

ICS 35.240
CCS A 90

GA

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

GA/T 1560-2019

**Information security technology - Security technical
requirements for security protecting and audit monitoring
products for industrial control system host**

信息安全技术 工业控制系统主机安全防护与审计监控产品安全技术要求
(English Translation)

Issued on: January 1, 1970

Implemented on: April 16, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Industrial control system host security protection and audit monitoring product description	
5 Safety function requirements	
5.1 Access Control	
5.2 Audit and monitoring of operational behavior	
5.3 Data security exchange	
5.4 Information display and data analysis	
5.5 Time synchronization	
5.6 User ID	
5.7 Identification	
5.8 Security audit	
5.9 Security management functions	
5.10 Hardware Failure Handling	
5.11 Network performance requirements	
6 Security requirements	
6.1 Development	
6.2 Guidance documents	
6.3 Life cycle support	
6.4 Testing	
6.5 Vulnerability assessment	
7 Classification of Security Levels and Requirements	
7.1 Classification	
7.2 Safety function requirements	
7.3 Security requirements	

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, and the Third Research Institute of the Ministry of Public Security.

1 Scope

This standard specifies the security function requirements, security guarantee requirements, and rating plans for industrial control system mainframe security protection and audit monitoring products.

This standard applies to the design, development, and testing of industrial control system mainframe security protection and audit monitoring products.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information technology security technology Information technology security assessment guidelines Part 3. Security assurance components GB/T 25069-2010 Information Security Technology Terminology GB/T 32919-2016 Information Security Technology Industrial Control System Security Control Application Guide

3 Terms and definitions

The terms and definitions defined in GB/T 18336.3-2015, GB/T 25069-2010, and GB/T 32919-2016, as well as the following terms, apply to this document Pieces.

Industrial control system host it is used in the field of industrial control systems, mainly for computers for monitoring and management, including the upper computer of industrial control systems.

Security protecting device Device for monitoring keyboard input, mouse operation, copy of removable storage media, and monitor screen of a protected host.

Security protecting platform A platform that receives audit and monitoring data uploaded by security protection devices, and performs data analysis and security policy configuration.

Data ferrying

A mechanism for implementing data exchange between the host computer of the industrial control system and the mobile storage medium by using a safety protection device, internal and external the port cannot communicate with the security protection device on the physical link at the same time, and the information transmission is completed by the ferry mode.

4 Industrial control system host security protection and audit monitoring product description

Industrial control system mainframe security protection and audit monitoring products are mainly structured by components such as security protection devices, security protection platforms, etc.

It is mainly used for security protection and audit monitoring of the mainframe of the industrial control system.

Figure 1 shows the typical deployment environment of this product, in which the safety protection device is deployed in an armored manner, which is mainly used to connect the engineer station,

Various peripheral interfaces of the host of industrial control system such as operator station, such as. VGA interface, USB interface, PS/2 interface, etc.

Access control of the host system's peripheral interface of the control system; the security protection platform is connected to the security protection device through a network, and is mainly used to receive security the audit and monitoring data uploaded by the protective device, and support for issuing security policies to achieve data ferry, data analysis and other functions. In addition, the property the product provides a malicious code defense server, which provides functions such as malicious code detection and data encapsulation of ferry data.

Industrial control network Engineer Station/Operator Station Mouse and keyboard Safety protection device safety protection platform monitor Peripheral interface Malicious code defense server Removable storage media

Figure 1 Typical deployment environment of industrial control system host security protection and audit monitoring products

5.1 Access control

The product shall be able to implement the following access control policies for the subject, object, and all operations between the subject and object.

a) Support the setting of access control policies according to the subject (such as. access

users, etc.), objects (such as protected hosts, etc.) and access rights;

b) the information flow sent and received between the subject and the object is transmitted after being allowed by the security policy;

c) Subject access rights include at least. protected host management rights, audit data query, access control policies, etc.

5.2.1 Operational behavior audit

The product shall record operational behavior, including but not limited to.

a) Provide graphical real-time monitoring function of industrial control system host;

b) Record the operation behavior of the industrial control system host through the keyboard and mouse;

c) recording the operation of the main body of the industrial control system for data exchange through the mobile storage exchange medium;

d) Record the operation behavior of the mainframe of the industrial control system for operation and maintenance management through the network.

5.2.2 Operation Behavior Response

The product shall respond to operations that violate access control policies, such as response policies such as log audits and dialog box alarms.

5.2.3 Traceback of operation events

The product shall support operational event traceback, including.

a) Supporting the traceback of the process of data exchange by users through mobile storage exchange media;

b) Supports the selection of designated nodes for backtracking operations, and can be checked by event occurrence time, audit event category, subject, object Inquiry.

5.2.4 Real-time monitoring

Products should support real-time monitoring capabilities, including.

a) Real-time monitoring of the current login status of the protected host, which can be found in time when an access person logs in;

b) Real-time monitoring of safety protection devices, which can be found in time when disconnected in the event of a failure.