

ICS 25.040

CCS N 10



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

GB/T 20438.3-2017

**Functional safety of electrical/electronic/programmable
electronic safety-related systems -- Part 3: Software
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 this Standard...	13
5 Documentation...	13
6 Additional Requirements for Management of Safety-Related Software...	13
6.1 Objectives...	13
6.2 Requirements...	13
7 Software Safety Lifecycle Requirements...	15
7.1 General...	15
7.2 Software safety requirements specification...	23
7.3 Validation plan for software aspects of system safety...	28
7.4 Software design and development...	30
7.5 Programmable electronics integration (hardware and software)...	46
7.6 Software operation and modification procedures...	48
7.7 Software aspects of system safety validation...	49
7.8 Software modification...	51
7.9 Software verification...	53
8 Functional Safety Assessment...	60
Annex A (Normative) Guide to the Selection of Techniques and Measures...	61
Annex B (Informative) Detailed Tables...	69
Annex C (Informative) Properties for Software Systematic Capability...	74

Foreword

GB/T 20438 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems can be divided into the following 7 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 3 of GB/T 20438.

This Part was drafted as per the rules specified in GB/T 1.1-2009.

This Part replaced GB/T 20438.3-2006 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 3. Software Requirements. Compared with GB/T 20438.3-2006, the major technical changes of this Standard are as follows.

- Add the attributes of the software's systematic capabilities (see Annex C of this Edition);
- Add additional requirements for compliance item safety manual - software components (see Annex D of this Edition);
- Add the relationship between GB/T 20438.2 and GB/T 20438.3 (see Annex E of this Edition);
- Add a technology for non-interference between software components in a single computer (see Annex F of this Edition);
- Add life cycle tailoring guidelines for data-driven systems (see Annex G of this Edition).

This Part uses translation method to equivalently adopt IEC 61508-3:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 3. Software Requirements.

This Part was proposed by China Machinery Industry Federation.

This Part shall be under the jurisdiction of National Technical Committee on Industrial Process Measurement, Control and Automation of Standardization (SAC/TC 124).

Drafting organizations of this Part. Instrumentation Technology and Economy Institute of China; Beijing SP Zhishen Control Technology Co., Ltd.; Shanghai Institute of Process

Automation & Instrumentation; Pilz Industrial Automation Trading (Shanghai) Co., Ltd.; Beijing HollySys Co., Ltd.; Omron Industrial Automation (China) Co., Ltd.; Siemens (China) Co., Ltd.; and Zonho Electronics Co., Ltd.

Chief drafting staffs of this Part. Feng Xiaosheng, Xia Ming, Xiong Wenzhe, Shi Xueling, Zhou

Youzheng, Yang Liu, Huang Zhijiong, Luo An, Zhuang Lingyun, Li Jia, Liu Xiaodong, Mei Hao, Hua Rong, Zhang Long, Ye Jun, Chu Weizhong, Qiu Kun, Meng Zouqing, Xiao Jiaqi, and Wang Deji.

The historical edition replaced by this Part is as follows.

--- GB/T 20438.3-2006.

1 Scope

One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

2 Normative References

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) is applicable to this document.

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-

4 Conformance to this Standard

The requirements for conformance of this Part to GB/T 20438 are given in Clause 4 of GB/T

20438.1-2017.

5 Documentation

The objectives and requirements for documentation are given in Clause 5 of GB/T 20438.1-2017.

6 Additional Requirements for Management of Safety- Related Software

The objectives are as detailed in 6.1 of GB/T 20438.1-2017.

The requirements are as detailed in 6.2 of GB/T 20438.1-2017, with the following additional requirements.

7 Software Safety Lifecycle Requirements

The objective of the requirements of 7.6 is to provide information and procedures concerning

software necessary to ensure that the functional safety of the E/E/PE safety-related system is maintained during operation and modification.

The objective of the requirements of 7.7 is to ensure that the integrated system complies with the software safety requirements specification at the required safety integrity level.

8 Functional Safety Assessment

For the selection of appropriate techniques and measures (see Annexes A and B) to implement the requirements of this clause, the following properties (see Annex C for guidance on

interpretation of properties, and Annex F of GB/T 20438.7-2017 for informal definitions) of the

functional safety assessment should be considered.

.....