

ICS 25.040
CCS N 10



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

GB/T 35673-2017

**Industrial communication networks -- Network and system
security -- System security requirements and security levels
(English Translation)**

Issued on: December 29, 2017

Implemented on: July 1, 2018

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China, Standardization
Administration of the People's Republic of China**

Table of Contents

Foreword
Introduction
0.1 Overview
0.2 Purpose and user of this standard
1 Scope
2 Normative references
3 Terms, definitions, abbreviations and conventions
3.1 Terms and Definitions

Foreword

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

This standard uses the translation method equivalent to the use of IEC 62443-3-3:2013 "Industrial Communication Network Network and System Security Part 3-3.

System Safety Requirements and Safety Levels" and its amendments corrigendum1.

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

---GB/T 33007-2016 Industrial Communication Network Network and System Security Establishing Industrial Automation and Control System Security Process Order (IEC 62443-2-1:2010, IDT) for ease of use, this standard has made the following editorial changes.

--- The standard name was changed to "Safety Requirements and Security Levels for Industrial Communication Network Networks and System Security Systems";

---Incorporating the contents of the Technical Corrigendum 1, the terms covered by these technical errata have passed the vertical double on its outer marginal position Line (||) is marked;

--- Corrected the wrong serial number in 5.7.1.

This standard is proposed by China Machinery Industry Federation.

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

0.1 Overview

Note: This standard is part of the series of standards concerning information security in the Industrial Automation and Control System (IACS). Is the fourth working group of the ISA99 Committee the Task Group 2 was developed in cooperation with IEC TC65/WG10. This standard describes the control system information defined in IEC 62443-1-1 Safety requirements are related to the seven basic requirements and the system of assessment (SuC) is assigned a system safety rating.

Industrial Automation and Control Systems (IACS) organizations increasingly use commercial network equipment products because of their low cost and high performance Effective and highly automated. For commercial purposes, control systems are also increasingly connected to non-IACS networks. These devices use Decentralized network technology and increasing network connectivity provide opportunities for cyber attacks against control system hardware and software. This weakness it can lead to health, safety, and environmental (HSE), financial, or reputational issues with the deployed system.

Organizations deploying commercial information network security solutions to respond to IACS security may not fully understand the adoption of this measure fruit. Although many commercial IT applications and security solutions can be applied to IACS, they need to be applied in a suitable way to avoid Avoid the consequences of negligence. Therefore, it is necessary to combine functional requirements and risk assessment, and usually include awareness of operational issues to define the system.

System requirements.

IACS security measures should not have the potential to cause the loss of basic services and functions (including emergency procedures). (often deployed IT security Measures do have this potential weakness.) IACS safety goals focus on the availability of control systems, plant protection, and plant operations (even if Hierarchical mode) and time-critical system response. IT security goals often have different levels of emphasis on these factors; they Perhaps more concerned with protecting information than tangible assets. Regardless of the degree of implementation of the factory integration, these different goals need to be clearly defined Expressed as a safety goal. According to the requirements of IEC 62443-2-1, a key step in risk assessment is to identify which services and functions are it is essential. (For example, in some facilities, engineering support may be judged as non-essential service or function.) In some cases, safety the actions of the whole nature cause temporary loss of non-essential services or functions is acceptable, but the basic services or functions should not be adversely affected.

influences.

This standard assumes that the system has established and operated a safety program in accordance with IEC 62443-2-1. Further assume that by using this standard the quasi-describing appropriate control system requirements and enhancement requirements

fulfill the patch management as recommended by IEC/T R62443-2-3 [5]. this in addition, IEC 62443-3-2 [8] describes how to define a risk-based safety level (SL) for a project and is used to select and comply with the criteria detailed in this standard.

The appropriate technical security capabilities of the product. The main reference standards of this standard include ISO/IEC 27002 [15] and NIST SP800-53 3 Edition [24] (see Chapter 2 and References).

