Standard was published on 27 February 2013.

The following are represented on Committee EL-027:

- Australian Communications and Media Authority
 - Australian Industry Group
 - Bureau of Steel Manufacturers of Australia
 - Engineers Australia
 - RMIT University
-

This Standard was issued in draft form for comment as Draft IEC 61800.5.2.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard[®]

**Adjustable speed electrical power drive
systems**

**Part 5.2: Safety requirements—
Functional**

First published as AS IEC 61800.5.2—2013.

COPYRIGHT

© Standards Australia Limited

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 the publisher, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 74342 363 9

PREFACE

This Standard was prepared by the Standards Australia Committee EL-027, Power Electronics.

The objective of this Standard is to specify requirements and make recommendations for the design and development, integration and validation of power drive systems that are suitable for use in safety-related applications {PDS(SR)} in terms of their functional safety considerations.

This Standard is identical with, and has been reproduced from IEC 61800-5-2, Ed.1.0 (2007), *Adjustable speed electrical power drive systems—Safety requirements—Functional*.

As this Standard is reproduced from an International Standard, the following applies:

- (a) Its number appears on the cover and title page while the International Standard number appears only on the cover.
- (b) In the source text ‘this part of IEC 61800’ should read ‘this part of AS 61800’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by reference to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>		<i>Australian Standard</i>	
IEC		AS	
60204	Safety of machinery—Electrical equipment of machines	60204	Safety of machinery—Electrical equipment of machines
60204-1	Part 1: General requirements	60204.1	Part 1: General requirements (IEC 60204-1, Ed. 5 (FDIS) MOD)
61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
61508-5	Part 5: Examples of methods for the determination of safety integrity levels	61508.5	Part 5: Examples of methods for the determination of safety integrity levels
61800	Adjustable speed electrical power drive systems	61800	Adjustable speed electrical power drive systems
61800-1	Part 1: General requirements—Rating specifications for low voltage adjustable speed d.c. power drive system	61800.1	Part 1: General requirements—Rating specifications for low voltage adjustable speed d.c. power drive systems
61800-2	Part 2: General requirements—Rating specifications for low voltage adjustable frequency a.c. power drive systems	61800.2	Part 2: General requirements—Rating specifications for low voltage adjustable frequency a.c. power drive systems
61800-3	Part 3: EMC requirements and specific test methods	61800.3	Part 3: EMC requirements and specific test methods
61800-4	Part 4: General requirements—Rating specifications for a.c. power drive systems above 1000 V a.c. and not exceeding 35 kV	61800.4	Part 4: General requirements—Rating specifications for a.c. power drive systems above 1000 V a.c. and not exceeding 35 kV
61800-5-1	Part 5-1: Safety requirements—Electrical, thermal and energy	61800.5.1	Part 5.1: Safety requirements—Electrical, thermal and energy

Only international references that have been adopted as Australian or Australian/New Zealand Standards have been listed.

The term ‘informative’ has been used in this Standard to define the application of the annex to which it applies. An ‘informative’ annex is only for information and guidance.

