

ICS 27.120.20
CCS F 83



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

GB/T 43532-2023

**Cybersecurity controls for instrumentation and control systems
of nuclear power plants**

核电厂仪表和控制系统网络安全防范管控
(English Translation)

Issued on: December 28, 2023

Implemented on: April 1, 2024

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Abbreviations
5 General Principles
6 Security Policy and Review
7 Cybersecurity Organizations
8 Human Resources Security
9 Asset Management
10 Access Control
11 Encryption Management
12 Physical and Environmental Security
13 Operational safety
14 Communication Security
15 System Acquisition, Development and Maintenance
16 Supplier Relations
17 Cybersecurity incident management
18 Cybersecurity aspects of business continuity management
19 Compliance
20 Nuclear Power Plants - Cybersecurity and Architecture
21 Nuclear Power Plant-Virtualized Environment and Facilities
Appendix A (Informative) Security Control Sources
Appendix B (informative) General considerations regarding security levels
Appendix C (informative) Security control details
References

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 is modified to adopt IEC 63096:2020 "Nuclear power plant instrumentation, control and power system network security prevention and control":

Compared with IEC 63096:2020, this document has made the following structural adjustments:

---Chapter 4 "Abbreviations" has been added, and the content of 3:2 in IEC 63096:2020 has been adjusted to Chapter 4 of this document, with the corresponding chapter number postpone in turn;

---According to the GB/T 1.1 format requirements, 5:1:1, 5:1:2, 7:3:1, 9:3:1, 10:1:1, 10:1:2, 12:2:1, 12:3:1, 12:7:1, 14:1:1, 14:3:1, 16:1:2~16:1:7, 17:2:1, 19:1:1~19:1:5, 20:1:1 are adjusted to 6:1, 6:2, 8:3, 10:3, 11:1, 11:2, 13:2, 13:3, 13:7, 15:1, 15:3, 17:2~17:7, 18:2, 20:1~20:5, 21, will 16:1:1:1~16:1:1:17 is adjusted to 17:1:1~17:1:7;

---Adjust 4:2:2~4:2:4 in IEC 63096:2020 to 5:2:1~5:2:3;

---Adjust the relevant instructions on safety control marks in 4:3:2 of IEC 63096:2020 to 5:3:3;

---Adjust 8:2:3 in IEC 63096:2020 to 9:1:5;

---Adjust the suspension section of 14:1:1:4 to 14:1:1:4:1, and the following bar numbers will be extended in sequence;

---Adjust the suspension section of 14:1:2 to 14:1:2:1, and the following bar numbers will be extended in sequence;

---Adjust the suspension section of 14:1:3 to 14:1:3:1, and the following bar numbers will be extended in sequence;

---Appendix A in the original IEC 63096:2020 is adjusted to Appendix C:

The technical differences between this document and IEC 63096:2020 and their reasons are as follows:

---According to the requirements of GB/T 1.1, the description of "Scope" in Chapter 1 has been changed (see Chapter 1):

---Replace ISO/IEC 27002:2013 with normatively quoted GB/T 22081-2016 (see 5.3:1~5:3:4, 5:4:2:1), to Adapt to my country's technical conditions and provide operability:

---Replace ISO/IEC 27033 (all parts) with normatively quoted GB/T 25068 (all parts) (see 12.2:6) to adapt my country's technical conditions provide operability:

---Replace ISO/IEC 27035 (all parts) with normatively quoted GB/T 20985 (all parts) [see 13.6:1u), 17:1:5e)], in order to adapt to my country's technical conditions and provide operability:

---In order to adapt to my country's technical conditions, this document has made some

adjustments to the content of Chapter 3, including:

- Changed the terms and definitions of "instrumentation and control systems" (see 3.2), "cybersecurity incidents" (see 3.8), and "cybersecurity incidents" (see 3.9), "Electrical/Electronic/Programmable Electronic Items" (see 3.13), "RACI Model" (see 3.21), "Safety Prevention Area Domain" (see 3.22);
- Added terms and definitions "security policy" (see 3.24), "security management and control of instrumentation and control platform and instrumentation and control system body" (see 3.25);
- The terms and definitions "third-party software (see IEC 63096.20203:1:1)" and "business continuity (see IEC 63096.20203:1:1)" are deleted:

