CCS N 10

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 40218-2021

Industrial communication networks - Network and system security - Security technologies for industrial automation and control system

Issued on: May 21, 2021 **Implemented on: December 1, 2021**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

Foreword

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

The translation method used in this standard is equivalent to IEC /T R62443-3-1.2009 "Industrial Communication Network Network and System Security No. 3-1

Part. Information Security Technology of Industrial Automation and Control System.

This standard has made the following editorial changes.

---Modified the standard name;

---Delete footnotes that are inconsistent with our country's situation.

This standard was proposed by the China Machinery Industry Federation.

This standard is under the jurisdiction of the National Industrial Process Measurement Control and Automation Standardization Technical Committee (SAC/TC124).

Drafting organizations of this standard. Institute of Comprehensive Technology and Economics of Machinery Industry Instrumentation, Central Electric Power Planning Institute Co., Ltd., China Nuclear Power Engineering

Co., Ltd., Hollysys Technology Group Co., Ltd., Beijing Water Supply Group Co., Ltd., Zhejiang University, Huazhong University of Science and Technology, Chongqing

University of Posts and Telecommunications, Computer and Microelectronics Development Research Center of the Ministry of Industry and Information Technology (China Software Evaluation Center), Siemens (China) Co., Ltd.

Division, Schneider Electric (China) Co., Ltd., Rockwell Automation (China) Co., Ltd., Shenyang Institute of Automation, Chinese Academy of Sciences, Beijing

Venus Star Information Security Technology Co., Ltd., Beijing Guodian Zhishen Control Technology Co., Ltd., Shenzhen Wanxun Automation Control Co., Ltd., China

The 30th Research Institute of Electronic Technology Group Corporation, the Fifth Research Institute of Electronics of the Ministry of Industry and Information Technology, Southwest University, China Dongfang Electric Group Co., Ltd.

Company, Beijing Sifang Relay Automation Co., Ltd., National Industrial Information Security Development Research Center, Beijing Rail Transit Design and Research

Institute Co., Ltd., Shanghai Automation Instrumentation Co., Ltd., Chongqing Xin'an Network Security Rating and Evaluation Co., Ltd., the Third Research Institute of the Ministry of Public Security, China

Network Security Review Technology and Certification Center, Beijing Wangyu Nebula Information Technology Co., Ltd.

Introduction

The need to protect the computer environment of industrial automation and control systems (IACS) from malicious code has increased over the past decade.

Having attention. More and more open systems, platforms and protocols are used in the IACS environment. With the increase in joint foreign investment activities, foreign

The combination of ministry partners and external resources will bring more threats and more advanced computer attacks. With these threats and vulnerabilities

The increase in the number of industrial communication networks will increase the risk of computer attacks on industrial communication networks. Therefore, there is a need for computer and network-based information sharing.

And the analysis center also needs to be protected. In addition, with the development of smart devices and embedded systems, the interconnection of computers, network devices, and software has increased.

Plus, enhanced external connections and the rapid growth of network intrusion incidents, more intelligent attackers and malicious and highly accessible software, all

These all increase risks.

Many electronic security technologies and computer intrusion prevention measures may be applicable to the IACS environment. This standard lists several types of computers

Information security technology and precautions, and discuss the vulnerabilities dealt with, deployment recommendations, and known strengths and weaknesses for each category.

point. In addition, it also provides guidelines for the use of various security technologies and preventive technologies to be taken against the risks mentioned above.

This standard does not compare the above-mentioned safety technologies and preventive measures, but only provides suggestions and guidelines for the use of these technologies and methods, and

Information to be considered in the development of on-site or enterprise-level information security policies, procedures, and procedures related to the IACS environment.

The working group will periodically update the technical requirements to reflect new information, computer security technology, countermeasures and computer risk reduction methods.

law. At the same time, readers are warned that when using the recommended guidelines in the standard, they do not ensure that their industrial automation or control system environment achieves the best design.

Computer security status. However, this standard helps to identify and deal with vulnerabilities and reduce unexpected network intrusions. These network intrusions may

Stealing confidential information, even causing harm to personnel and the environment, or leading to industrial networks, control systems, and industries and infrastructure for monitoring and management

The key assets of the facility are damaged or become invalid.

This standard provides the evaluation and assessment of many types of current electronic computer security technologies, mitigation measures and tools, which are used to protect

Protect the IACS environment to prevent unfavorable computer intrusions and attacks. This standard introduces various technologies, methods and tools, and provides

Discussion of content development, implementation, operation, maintenance, project implementation/management and other services. This standard also provides

Information security practitioners, facilities, and factories for business and end users to protect automation in terms of technology selection and countermeasures

The IACS (and its related industrial networks) are protected from electronic (computer) attacks.

The guidelines given in this standard cannot ensure that IACS has achieved the best computer information security. However, these guidelines help

Identify and point out vulnerabilities, and can reduce the risk of unexpected intrusion to prevent the leakage of confidential information or cause the control system and its automatic

Damage or failure of key assets under control. More concerned, when a computer leak occurs in the automation control system or its related industrial network,

The use of these guidelines can help reduce the risk of damage to any personnel or the environment.

The cybersecurity guidelines in this standard are general/general, depending on the application of personnel knowledge in industrial automation systems/and should

According to the applicable and specific industrial automation system personnel knowledge,

it is correctly applied to every control system and network. This guide identifies the

In terms of providing network security control systems, typical and important activities. However, the above activities are not always related to the effectiveness of system functions.

Compatible with operation or maintenance. The guidelines include applicable information security recommendations and recommendations for specific control systems. However, the selection and ministry

It is the responsibility of the system owner to assign information security activities and practices specific to a given control system and its related industrial network.

With the acquisition of control system vulnerability experience, the maturity of specific network information security implementation and the new control-based network information security

This standard will gradually be revised and improved for the use of all technologies. In this way, while the main structure of this standard remains relatively stable, its application and

The solution will also be gradually improved.

Industrial communication network network and system security

Industrial Automation and Control System Information Security Technology

1 Scope

This standard provides an assessment of various current network information security tools, mitigation countermeasures and technologies. These techniques can be used effectively

In IACS based on modern electronics, a large number of industries and critical infrastructures can be adjusted and monitored. This standard describes several types

The control system-centric network information security technology, the product categories available in these categories, the use of this in an automated IACS environment

The pros and cons of these products, relative to the expected threats and known network vulnerabilities, and more importantly, the use of these network information security technologies

Preliminary recommendations and guidelines for products and/or countermeasures.

The IACS cyber security concept applied by this standard is to cover the components, factories, and equipment in all industries and critical infrastructure to the greatest extent possible.

Implementation and system. IACS includes but is not limited to.

* Hardware (such as historical data server) and software systems (such as operating