

ICS 35.040
CCS L 80

GA

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

GA/T 1390.5-2017

**Information security technology--General requirements for
classified protection of cyber security--Part 5: Special security
requirements for industrial control system**

信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求
(English Translation)

Issued on: May 8, 2017

Implemented on: May 8, 2017

Issued by: Ministry of Public Security

Table of Contents

Preface	
Introduction	
1 Scope	
2 Normative references	
3 Terms, definitions and abbreviations	
3.1 Terms and Definitions	
3.2 Abbreviations	
4 Overview	
4.1 General requirements for safety	
4.2 Overview of Industrial Control Systems Summary	
4.2.1 General	
4.2.2 Hierarchical Model	
4.2.3 Regional Model	
4.2.4 Security Domain Division Principle	
4.3 Industrial Control System Level Protection Principles and Requirements	
4.3.1 General	
4.3.2 Security Domain Protection Principles	
4.3.3 Implementation Instructions for the Protection of the Security Domain	
4.3.4 Technical Requirements and Management Requirements	
4.4 Industrial Control System Rating	
4.5 Industrial Control System Level Protection General Constraints	
4.5.1 Overview	
4.5.2 Basic Function Support	
4.5.3 Compensation measures	
5 The first level of basic requirements	
5.1 Technical Requirements	
5.1.1 Physical Security	
5.1.2 Border Protection	
5.1.3 Production Management Security Requirements	
5.1.4 Process Monitoring Layer Security Requirements	
5.1.5 Field Control Layer Security Requirements	
5.1.6 Field Device Layer Security Requirements	

- 5.2 Management Requirements
 - 5.2.1 Safety Management Organizations and Personnel
 - 5.2.2 Security Operations Maintenance Vulnerability and Risk Management
- 6 Second-level basic requirements
 - 6.1 Technical Requirements
 - 6.1.1 Physical and Environmental Security
 - 6.1.2 Border Protection
 - 6.1.3 Safety Requirements for Production Management
 - 6.1.4 Process Monitoring Layer Security Requirements
 - 6.1.5 Field Control Layer Security Requirements
 - 6.1.6 Field Device Layer Security Requirements
 - 6.2 Management Requirements
 - 6.2.1 Safety Management Organizations and Personnel
 - 6.2.2 Security Operations Management Vulnerability and Risk Management
- 7 Level 3 Basic Requirements
 - 7.1 Technical Requirements
 - 7.1.1 Physical and Environmental Security
 - 7.1.2 Border Protection
 - 7.1.3 Centralized Control
 - 7.1.4 Production Management Security Requirements
 - 7.1.5 Process Monitoring Layer Security Requirements
 - 7.1.6 Field Control Layer Security Requirements
 - 7.1.7 Field Device Layer Security Requirements
 - 7.2 Management Requirements
 - 7.2.1 Security Policy and Management System
 - 7.2.2 Security Administration and Staff
 - 7.2.3 Security Construction Management Outsourcing Software Development
 - 7.2.4 Security Operations Maintenance Vulnerability and Risk Management
- 8 Level 4 Basic Requirements
 - 8.1 Technical Requirements
 - 8.1.1 Physical and Environmental Security
 - 8.1.2 Border Protection
 - 8.1.3 Centralized Control
 - 8.1.4 Safety Requirements for Production Management
 - 8.1.5 Process Monitoring Layer Security Requirements

8.1.6 Field Control Layer Security Requirements

8.1.7 Field Device Layer Security Requirements

8.2 Management Requirements

8.2.1 Security Policy and Management System Security Policy

8.2.2 Security Administration and Staff

8.2.3 Security Management Construction Outsource Software Development

8.2.4 Security Operations Maintenance Vulnerability and Risk Management

Appendix A (Informative) Industrial Control System Overview

Appendix B (Informative) Examples of Security Domain Division

Appendix C (Informative) Protection of Industrial Control System Security Levels Based on Trusted Computing Technology

References

Foreword

GA/T 1390 "Basic Requirements for Information Security Technology Network Security Level Protection" has or plans to issue the following parts.

- Part 1. General requirements for safety;
- Part 2. Cloud computing security extension requirements;
- Part 3. Mobile Internet Security Extension Requirements;
- Part 4. IoT Security Extension Requirements;
- Part 5. Industrial Control System Security Extension Requirements;
- Part 6. Big Data Security Extension Requirements.

This section is Part 5 of GA/T 1390.

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

This part is proposed and managed by the Information Systems Security Standardization Technical Committee of the Ministry of Public Security.

This section is responsible for drafting. Zhejiang University, Zhejiang Institute of Control Research Co., Ltd.

The Institute of Public Security, Third Institute, Hangzhou College of Science and Technology, Beijing Qixing Chen Information Security Technology Co., Ltd.

This section participated in the drafting unit. China Electric Power Engineering Consulting Group Southwest Electric Power Design Institute Co., Ltd., Beijing Guodian Zhishen Control

Technology Co., Ltd.

Limited Company, Siemens (China) Co., Ltd., Schneider Electric (China) Co., Ltd., the Fifth Institute of Electronics, Ministry of Industry and Information Technology, and Beijing Li Shi System Engineering Corporation, Dongfang Electric Central Research Institute, Beijing Rail Transit Design & Research Institute Co., Ltd., National Information Technology Security Research Institute Center, China Software Evaluation Center, Sinopec Qilu Petrochemical Company, Shenyang Institute of Automation, Chinese Academy of Sciences, China Electronics Technology Group Corporation No.30 Research Institute, State Power Investment Corporation, China Electric Power Engineering Consulting Group, North China Electric Power Design Institute Co., Ltd., National Nuclear Automation System Project Ltd., Beijing Water Group.

Introduction

In order to adapt to new technologies and new applications such as mobile internet, cloud computing, big data, internet of things and industrial control, information security level protection to carry out work, it is necessary to revise GB/T 22239-2008. The revised ideas and methods are for mobile internet, cloud computing, big data, New technologies and new application areas such as the Internet of Things and industrial control propose expanded security requirements.

Information Security Technology Network Security Level Protection Basics Requirements
Section 5. Industrial Control System Security Extension requirements

1 Scope

This part of GA/T 1390 specifies the safety extension requirements for industrial control systems with different levels of safety protection.

This section applies to batch control, continuous control, discrete control and other industrial control systems, for industrial control system network security level protection Provide guidance on the design, implementation, testing and evaluation of measures.

2 Normative references

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

GB 17859-1999 Guidelines for the classification of security levels for computer information systems
GB/T 22239 Information Security Technology Information System Security Level Protection Basic Requirements
GB/T 25069-2010 Information Security Technical Terms
IEC 62443-1-1 Industrial communication network networks and system security. Part 1-1. Terms,