

ICS 35.240
CCS A 90

GA

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

GA/T 1559-2019

**Information security technology - Security technical
requirements for industrial control system software
vulnerability scanners**

信息安全技术 工业控制系统软件脆弱性扫描产品安全技术要求
(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 Acronyms
- 5 General description
 - 5.1 Classification of safety technical requirements
 - 5.2 Classification of Security Levels.
- 6 Safety function requirements
 - 6.1 Information acquisition
 - 6.2 Vulnerability scan content
 - 6.3 Scanning result analysis and processing
 - 6.4 Scan configuration
 - 6.5 Target object security
 - 6.6 Upgrade capability
 - 6.7 Scanning IP Address Restrictions
 - 6.8 Self-safety requirements
- 7 Security requirements
 - 7.1 Development
 - 7.2 Guidance documents
 - 7.3 Life cycle support
 - 7.4 Testing
 - 7.5 Vulnerability assessment
- 8 Requirements for different security levels
 - 8.1 Safety function requirements
 - 8.2 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, security assurance requirements, and classification requirements for industrial control system software vulnerability scanning products.

This standard applies to the design, development, and testing of industrial control system software vulnerability scanning 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 30976.1-2014 Information security of industrial control systems-Part 1. Evaluation specifications

3 Terms and definitions

GB/T 25069-2010 and GB/T 30976.1-2014 and the following terms and definitions apply to this document.

Industrial control system software A collection of upper computer software and lower computer software for industrial control systems.

Vulnerability

Defects or weaknesses in system design, implementation, or operation and management can be exploited to compromise system integrity or security policies.

Flag banner

A piece of information sent by an application, usually including a welcome message, application name, and version.

4 Acronyms

The following abbreviations apply to this document.

DCS. Distributed Control System HMI. Human Machine Interface 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 industrial control system software vulnerability scanning products into security functions and security assurance requirements. Of which, An Full-featured requirements are specific requirements for the security functions that industrial control system software vulnerability scanning products should possess.

Identification and identification to limit the use of product functions and control of data access, so that the product has the ability of independent security protection, and ensure industrial control the normal operation of the system software vulnerability scanning product and the requirements of the audit function make the administrator's various operating behaviors and scanning events all Traceable. Security assurance requirements put forward specific requirements for the content of the development and use documents of industrial control system software vulnerability scanning products Requirements, such as development, testing, and instructional documentation.

5.2 Classification of security levels

The security level of industrial control system software vulnerability scanning products is divided into according to the strength of its safety function requirements and safety assurance requirements.

Basic level and enhanced level, in which security requirements refer to GB/T 18336.3-2015.

6.1.1 Support system information

It should be able to detect the operating system type and version number of the supporting platform on which the industrial control system software is located, and be able to obtain the opened items.

Flag for TCP/IP services.

6.1.2 Open Port

It should be able to detect the TCP and UDP ports open by the operating system where the industrial control system software is located, and be able to determine the general port corresponding to the corresponding port.

Service or Use Agreement

6.1.3 Protocol support

Should support typical industrial control protocols, such as MODBUS TCP, OPC, Siemens S7, IEC 60870-5-104, IEC 61850, etc.

6.2.1 Vulnerability Discovery

It should be possible to discover the security vulnerability issues of open industrial control system software.

6.2.2 Vulnerability mining

It should be possible to discover the security vulnerability of unknown industrial control system software.

6.2.3 Weak passwords

It should be able to check the robustness of system user passwords using dictionaries or exhaustive methods. The check items should include.

- a) Whether the system uses a simple converted password for the user name;
- b) Whether the system uses easy-to-guess passwords.

6.2.4 File sharing

It should be able to check the file sharing mechanism and find dangerous settings. The inspection items should include.

- a) important directories are shared;
- b) the shared directory can be written by anonymous users;
- c) Whether a default or overly simple shared password was used.

6.3.1 Scanning Results Export and Export

Scanning result browsing function shall be provided, and export operation of scanning result data shall be supported.

6.3.2 Report generation

Can generate corresponding reports based on the scan results. The report requirements include the following.

- a) Vulnerability name, vulnerability description, scope of influence, etc. of each vulnerability;