CCS N 10

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 40211-2021

Industrial communication networks - Network and system security - Terminology, concepts and models

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 S62443-1-1.2009 "Industrial Communication Network Network and System Security Part 1-1

Sub. Terminology, Concept and Model.

The Chinese documents that have a consistent correspondence relationship with the normatively cited international documents in this standard are as follows.

---GB/T 18336.1-2015 Information Technology Security Technology Information Technology Security Assessment Criteria Part 1.Introduction and One

General model (ISO /IEC 15408-1.2009, IDT)

---GB/T 20720.1-2019 Enterprise Control System Integration Part 1.Model and Terminology (IEC 62264-1.2013, IDT)

This standard has made the following editorial changes.

---Modified the standard name.

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 subject of this standard is the safety of industrial automation and control systems. In order to be applicable to different applications (e.g. industry types), each term

Both have a broad interpretation.

The term "industrial automation and control system" (IACS) includes control systems used in manufacturing and process industries, building control systems,

Geographically dispersed operations such as public facilities (e.g. electricity, natural gas and water supply), pipelines and oil production and distribution facilities, other industries and

Applications such as transportation networks, those that use automated or remotely controlled or monitored assets.

The term "safety" in this standard refers to the prevention of illegal or harmful infiltration, intentional or unintentional obstruction of normal and expected operation, or failure to

Appropriate access to the confidential information of IACS. Computer security that this standard pays special attention to, including computers, networks, operating systems, applications and systems

Other programmable components of the system.

The readers of this standard include all IACS users (including part of the facility operation, maintenance, construction and user organization), production

Affected, control system computer security, control system practitioners, and security

practitioners, including operators, suppliers, and government organizations. Because of the letter

Mutual understanding and cooperation between information technology (IT) and operators, engineering personnel, and manufacturers' organizations are essential for any information initiative to achieve comprehensive

Success is very important. This standard is also a reference for those responsible for IACS and enterprise network integration.

This standard mainly involves the following typical issues.

a) What is the scope of IACS security application?

b) How to use uniform terminology to define the needs and requirements of the safety system?

c) What basic concepts are used as the basis for further analysis of activities, system attributes and actions, which provide electronic security control

Is very important for the control system?

d) How to group or classify IACS components for use in defining and managing security?

e) What are the different safety goals in control system applications?

f) How were these goals established and modified?

Each issue is described in detail in this standard.

Industrial communication network network and system security

Terminology, concepts and models

1.1 Overview

This standard is a technical specification that defines the terms, concepts and models used for industrial automation and control system (IACS) security. It is a series of standards.

The basis of other standards in the standard.

In order to fully and clearly express the systems and components of this standard, the scope of coverage can be defined and understood from several aspects, including.

---The scope of functionality contained;

---Specific systems and interfaces;

---Criteria for selecting the included activities;

---Criteria for the selection of included assets.

The following sections are an introduction to these contents.