

ICS 29.020
CCS K 62



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 12668.502-2013

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

调速电气传动系统 第5-2部分：安全要求 功能

(English Translation)

Issued on: November 12, 2013

Implemented on: August 7, 2014

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China, Standardization
Administration of the People's Republic of China**

Table of Contents

Foreword

1 Scope

2 Normative references

3 Terms and definitions

3.1 Common Cause Failure 3.14 Security Failure

3.2 Dangerous Failure 3.15 Safety Failure Score

3.3 Diagnostic coverage 3.16 [PDS (SR)] security function

3.4 Diagnostic Test 3.17 Safety Integrity

3.5 Fault response function 3.18 Safety integrity level

3.6 Functional Safety 3.19 Safety Related Systems

3.7 Hazard 3.20 Safety Requirements Specification

3.8 Device 3.21 Safety Integrity Level Capability

3.9 Run Time 3.22 Subsystem

3.10 Operating Mode 3.23 Systematic Failure

3.11 Electrical Drive Systems (Safety Related) 3.24 System Safety Integrity

3.12 PFH 3.25 Confirmation

3.13 Inspection Test 3.26 Verification

4 Specific security features

4.1 General

4.2 Security features

Foreword

GB/T 12668 "Speed Control Electric Drive System" is divided into the following parts.

---Part 1. General requirements for the rated value of the low-voltage DC-regulated electric drive system;

---Part 2. General requirements for the rated value of low-voltage AC variable frequency electric drive system;

--- Part 3. Electromagnetic compatibility requirements and their specific test methods;

---Part 4. General requirements for AC speed control electric drive systems with AC voltages above 1000V but not exceeding 35kV Provision of value;

- Part 5. Safety requirements;
- Part 6. Guidelines for determining the type of load duty and the corresponding current rating;
- Part 7. General interface and specification for electric drive systems;
- Part 8. Specification of the power supply interface voltage.

This part is part 5-2 of GB/T 12668.

This part is drafted in accordance with the rules given in GB/T 1.1-2009.

This part uses the translation method equivalent to IEC 61800-5-2:2007 "Speed Control Electric Drive System Part 5-2. Safety Requirements can".

The documents of our country that have a consistent correspondence with the international documents referenced in this part are as follows.

- GB/T 20438 (all parts) Functional safety of electrical/electronic/programmable electronic safety related systems [IEC 61508 (all section)];
- GB/T 24339 (all parts) Rail transit communication, signal and processing systems [IEC 62280 (all parts)].

This section has made the following editorial changes.

- The decimal point symbol replaces "," with ".";
- For unnumbered column items, the first level of the column item is preceded by a dash;
- Removed the preface to international standards.

This part was proposed by China Electrical Equipment Industry Association.

This part is under the jurisdiction of the National Power Electronics Standardization Technical Committee (SAC/TC60).

This section drafted by. Tianjin Electric Drive Design Institute, Shenzhen Yingweiteng Electric Co., Ltd., Shanghai Aotong Weir Power Electronics Co., Ltd., Beijing Hekang Yisheng Frequency Technology Co., Ltd., Hope Senlan Technology Co., Ltd., Beijing Lied Huafu Electric Co., Ltd.

Technology Co., Ltd., Shenzhen Kumak New Technology Co., Ltd., Harbin Kyushu Electric Co., Ltd., Shandong Xinfengguang Electronics Division Technology Development Co., Ltd., MCC Saidi Electric Technology Co., Ltd., Shandong Taikai Automation Co., Ltd., Guangzhou Zhiguang Electric Co., Ltd.

Shanghai Renault Technology Co., Ltd., Beijing ABB Electric Drive System Co., Ltd., National Electrical Control and Distribution Equipment Quality Supervision and Inspection Heart, Guangdong Huana East Energy Co., Ltd.

1 Scope

This part of GB/T 12668 specifies the design of the electric drive system (safety related) [PDS (SR)] from the perspective of functional safety.

Development, integration, and verification, detailed requirements, and recommendations.

This section applies to other standards related to variable speed electric drive systems in "Speed Control Electric Drive System".

Note 1: The term "integration" is for the PDS (SR) itself, not for security-related applications.

This section applies only when the functional safety of the PDS (SR) is identified and the PDS (SR) is operated in a high demand or continuous mode (see 3.10).

For low demand applications, see IEC 61508.

This part is a product standard that describes the PDS (SR) safety related considerations in the IEC 61508 architecture and introduces the PDS.

(SR) is required as a safety-related subsystem. This section is intended to promote PDS (SR) electrical/electronic/programmable electronic components (E/E /PE) to implement the security features of the PDS security function.

Manufacturers and suppliers of PDS (SR) design to control systems integrators and outfits by using this part of the regulatory requirements , etc.) show the security features of their devices. By applying the principles of IEC 61508 and implementation in their related fields (eg IEC 61511, IEC 61513, IEC 62061) or ISO 13849 help to incorporate PDS (SR) into safety-related control systems.

All requirements required for PDS (SR) in IEC 61508 are met in accordance with this section.

This section does not address the following requirements.

- Hazard and risk analysis for specific applications;
- Identification of security features for specific applications;
- The initial assignment of those safety functions to the Safety Integrity Level (SIL);
- Transmission equipment other than interface configuration;
- Secondary hazards (such as failures in production and manufacturing processes);
- Electrical, thermal and energy safety considerations included in IEC 61800-5-1;
- PDS (SR) production process;
- The effectiveness of the PDS (SR) signal and instructions.

Note 2: The functional safety requirements for PDS (SR) are application dependent and must be considered as part of the overall risk assessment of the equipment. PDS (SR) supplier does not drive where the equipment is responsible, the equipment designer is responsible for the risk assessment and specifies the overall functional and safety requirements of the PDS (SR).

Note 3: Even though malicious behavior can affect the functional security of PDS (SR), the guarantee issue is not considered in this section.

This section only applies to PDS (SR) which is not greater than the safety function of SIL3 SIL.

Figure 1 shows the functional components of the PDS (SR) considered in this section.

Figure 1 Functional components of PDS (SR)

Figure 1 is a logical representation of the PDS (SR), not a physical description.

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only dated versions apply to this article.

Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 20438.1-2006 Functional safety of electrical/electronic/programmable electronic safety systems - Part 1. General requirements (IEC 61508-1:1998, IDT) GB/T 20438.2-2006 Functional safety of electrical/electronic/programmable electronic safety related systems - Part 2. Electrical/electronic /Requirements for programmable electronic safety related systems (IEC 61508-2:2000, IDT) GB/T 20438.3-2006 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3. Software requirements (IEC 61508-3:1998, IDT) GB/T 20438.6-2006 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6 Application Guide for GB/T 20438.2 and GB/T 20438.3 (IEC 61508-6:2000, IDT) GB/T 20438.7-2006 Functional safety of electrical/electronic/programmable electronic safety related systems Part 7. Techniques and measures Overview (IEC 61508-7:2000, IDT) IEC 60204-1 Mechanical safety machinery and electrical equipment - Part 1. General technical conditions (Safetyofmachinery-Electricalequipmentofmachines-Part 1: Generalrequirements) IEC 61508 (all parts) Functional safety of electrical/electronic/programmable electronic safety related systems (Functional safety of Electrical/electronic/programmableelectronicsafety-relatedsystems) Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5. Determination of safety integrity, etc.

Level method example

(Functionalsafetyofelectrical/electronic/programmableelectronicsafety-relatedsys-tems-Part