

ICS 25.040.40

CCS N 10



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

GB/T 33007-2016

**Industrial communication networks -- Network and system
security -- Establishing an industrial automation and control
system security program**

工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序

(English Translation)

Issued on: October 13, 2016

Implemented on: May 1, 2017

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

Table of Contents

- Preface
- Introduction
- 1 Scope
- 2 Normative reference document
- 3 Terms and definitions, acronyms and conventions
 - 3.1 Terms and definitions
 - 3.2 Abbreviations and Abbreviations
 - 3.3 Conventions
- 4 Elements of network security management system
 - 4.1 Overview
 - 4.2 Category. Risk analysis
 - Category. Use CSMS to handle risk
 - 4.4 Category. CSMS Monitoring and Improvement
- Appendix A (Normative Appendix) CSMS Element Development Guide
 - A.1 Overview
 - A.2 Category. Risk analysis
 - A.3 Category. Resolving risk with SCSMS
 - A.4 Classification. Monitoring and enhancing CSMS
- Appendix B (informative) Procedure for developing CSMS
 - B.1 Overview
 - B.2 Description of the process
 - B.3 Activity. Initialize CSMS project
 - B.4 Activities. Advanced risk assessment
 - B.5 Description of the process

Foreword

This standard is in accordance with GB/T 1.1-2009 "Standardized working guidelines Part 1. Standard structure and preparation" and GB/T 20000.2-2009 "Standardization Work Guide Part 2. Adoption of International Standards".

This standard uses the translation method equivalent to IEC 62443-2-1.:2010 "Industrial communication network and system security Part 2-1.

Establishment of Industrial Automation and Control System Safety Procedures "(English version). Its technical content, text structure and expression form IEC 62443-2-1.:2010 is fully equivalent.

For ease of use, this standard has been modified as follows.

--- deleted the original words in the original;

- will introduce the contents of the part as the introduction of this standard;

--- If you do not explain, the text of the "security" refers to "network security." this standard is proposed by the China Machinery Industry Federation.

This standard by the National Industrial Process Measurement Control and Automation Standardization Technical Committee (SAC/TC124) and the national information security standards Technical Committee (SAC/TC260).

The drafting unit of this standard. Institute of Mechanical and Industrial Instrumentation Integrated Technology and Economy, China Electronics Technology Standardization Research Institute, China Power Scientific Research Institute, China Nuclear Power Engineering Co., Ltd., Shanghai Automation Instrumentation Co., Ltd., Beijing Jiaotong University, Eastern Science and Technology Co., Ltd.

Company, Tsinghua University, Siemens (China) Co., Ltd., Zhejiang University, Southwest University, Chongqing University of Posts and Telecommunications, Schneider Electric (China) Co., Ltd.

Division, Beijing Iron and Steel Design and Research Institute, Huazhong University of Science and Technology, Beijing Austin Technology Co., Ltd., Rockwell Automation (China) Co., Ltd.

Division, China Institute of Instrumentation, Beijing and Lee Department of Systems Engineering Co., Ltd., Ministry of Industry and Information Technology Institute of Electronics Fifth, the Chinese Academy of Sciences Shen Yang Automation Institute, Beijing Haitai radius of Science and Technology Co., Ltd., Qingdao Duo Fenuo Information Security Technology Co., Ltd., Beijing Guodian Zhi deep control Technology Co., Ltd., Beijing Power Control Huakang Technology Co., Ltd., Guangdong Aerospace Satellite Technology Co., Ltd., North China Electric Power Design Institute Engineering Co., Ltd.

Division, Huawei Technologies Co., Ltd., Venus, China Electronics Technology Group Corporation 30th Institute, Shenzhen million-controlled Co., Ltd., Winning Software Co., Ltd., Yokogawa Electric (China) Co., Ltd. Beijing R & D Center.

