

ICS 35.040
CCS A 90

GA

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

GA/T 1562-2019

**Information security technology - Security technical
requirements for boundary security special gateway products
of industrial control system**

信息安全技术 工业控制系统边界安全专用网关产品安全技术要求
(English Translation)

Issued on: January 1, 1970

Implemented on: May 5, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Acronyms
5 General description
5.1 Classification of safety technical requirements
5.2 Classification of Security Levels.
6 Safety function requirements
6.1 Whitelist-based access control
6.2 Control function protection
6.3 Attack response processing
6.4 Time proofreading
6.5 Business audit
6.6 Industrial control protocol support
6.7 Suitable for a variety of field environments
6.8 Time synchronization
6.9 Dual-System Hot Backup
6.10 Support IPv4/IPv6
6.11 Protocol customization
6.12 Management control functions
6.13 Identification
6.14 Administrator Management
6.15 Security Audit
6.16 Event data security
6.17 Communication security
6.18 Self-monitoring
7 Performance requirements
7.1 Throughput
7.2 Delay
7.3 Data transmission reliability
7.4 Number of nodes that can be protected

8 Security requirements

8.1 Development

8.2 Guidance documents

8.3 Life cycle support

8.4 Testing

8.5 Vulnerability assessment

9 Requirements for different security levels

9.1 Safety function requirements

9.2 Performance requirements

9.3 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.

1 Scope

This standard specifies the security function requirements, performance requirements, and security requirements of industrial control system border security dedicated gateway products.

This standard applies to the design, development, and testing of industrial control system border security dedicated gateway 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 criteria Part 3. Security assurance components GB/T 25069-2010

Information Security Technology Terminology

3 Terms and definitions

GB/T 18336.3-2015 and GB/T 25069-2010 and the following terms and definitions apply to this document.

Gateway

Between networks or subnets, and between software application systems in different security domains, one designed to protect according to a given security policy the connection point of the network.

4 Acronyms

The following abbreviations apply to this document.

DCS. Distributed Control System IP. Internet Protocol OSI. Open System Interconnection
PLC. Programmable Logic Controller SCADA. Supervisory Control And Data Acquisition

5.1 Classification of safety technical requirements

This standard divides the security technical requirements of the dedicated security gateway products for industrial control systems into three major functions. security functions, performance, and security assurance.

class. Among them, the security function requirements are specific requirements for the security functions that industrial control system border security dedicated gateway products should have. For example, such as. white list-based policy-based access control, function protection, attack response processing, time proofreading, business auditing, and industrial control protocols Support, suitable for multiple field environments, time synchronization, dual-system hot backup, support for IPv6/IPv4, protocol customization, management control function, physical Authentication, administrator management, security audit, event data security, communication security, self-monitoring, etc .; performance is the boundary of industrial control systems the performance of the security dedicated gateway product puts forward specific requirements, such as throughput, delay, reliability of data transmission, number of nodes that can be protected, etc .; security the assurance requirements put forward specific requirements for the content of the development and use documents of the dedicated security gateway products for industrial control systems, such as the development of Development, instructional documentation, lifecycle support and testing.

5.2 Classification of security levels

The security level of the industrial control system border security dedicated gateway product is based on its security function requirements, performance requirements, and

security assurance requirements.

The strength is divided into basic level and enhanced level, in which security requirements refer to GB/T 18336.3-2015.

6.1 Whitelist-based access control

Products should support access control based on whitelist policies, including network layer and application layer.

6.2 Control function protection

The product shall provide protection for the protected industrial control system and equipment with control functions, block abnormal operations, and ensure the stability of normal operations.

run.

6.3 Attack response processing

When the product may be attacked, it can automatically record the IP address of the attacker and the time of the attack. Product safety features should.

- a) Generate real-time alarm information;
- b) Block the re-access of the IP address that initiated the attack.

6.4 Time proofreading

Products should provide a reliable time proofing mechanism for their own applications.

6.5 Business Audit

The product should have the function of auditing business events. The auditing content includes protocol inspection, filtering, exchange, blocking, etc., including normal Operation and abnormal operation. Each audit log should include at least the date, time, source IP, destination IP, protocol, and event description of the event.

Remarks and results.

6.6 Industrial Control Protocol Support

The product shall have the functions of inspection, filtering, exchange, blocking, etc. of the proprietary protocols of industrial control and data in various states or instructions in mainstream formats, the number of supported agreements is as follows.

- a) Basic level supports at least 2 industrial control protocols;