

ICS 25.040
CCS N 10



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

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
(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...	3
Introduction...	5
1 Scope...	8
2 Normative references...	10
3 Definitions and abbreviations...	12
4 Conformance to GB/T 20438...	12
5 Documentation...	12
6 Management of functional safety...	12
7 E/E/PE system safety lifecycle requirements...	12
7.1 General...	12
7.2 E/E/PE system design requirements specification...	17
7.3 E/E/PE system safety validation planning...	20
7.4 E/E/PE system design and development...	21
7.5 E/E/PE system integration...	52
7.6 E/E/PE system operation and maintenance procedures...	54
7.7 E/E/PE system safety validation...	56
7.8 E/E/PE system modification...	58
7.9 E/E/PE system verification...	59
8 Functional safety assessment...	61

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 2 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 20438.2-2006 "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2. Requirements for electrical/electronic/programmable electronic safety-related systems". Compared with GB/T 20438.2-2006, the major technical changes are as follows.

-- Add ASIC development lifecycle (see Figure 3);

-- Add safety manual for compliant items (see Annex D).

This Part uses the translation method to equivalently adopt IEC 61508-2:2010 "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2.Requirements for electrical/electronic/programmable electronic safety-related systems".

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., Pilz Industrial Automation Trading (Shanghai) Co., Ltd., Shanghai Institute of Process Automation & Instrumentation, Beijing Hollysys System Engineering 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. Shi Xueling, Tian Yucong, Feng Xiaosheng, Huang Zhijiong, Zhang Aisen, Zheng Wei, Zhou Youzheng, Hua Rong, Luo An, Xiong

Wenze, Yang Liu, Li Jia, Mei Hao, Zhou Chunjie, Xu Aidong, Qian Datao, Meng Zouqing, Liu Yao, Wang Deji.

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

-- GB/T 20438.2-2006.

1 Scope

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. GB/T 20438.1, GB/T 20438.2, GB/T

20438.3 and GB/T 20438.4 are also intended for use as stand-alone publications.

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 20438.1-2017, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1. General requirements (IEC 61508-1:2010, 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 requirements for conformance to this part are as detailed in Clause 4 of GB/T 20438.1-2017.

5 Documentation

The requirements for documentation are as detailed in Clause 5 of GB/T 20438.1-2017.

6 Management of functional safety

The requirements for management of functional safety are as detailed in Clause

7 E/E/PE system safety lifecycle requirements

When quantifying the effect of random hardware failures of a subsystem, having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if.

8 Functional safety assessment

The requirements for functional safety assessment are as detailed in Clause 8 of GB/T 20438.1-2017.

Annex A

(Normative)

Techniques and measures for E/E/PE safety-related systems -
control of failures during operation

This annex shall be used in conjunction with 7.4.

.....