

ICS 25.040.30

CCS J 28



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

GB/T 39404-2026

Replacing GB/T 39404-2020

**General security requirements for the control units of industrial
robots**

工业机器人控制单元的信息安全通用要求

Issued on: April 30, 2026

Implemented on: November 1, 2026

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

Table of Contents

6 Information Security Requirements
6.3 General Technical Requirements for Information Security
6.3.1 Audit Requirements
6.3.2 Integrity Requirements
6.3.3 Confidentiality Requirements
6.3.4 Communication Reliability Requirements
6.3.5 Availability Requirements
6.3.6 System Requirements
6.4 Information security requirements between the main control and control units
6.4.1 Time Requirements
6.4.2 Labelling and Certification Requirements
6.5 Information security requirements within the control unit
6.5.1 Labelling and Certification Requirements
6.5.4 Programming Code Requirements

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 supersedes GB/T 39404-2020 "General Requirements for Information Security of Industrial Robot Control Units" and is consistent with GB/T 39404- Compared to 2020, aside from structural adjustments and editorial changes, the main technical changes are as follows:

a) The definition of "information security" has been changed (see 3.4, 2020 version 3.4);

b) The communication architecture diagram of the industrial robot control unit has been modified (see Chapter 5,

5.1 of the 2020 edition);

c) Removed "Vulnerability between teach pendant and industrial robot CU", "Vulnerability between main controller and industrial robot CU", and "Machine" Vulnerability between robot controllers and private server drivers (see sections 5.2, 5.3, and

5.4 in the 2020 edition);

d) The description of audit storage capacity has been changed (see 6.3.1.2, 6.3.1.3 in the 2020 version), and the protection of audit information has been modified (see 6.3.1.4, 2020 version). Version

6.3.1.5 of the 2018 version added "issue a warning when the audit log storage capacity limit is reached" (see 6.3.1.3), and removed "central..." "Managed, system-wide audit trails," "Responses to audit process failures," and "Audit logs written to media in a one-time process." "Accessibility of audit logs" (see 6.3.1.2, 6.3.1.4, 6.3.1.6, and

6.3.1.7 in the 2020 edition);

e) The description of communication integrity (see 6.3.2.1, 2020 version 6.3.2.1) and the description of cryptographic integrity protection (see...) have been modified. 6.3.2.2 (

6.3.2.2 in the 2020 version), software and information integrity description (see 6.3.2.3,

6.3.2.3 in the 2020 version), and damage control. Automatic notifications for bad integrity are now provided (see 6.3.2.4, version

6 Information Security Requirements

6.1 General Rules Information security for industrial robot control units should primarily include.

a) Information security between the main control and control units;

b) Information security within the control unit. Information security requirements for industrial robot control units include system requirements (SR) and system enhancement requirements (RE), and should comply with GB/T 30976.1- The relevant requirements of 2014 and GB/T 33008.1-2016 apply. See Appendix B for the information security classification requirements for industrial robot control units.

6.2 Physical Requirements for Information Security Information security physical requirements shall comply with the requirements of B.7 in GB/T 32919-2016.

6.3.1 Audit Requirements

6.3.1.1 Auditable Events Auditable events (SR2.8) should comply with the requirements of 6.3.8 in GB/T 30976.1-2014. The control unit should generate the following events. Audit Log.

a) Access control;

b) Request error;

c) System events;

d) Backup and storage events;

e) Configuration changes;

f) Potential investigative activities and audit log events.

Note. Auditable events can be viewed on the teach pendant, programming software, or other human-machine interfaces.

6.3.1.2 Audit Storage Capacity The audited storage capacity (SR2.9) should comply with the requirements of

6.3.9 in GB/T 30976.1-2014. The control unit should be based on log management... The system should be configured to allocate sufficient audit log storage capacity. The control unit should provide auditing mechanisms to reduce the possibility of exceeding this capacity. The system can provide sufficient audit storage capacity based on factors including, but not limited to, storage policies and audits to be performed.

6.3.1.3 Issue a warning when the audit log storage capacity limit is reached. A warning should be issued when the audit log storage capacity limit is reached [SR2.9RE(1)], which should comply with

6.3.9.1 of GB/T 30976.1-2014. Requirements. When the allocated audit log storage volume reaches a configurable proportion of the maximum audit log storage capacity, the control unit should issue a warning, and It should have the capability to back up audit logs to a separate external storage space to ensure their integrity. Simultaneously, warning messages and backup operation status should be displayed. It can be viewed through the human-computer interface.

6.3.1.4 Protection of Audit Information The protection of audit information (SR3.9) shall comply with the requirements of

6.3.2 Integrity Requirements

6.3.2.1 Communication Integrity Communication integrity (SR3.1) shall comply with the requirements of

6.4.1 in GB/T 30976.1-2014. Robot controller and teach pendant, programming. Software should protect the integrity of information transmitted over communication channels.

6.3.2.2 Integrity Protection Based on Cryptographic Technology Integrity protection based on cryptographic technology [SR3.1RE(1)] shall comply with the requirements of

6.4.1.1 in GB/T 30976.1-2014. Control The unit should employ cryptographic mechanisms to identify changes to information during communication, and to protect communications where information has been protected by other alternative physical measures. This requirement does not apply to links. Note

1. Cryptographic mechanisms include, but are not limited to, message digest algorithms, message authentication codes, digital signatures, and other technologies. Note

2. Physical protection measures include, but are not limited to, dedicated cables, physically isolated networks, and enclosed communication backplanes.

6.3.2.3 Software and Information Integrity Software and information integrity (SR3.4) shall comply with the requirements of

6.4.4 in GB/T 30976.1-2014. The control unit shall possess software, The ability of firmware to resist unauthorized modifications.

6.3.2.4 Automatically notify of breaches of integrity Automatic notification of breaches of integrity [SR3.4RE(1)] shall comply with the requirements of

6.4.4.1 in GB/T 30976.1-2014. Control The unit should notify the user if any discrepancies are found during integrity verification.

6.3.3 Confidentiality Requirements

6.3.3.1 Information confidentiality Information confidentiality (SR4.1) shall comply with the requirements of

6.5.1 in GB/T 30976.1-2014. The control unit shall ensure that information is stored and Confidentiality during transmission.

6.3.3.2 Encryption Protocol Security The security of the data encryption algorithm should be guaranteed, and there should be no security risks such as weak keys, predictable random numbers, or identity forgery.

6.3.3.3 Information Retention Information retention (SR4.2) shall comply with the requirements of

6.5.2 in GB/T 30976.1-2014. The control unit shall provide decommissioning capability and clear [data/information]. All security-related data in components released by services in use.

6.3.4 Communication Reliability Requirements

6.3.4.1 Bus Topology The high-speed communication bus used for control unit communication can form a site network structure that conforms to tree, chain, star, or ring network structures. One or more of the structures.

6.3.4.2 Error Checking The high-speed communication bus data link layer protocol of the control unit should include error detection and correction functions for the transmitted data.

6.3.4.3 Maximum Communication Delay The maximum communication delay of the control unit's high-speed communication bus should meet the real-time communication requirements of the specific application.

6.3.4.4 Time Synchronization Accuracy The control unit should achieve time