

ICS 27.120.20
CCS F 83



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

GB/T 13629-2023

Replacing GB/T 13629-2008

**Criteria for programmable digital devices in safety systems of
nuclear power generating stations**

核电厂安全系统中可编程数字设备的适用准则

Issued on: December 28, 2023

Implemented on: April 1, 2024

**Issued by: State Administration for Market Regulation;
Standardization Administration of China**

Table of Contents

Foreword	III
1 Scope	1
2 Normative references	1
3 Terms and definitions, abbreviations	1
3:1 Terms and definitions	1
3:2 Abbreviations	2
4 Safety System Design Basis	3
5 Safety System Guidelines	3
5:1 Single Failure Criterion	3
5:2 Completion of protective action	3
5:3 Quality	3
5:4 Equipment Qualification	7
5:5 System integrity	7
5:6 Independence	9
5:7 Testing and calibration capabilities	12
5:8 Information display	12
5:9 Access control	14
5:10 Maintenance	18
5:11 Identification	19
5:12 Auxiliary facilities	19
5:13 Multi-unit nuclear power plants	19
5:14 Human Factors Engineering Considerations	19
5:15 Reliability	19
5:16 Common cause failure criterion	19
5:17 Use of commodity-grade digital devices	20
5:18 Simplicity	20
6 Function and design requirements for monitoring command equipment	21
7 Function and design requirements of execution device	21
8 Requirements for power source	21
Appendix A (informative) Hazard identification and control	22
A:1 Background	22
A:2 Purpose of hazard analysis	22

A:3 Hazard Analysis Implementation Guide	22
Appendix B (Informative) Communications Independence	34
B:1 Background	34
B:2 Discussion	34
Appendix C (informative) Determination of diversity needs	39
C:1 Diversity and Defense in Depth Analysis	39
C:2 Sufficient diversity to eliminate common cause failures	39
C:3 Increase diversity to address common cause failure vulnerabilities	39
C:4 Diversity of manual controls and displays	39
C:5 Diversity of automatic control	40
Appendix D (informative) Confirmation of applicability of commodity-level items	41
D:1 General principles	41
D:2 Preparation for confirmation of applicability of commodity-level items	41
D:3 Development of applicability confirmation of commodity-level items	42
D:4 Maintenance of product-level item suitability confirmation	44
Reference	46

Foreword

This document complies with the provisions of GB/T 1:1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents" Drafting:

This document replaces GB/T 13629-2008 "Applicable Guidelines for Digital Computers in Nuclear Power Plant Safety Systems" and is consistent with GB/T 13629-

Compared with:2008, in addition to structural adjustments and editorial changes, the main technical changes are as follows:

---Changed the scope of application of the document, changing "digital computer" to "programmable digital device" (see Chapter 1,:2008 version Chapter 1);

---Changed the definitions of the terms "commodity-level items", "firmware", "hazard" and "hazard analysis" (see Chapter 3, Chapter 3 of the:2008 edition);

---Deleted the terms and definitions "acceptance testing", "application software", "structure", "complexity", "component", "computer" and "computer instructions"

"Computer Program" "Computer System" "Configuration" "Configuration Control"
"Configuration Items" "Configuration Management" "Correctness" "Data" "Data Structure"

"Construction", "Design", "File", "Documentation", "Error", "Execution", "Failure", "Fault",
"Function", "Functional Unit", "Hardware", "Implementation", "Interface"

"Modules" "Procedures" "Qualification Tests" "Requirements" "Requirements Specifications" "Software" "Software Maintenance" "Software Quality Measurement" "Software Tools"

"Specification", "System", "System Software", "System Test", "Test", "Test Outline", "Confirmation", "Verification", "Verification and Confirmation" (see Chapter 3 of the:2008 edition);

---Added terms and definitions "safety state", "functional state", "key characteristics", "basic components", "programmable digital device", "digital security"

System-wide" (see Chapter 3);

---Added abbreviations (see 3:2);

---Added relevant criteria requirements for single faults (see 5:1);

---Changed the content of software tools used in digital devices, software and hardware development, firmware and programmable logic device development (see

5:3:3, :2008 version of 5:3:2);

---Added relevant requirements for function priority (see 5:5:5);

1 Scope

This document specifies the design guidelines for programmable digital equipment used in nuclear power plant safety systems, including safety system guidelines, monitoring command equipment

The function and design requirements of the actuator, the function and design requirements of the actuator, and the requirements for the power source:

This document applies to programmable digital devices in nuclear power plant safety systems:

2 Normative reference documents

The contents of the following documents constitute essential provisions of this document through normative references in the text: Among them, the dated quotations

For undated referenced documents, only the version corresponding to that date applies to this document; for undated referenced documents, the latest version (including all amendments) applies to this document:

GB/T 12727-2017 Qualification of safety-level electrical equipment for nuclear power plants

GB/T 13284:1-2008 Nuclear power plant safety system Part 1: Design criteria

GB/T 13625-2018 Seismic appraisal of safety-level electrical equipment in nuclear power plants

GB/T 22032-2021 System and software engineering system life cycle process

NB/T 20448-2017 Verification and validation of nuclear power plant systems and software

3 Terms and definitions, abbreviations

3.1 Terms and definitions

The following terms and definitions apply to this document:

A system state that is considered safe in its application scenario or a system condition that is consistent with the safety analysis of a nuclear power plant:

functionalstate functionalstate

The operating state of a component or system specified by the programmable digital device (PDD) design:

Note: Including operating mode, fault tolerance mode, and test/diagnosis/fault detection mode:

A combination of a hardware device and computer instructions and data that reside on the device as read-only software:

Note: For consistency with this document, firmware is treated as software in a programmable device:

In order to ensure that commodity-level items can perform their intended safety functions, the important design, materials and performance of the items need to be verified (including the design process)