20203:1:2)" "Application software (see IEC 63096.20203:1:4)" "Computer-based items (see IEC 63096:

20203:1:6)" "Existing instrumentation and control systems (see IEC 63096.20203:1:19)" "Mobile equipment (see IEC 63096.2020 3:1:21)" "Entity control (see IEC 63096.20203:1:24)" "Product (see IEC 63096.20203:1:25)" "Programmable Process logic items (see IEC 63096.20203:1:27)" "Serious safety events (see IEC 63096.20203:1:34)" "Source Code (see IEC 63096.20203:1:35)" "Applicability Statement (see IEC 63096.20203:1:36)" "Teleworking (See IEC 63096.20203:1:38)" "Tools (see IEC 63096.20203:1:39)" "Virtualization (see IEC 63096:

20203:1:40)" "World Wide Web (see IEC 63096.20203:1:41)":

---In order to adapt to my country's technical conditions, this document deletes abbreviations not used in the main text of Chapter 4, including:

---In order to adapt to my country's technical conditions, this document has made technical adjustments to Chapter 5, including:

- Change the title from "Safety Control of Nuclear Power Plant Instrumentation and Control Systems" to "General Principles" to better suit the content of this chapter and GB/T 1.1-Related requirements in 2020 (see Chapter 5);
- Adjust the description of network security prevention and control sources in 4:2:1 in IEC 63096:2020 to informative appendix A (see citation Word);
- Added relevant statistical data description on the safety control list (see 5.3:1);
- The description of the meaning of safety control of the instrumentation and control platform and the instrumentation and control system body has been deleted (see IEC 63096.20204:3), and Relevant definitions and descriptions have been added to terminology;
- Change "IEC SC45A network security standard" to "relevant network security standards"

(see 5.4:1, 5:4:2:1);

- Updated "Ontology safety management and control is executed on the instrument and control platform through the development environment without the need to carry out instrument and control platform development activities" Change to note (see 5.4:2:3):

---In order to adapt to my country's technical conditions, this document has made technical adjustments to Chapter 9, including:

- Change "ISO/IEC 19770" to "Relevant Management Requirements" [see 9.1:1c)];

- Changed the duplication of life cycle stages in IEC 63096:2020 [see 9.3:4d)];

---In order to adapt to my country's technical conditions, this document has made technical adjustments to Chapter 10, including:

- Changed the management requirements for the use of wireless networks by instrument and control systems with levels S3 and BR [see 10.1:2:4b)];

- Changed the duplication of life cycle stages in IEC 63096:2020 [see 10.4:3c)];

---In order to adapt to my country's technical conditions, this document has made technical adjustments to Chapter 11, including:

- Clarify the relevant national guidance as the "Cryptozoology Law of the People's Republic of China" [see 11.1h)];

---In order to adapt to my country's technical conditions, this document has made technical adjustments to Chapter 12, including:

- Changed the duplication of life cycle stages in IEC 63096:2020 [see 12.2:5e)];

- Changed the unspecified life cycle stages in IEC 63096:2020 [see 12.1:1g), 12:1:3b), 12:1:3q), 12:2:1q)];

- Added explanation about the "two-person principle" [see 12.1:2g)];

---In order to adapt to my country's technical conditions, this document has made technical adjustments to Chapter 13, including:

- Change the website link address for vulnerability release in IEC 63096:2020 to "Public Network for Vulnerability Release" Station" (see 13.6:3);

- Optimized the example on management capacity requirements in IEC 63096:2020 (see 13.1:3):

---In order to adapt to my country's technical conditions, this document has made technical adjustments to Chapter 17, including:

- Added relevant requirements for the establishment, implementation and maintenance of network security programs (see 17.1:7):