The main purpose of the IEC 62443 series of standards is to provide a flexible framework to respond to the current and future vulnerability of IACS and to adopt Use a systematic defense approach to implement the necessary mitigation methods. The purpose of the IEC 62443 series of standards is to expand the security of enterprises to adapt them the requirements of business IT systems, combined with IACS' unique high availability requirements.

0.2 Purpose and user of this standard

Users of this standard in the IACS field include asset owners, system integrators, product suppliers, service providers, and compliance management mechanism. Compliance management agencies include government agencies and regulatory authorities that have statutory powers to conduct compliance audits in accordance with laws and regulations.

System integrators, product vendors, and service providers will use this standard to evaluate whether their products and services can provide assets Owner's target security level (SL-T) required security capabilities. For SL-T allocation, the requirements (SR) and enhancements for a single control system the applicability of (RE) will be based on the asset owner's security policy, procedures, and site-specific risk assessment. It is worth noting that some Some SRs have certain conditions that allow exceptions, such as when satisfying the SR will violate the basic operating requirements of the control system (this may need to increase Compensation countermeasures).

When designing a control system to satisfy a specific SL-T related series of SRs, it is not necessary that every component of the control system meets this each system requirement for the standard mandatory level. Compensation countermeasures can be used to provide the functions required by other subsystems, at the control system level, full the Department's SL-T requirements have been met. At the design stage, consideration should be given to the inclusion of compensation measures with detailed documentation so that the achieved control Systems SL and SL-A (control systems) fully embody the design expectations of security capabilities. Similarly, in order to meet the SL of the entire control system, During the certification test and/or post-installation audit, compensation measures can be applied and documented.

This standard does not provide details on the design and establishment of an integrated security architecture. This requires additional system-level analysis and the IEC 62443

series the other criteria (see 0) derived requirements. It should be noted that the goal of this standard is not to provide detailed specifications to establish a safety rack Structure. The objective of this standard is to define a generic minimum requirement and gradually achieve a more stringent level of information security. Meet these requirements the actual design of the architecture is the work of system integrators and product suppliers. In this work, they are free to choose to support competition and Innovation. Therefore, this standard only strictly defines the functional requirements and does not involve how these functional requirements should be met.

0.3 The application of this standard in the IEC 62443 series of standards

Figure 1 shows the composition of the IEC 62443 series of standards at the time of writing this standard.

IEC 62443-3-2 uses SR and RE as a checklist. In the system to be evaluated (SuC) using regional and pipeline terminology Description, as well as the corresponding target SL assigned to these areas and pipelines, the SR and RE defined in this standard, and their security capabilities the mapping of level SL (SL-C) is compiled into a list of requirements that control system design needs to meet. A given control system design SL-A can be used as a condition to perform an integrity check.

Figure 1 Structure of the IEC 62443 series of standards

IEC/T S62443-1-3 [2] uses the mapping of basic requirements (FR), SR, RE and SL-C as a checklist to test the specification of quantitative indicators.

Integrity. Quantified safety compliance indicators are based on specific contexts. In combination with IEC 62443-3-2, the task of the asset owner's SL-T Requires conversion to quantitative indicators to support system analysis and design trade-off research, and to develop security architectures.

IEC 62443-4-1 [9] proposes general requirements in the product development process. For example, the contents of IEC 62443-4-1 are all around the product supplier. Product safety requirements are derived from the list of baseline requirements and REs specified in this standard. When developing the features of these products, Use the IEC 62443-4-1 quality specification.

IEC 62443-4-2 [10] contains a series of derived requirements that provide a detailed mapping of this standard SR to subsystems and SuC components. in at the time of writing of this standard, the component categories covered by IEC 62443-4-2 are. embedded devices, host devices, network devices and applications.

sequence. Similarly, IEC 62443-4-2 focuses on suppliers (product suppliers and service providers). Product safety requirements, first from the basic requirements and RE list specified in this standard. The safety requirements and metrics of IEC 62443-3-2 and IEC/T S62443-1-3 were Used to perfect these normative derivative requirements.