

ICS 25.040
CCS N 10



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

GB/T 20438.1-2017

**Functional safety of electrical/electronic/programmable
electronic safety-related systems -- Part 1: General
requirements**

(English Translation)

Issued on: December 29, 2017

Implemented on: July 1, 2018

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine**

Table of Contents

FOREWORD...	4
INTRODUCTION...	6
1 Scope...	9
2 Normative references...	12
3 Definitions and abbreviations...	13
4 Conformance to GB/T 20438...	13
5 Documentation...	14
5.1 Objectives...	14
5.2 Requirements...	14
6 Management of functional safety...	16
6.1 Objectives...	16
6.2 Requirements...	16
7 Overall safety lifecycle requirements...	21
7.1 General...	21
7.2 Concept...	31
7.3 Overall scope definition...	31
7.4 Hazard and risk analysis...	32
7.5 Overall safety requirements...	35
7.6 Overall safety requirements allocation...	38
7.7 Overall operation and maintenance planning...	46
7.8 Overall safety validation planning...	49
7.9 Overall installation and commissioning planning...	50
7.10 E/E/PE system safety requirements specification...	52
7.11 E/E/PE safety-related systems - realisation...	55
7.12 Other risk reduction measures - specification and realisation...	56
7.13 Overall installation and commissioning...	56
7.14 Overall safety validation...	57
7.15 Overall operation, maintenance and repair...	58
7.16 Overall modification and retrofit...	62
7.17 Decommissioning or disposal...	65
7.18 Verification...	67
8 Functional safety assessment...	68

8.1 Objective...	68
8.2 Requirements...	68
Annex A (Informative) Example of a documentation structure...	74
Bibliography...	80

FOREWORD

GB/T 20438 "Functional safety of electrical/electronic/programmable electronic safety-related systems" is divided into seven parts.

- Part 1.General requirements;
- Part 2.Requirements for electrical/electronic/programmable electronic safety-related systems;
- Part 3.Software requirements;
- Part 4.Definitions and abbreviations;
- Part 5.Examples of methods for the determination of safety integrity levels;
- Part 6.Guidelines on the application of GB/T 20438.2 and GB/T 20438.3;
- Part 7.Overview of techniques and measures;

This Part is Part 1 of GB/T 20438.

This Part was drafted in accordance with the rules given in GB/T 1.1-2009.

This Part replaces GB/T 20438.1-2006 "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1. General requirements". Compared with GB/T 20438.1-2006, the major technical changes are as follows.

- Add the requirements for the competence of persons in management of functional safety (see Clause 6);
- Add the E/E/PE system safety requirements specification phase in the overall safety lifecycle (see 7.10);
- Modify the evaluation method for evaluating independence (see Clause 8).

This Part uses the translation method to equivalently adopt IEC 61508-1:2010 "Functional safety of electrical/electronic/programmable electronic safety-

related systems - Part 1.General requirements".

This Part was proposed by China Machinery Industry Federation.

This Standard shall be under the jurisdiction of National Technical Committee

124 on Industrial Process Measurement and Control of Standardization

Administration of China (SAC/TC 124).

The drafting organizations of this Part. Instrumentation Technology and Economy Institute, Beijing SP Zhishen Control Technology Co., Ltd., China Academy of Safety Science and Technology, Shanghai Institute of Process Automation & Instrumentation, Hangzhou Hollysys Automation Co., Ltd., Omron Industrial Automation (China)Co., Ltd., Siemens Ltd. China, ZONHO Electronic Technology Research and Design Institute of Shanghai.

The drafters of this Part. Feng Xiaosheng, Xiong Wenze, Pan Gang, Shi Xueling, Wu Zongzhi, Luo An, Zhou Youzheng, Yang Liu, Fang Laihua, Li Jiajia, Li Jia, Zheng Wei, Zhang Long, Wang Haiqing, Meng Zouqing, Mei Hao.

The previous versions of the standards which are replaced by this Part.

-- GB/T 20438.1-2006.

1 Scope

GB/T 20438.1, GB/T 20438.2, GB/T 20438.3 and GB/T 20438.4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.3 of GB/T 20438.4-2017).

As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51.

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.

GB/T 20438.2-2017, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2.Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2010, IDT)

3 Definitions and abbreviations

For the purposes of this document, the definitions and abbreviations given in GB/T 20438.4-2017 apply.

4 Conformance to GB/T 20438

The following equipment and materials shall be used.

GB/T 20438 specifies the requirements for E/E/PE safety-related systems and has been developed to meet the full range of complexity associated with such systems.

5 Documentation

The information to be documented shall be as stated in the various clauses of this standard unless justified or shall be as specified in the product or application sector standard relevant to the application

6 Management of functional safety

Suppliers providing products or services to an organization having overall responsibility for one or more phases of the overall, E/E/PE system or software safety lifecycles (see 6.2.1), shall deliver products or services as specified by that organization and shall have an appropriate quality management system.