0.1 Overview

Network security is an increasingly important topic in modern organizations. Over the years, many organizations involved in information technology and business have been Attention to

network security, and in accordance with the ISO and IEC standards have been established an effective network security management system (CSMS) (see ISO/IEC 17799 [23] 1 and ISO/IEC 27001 [24]), these management systems provide an effective way for the organization to protect their assets from cyber attacks.

The Industrial Automation Control System (IACS) organization has begun to use commercially available off-the-shelf technology for business systems in its daily processes (COTS), which makes the IACS equipment by the possibility of network attacks increased. Due to various reasons, in the fight against the network attack side these systems are usually less robust than those designed for the IACS environment. These weaknesses can lead to health, safety and environmental aspects (HSE) consequences.

Without understanding these consequences, the organization may attempt to use existing information technology and business security solutions to address IACS security issues. Although many solutions can be applied to IACS, but need to take the right way to eliminate the adverse consequences.

0.2 IACS network security management system

The management system usually provides guidance on what should be included in the management system, but does not provide guidance on how to develop the management system. this the standard describes the elements contained in the CSMS of IACS, and also provides guidance on how to develop CSMS for IACS.

In the face of a challenging problem, a very common engineering approach is to break down the problem into smaller sub-problems, Way to solve each sub-problem. This is a reasonable way to solve the IACS network security risk. However, in the settlement of network security often committed the mistake is to try to solve all the network security problems with a system at once. Network security is a bigger challenge that needs to be considered throughout IACS and policies, procedures, practices and personnel that surround and utilize IACS. Implementing such a wide range of management systems may be required within the organization Department of cultural change.

It is a daunting task to solve network security on the basis of the whole organization. But for security, there is no ready solution Program. It is easy to understand because there is no safe practice for all situations. In theory, absolute security may be possible, but it is possible can not be desirable, because to achieve such a near-perfect state is bound to lose practicality. Security is actually a risk and cost balance. All the situation is different. In some cases, the risk may be related to the HSE factor rather than the mere economic impact. wind Risk may bring irreversible consequences rather than temporary financial setbacks. So a set of mandatory safety practices is either a solution in strict, expensive to follow, or not enough to deal with the risk.

The relationship between this standard and ISO/IEC 17799 and ISO/IEC 27001 ISO/IEC

17799 [23] and ISO/IEC 27001 [24] are excellent descriptions of network security management systems for business/information technology systems standard. Most of the contents of these standards also apply to IACS. This standard emphasizes the management and business/information of IACS network security practices. There is a need for consistency between the management of technical systems for network security. Consistency of these procedures can save money. The standard encourages users to read ISO/IEC 17799 and ISO/IEC 27001 for additional support information. This standard is based on these ISO/IEC standards IACS and general business/information technology systems. This standard introduces an important concept that IACS's network security risks can be can bring HSE impact, should be combined with other existing risk management practices to deal with these risks.

Industrial communication network and system security Establish industrial automation and control System security program

1 Scope

This standard specifies how to establish a network security management system in the Industrial Automation and Control System (IACS) and provide information on how to develop A guide to these elements. This standard has a broader definition and scope than the IACS described in IEC 62443-1-1.

The elements of the CSMS described in this standard are primarily policies, procedures,, and personnel-related elements that describe the elements What the final CSMS will include or should include.

Note 1: Other documents in the IEC 62443 series of standards and references discuss more detailed and specific techniques and protocols for safety.

How to develop CSMS guidance is an example, it represents the author's point of view. an organization can go to develop elements, but it may not be able to Apply in all cases. In order to develop a complete set of functional CSMS for the organization, the user of this standard must carefully read the requirements and Proper use of guidance. The strategies and procedures discussed in this standard should be tailored to the needs of the organization.

Note 2: There may be a situation where the enterprise already has its own CSMS and added IACS, or has not formally established CSMS. The author can not IACS establishes a CSMS organization to predict all situations, so this standard does not attempt to provide a solution for all situations.

2 Normative reference documents

The following documents are indispensable for the application of this document. For dated references, only the dated edition applies to this article Pieces. For undated references, the latest edition (including all modifications) applies to this document.