ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 47689-2026

Cybersecurity technology - Security technical specification for embedded operating systems

网络安全技术 嵌入式操作系统安全技术规范

Issued on: May 25, 2026 **Implemented on: December 1, 2026**

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

Table of Contents

5 General Rules

Embedded operating systems typically run on computer systems or hardware devices with specific requirements for computing and storage capabilities, and are therefore specialized. It features powerful performance, streamlined system, high real-time performance, and multitasking capabilities. Embedded operating systems typically include basic functions and security functions; the basic functions generally... Includes hardware management modules (drivers, board support packages), computing modules (task management, process management), storage modules, communication modules, and software (system). The system software (including application software) includes management modules, human-computer interaction modules, user management modules, etc., and security functions generally include network access security and communication security. The embedded operating system security framework includes security features such as identity authentication and access control, as shown in Figure

1.Embedded operating systems have wide applications and are used in various scenarios. The functional requirements vary considerably. By customizing and configuring the embedded operating system, different combinations of functions can be achieved to meet various application scenarios. need.

6.1.1 Network Access Security

6.1.1.1 Network Access Authentication The functional requirements are as follows:

a) It should have the function of uniquely identifying terminal devices on the network;

b) It should have a two-way authentication mechanism for terminal devices accessing the network.

6.1.1.2 Network Access Control The functional requirements are as follows:

a) The principle of minimizing network port exposure should be followed, and communication ports other than those required for business needs should be disabled;

b) It should be able to set network access control policies to prevent unauthorized network access;

c) It should have the function of limiting network traffic.

6.1.2 Communication security The functional requirements are as follows:

a) A security mechanism based on cryptography should be adopted to ensure the integrity of important data transmissions such as control commands, authentication data, and key data. The cryptographic techniques used are in accordance with the relevant regulations of the national cryptography administration department, ensuring security and confidentiality.

b) Security measures, such as using sequence codes or timestamps, should be adopted to prevent replay attacks.

6.1.3 Identity Authentication For scenarios involving user login to the operating system, the system must have identity authentication capabilities, with the following requirements.

a) User identities should be identified and verified;

b) When using password authentication, a function to verify the complexity of identity authentication information should be provided;

c) A login failure handling function should be provided, such as limiting the number of consecutive login failures;

6.1.14 Data Security

6.1.14.1 Data Integrity The functional requirements are as follows:

a) Perform integrity checks on important stored data (such as authentication data, key data, system configuration data, etc.);

b) Necessary recovery measures should be taken when an integrity error is detected.

6.1.14.2 Data Availability The functional requirements are as follows:

a) It should be able to back up important data (such as basic data that ensures the normal operation of the system);

b) It should have a data loss protection mechanism, and be able to take necessary measures (such as alarms, opening new storage spaces) when it detects that the system storage space is about to run out. Temporary storage areas, etc., to prevent data loss.

6.1.14.3 Data Confidentiality Important data such as authentication data, key data, and system configuration data should be encrypted and protected.

6.1.15 Reliability Requirements

6.1.15.1 Resource Constraints The system should provide a mechanism for detecting and controlling resource usage to prevent applications from consuming resources without limit due to logical errors or malicious behavior.

6.1.15.2 Failure Protection The system should be able to self-detect defined system faults and provide corresponding protection measures to prevent the system from being in a state of failure due to faults.

6.1.15.3 Reliable Clock The system should provide functions such as manually setting the system clock or automatically synchronizing the clock through a remote clock service.

6.2.1 Development

6.2.1.1 Security Architecture Developers should provide a security architecture description for the embedded operating system's security features. This security architecture description should meet the following requirements.

a) Consistent with the level of abstract description of security functions in the system design document;

b) Describe the security domains of the embedded operating system security functions that are consistent with the security function requirements;

c) Describe why the initialization process of the embedded operating system's security features is secure;

d) Verify that the embedded operating system's security features can prevent breaches;

e) Verify that the embedded operating system's security features can prevent security features from being bypassed.

6.2.1.2 Functional Specifications Developers should provide a system functional specification, which should meet the following requirements.

a) Describe the security features of the embedded operating system;

b) Describe the purpose and usage of all security function interfaces;

c) Identify and describe all parameters associated with each security function interface;

d) Describe the implementation behavior of security functions related to the security function interfaces;

e) Describe the direct error message caused by the behavior processing implemented by the security function;

f) Verify the traceability from security function requirements to security function interfaces.

6.2.1.3 Implementation Representation Developers should provide implementation representations for all security features, and these should meet the following requirements.

6.2.2 Guidance Documents

6.2.2.1 User Guide Developers should provide clear and reasonable user guidelines, which should be consistent with all other documentation provided for the evaluation. Therefore, the description of each user role should meet the following requirements.

a) Describe the user-accessible functions and privileges controlled within the secure processing environment, including appropriate warning messages;

b) Describe how to use the available interfaces provided by the embedded operating system in a safe manner;

c) Describe the available functions and interfaces, especially all security parameters under user control, and specify the security values where appropriate;

d) Clearly describe every security-related event associated with the user-accessible functionality that needs to be performed, including changes to the security functionality controlled by it. Safety characteristics of the controlled entity;

e) Identify all possible states of the embedded operating system (including operational failures or operational errors), and their... The causal relationship and connection between and maintaining safe operation;

f) Clearly state the security policies implemented to achieve security objectives.

6.2.2.2 Preparation Procedure Developers should provide an embedded operating system and its preparatory procedures. The description of the preparatory procedures should meet the following requirements.

a) Describe all steps necessary for securely receiving the delivered embedded operating system, consistent with the developer's delivery procedure;

b) Describe all the steps necessary for the secure installation of an embedded operating system and its operating environment.