Currently in preview, click buy full version

CONTENTS

1	Scope and object.....	8
2	Normative references	9
3	Terms and definitions	10
4	Designated safety functions.....	15
4.1	General.....	15
4.2	Safety functions	16
4.2.1	Limit values	16
4.2.2	Stopping functions.....	16
4.2.3	Other safety functions.....	17
5	Management of functional safety	18
5.1	Objective.....	18
5.2	PDS(SR) development lifecycle	18
5.3	Functional safety planning.....	19
5.4	Safety requirements specification (SRS) for a PDS(SR)	21
5.4.1	General	21
5.4.2	Safety functionality requirements specification	21
5.4.3	Safety integrity requirements specification.....	22
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	23
6.1.4	Safety integrity and fault detection.....	23
6.1.5	Safety and non-safety functions.....	23
6.1.6	SIL to be used	23
6.1.7	Software requirements	23
6.1.8	Review of requirements.....	23
6.1.9	Design documentation	24
6.2	PDS(SR) design requirements.....	24
6.2.1	Requirements for probability of dangerous random hardware failures per hour (PDRFH)	24
6.2.2	Architectural constraints	26
6.2.3	Estimation of safe failure fraction (SFF).....	28
6.2.4	Requirements for systematic safety integrity of a PDS(SR) and PDS(SR) subsystems	28
6.2.5	Electromagnetic (EM) immunity requirement of a PDS(SR).....	31
6.3	Behaviour on detection of fault.....	31
6.3.1	Fault detection.....	31
6.3.2	Fault tolerance greater than zero.....	32
6.3.3	Fault tolerance zero.....	32
6.4	Additional requirements for data communications.....	32
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	Information and instructions for safe application of a PDS(SR).....	34
8	Verification and validation	35
8.1	General.....	35
8.2	Verification	36
8.3	Validation	36
8.4	Documentation	36
9	Test requirements	36
9.1	Planning of tests	36
9.2	Test documentation.....	36
10	Modification.....	37
10.1	Objective.....	37
10.2	Requirements.....	37
10.2.1	Modification request	37
10.2.2	Impact analysis.....	37
10.2.3	Authorization	37
10.2.4	Documentation	37
	Annex A (informative) Sequential task table.....	38
	Annex B (informative) Example for determination of <i>PFH</i>	41
	Annex C (informative) Available failure rate databases	52
	Annex D (informative) Fault lists and rate exclusions	54
	Bibliography.....	64
	Figure 1 – Functional elements of a PDS(SR).....	9
	Figure 2 – PDS(SR) development lifecycle.....	19
	Figure 3 – Architectures for data communication (a) White channel; b) Black channel)	33
	Figure B.1 – Example PDS(SR)	41
	Figure B.2 – Subsystems of the PDS(SR)	42
	Figure B.3 – Function blocks of subsystem A/B.....	43
	Figure B.4 – Reliability model (Markov) of subsystem A/B.....	46
	Figure B.5 – Function blocks of subsystem PS/VM.....	48
	Figure B.6 – Reliability model (Markov) of subsystem PS/VM	50
	Table 1 – Alphabetical list of definitions	11
	Table 2 – Safety integrity levels: target failure measures for a PDS(SR) safety function	24
	Table 3 – Hardware safety integrity: architectural constraints on type A safety-related subsystems.....	27
	Table 4 – Hardware safety integrity: architectural constraints on type B safety-related subsystems.....	28

	<i>Page</i>
Table B.1 – Determination of DC factor of subsystem A/B.....	45
Table B.2 – PFH value calculation results for subsystem A/B.....	47
Table B.3 – Determination of DC factor of subsystem A/B.....	48
Table B.4 – PFH value calculation results for subsystem PS/VM.....	51
Table D.1 – Conductors/cables	55
Table D.2 – Printed wiring boards/assemblies.....	55
Table D.3 – Terminal block	56
Table D.4 – Multi-pin connector	56
Table D.5 – Electromechanical devices (for example relay, contactor relays).....	57
Table D.6 – Transformers	57
Table D.7 – Inductances	58
Table D.8 – Resistors	58
Table D.9 – Resistor networks	58
Table D.10 – Potentiometers.....	59
Table D.11 – Capacitors	59
Table D.12 – Discrete semiconductors (for example diodes, Zener diodes, transistors, triacs, GTO thyristors, IGBTs, voltage regulators, quartz crystals, phototransistors, light-emitting diodes [LEDs]).....	59
Table D.13 – Optocouplers	60
Table D.14 – Non-programmable integrated circuits.....	60
Table D.15 – Programmable and/or complex integrated circuits.....	61
Table D.16 – Motion and position feedback sensors	62

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.

AUSTRALIAN STANDARD

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).