



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

GB/T 42457-2023

**Security for industrial automation and control systems - Secure
product development lifecycle requirements**

Issued on: March 17, 2023

Implemented on: October 1, 2023

Issued by: SAMR; SAC

Table of Contents

Foreword...	4
Introduction...	5
1 Scope...	8
2 Normative References...	8
3 Terms, Definitions, Abbreviated Terms, Acronyms and Conventions...	8
3.1 Terms and Definitions...	9
3.2 Abbreviated Terms and Acronyms...	15
3.3 Conventions...	16
4 General Principles...	17
4.1 Concepts...	17
4.2 Maturity Model...	18
5 Practice 1 - Security Management...	20
5.1 Purpose...	20
5.2 SM-1.Development Process...	20
5.3 Rationale and Supplemental Guidance...	21
5.4 SM-2.Identification of Responsibilities...	21
5.5 SM-3.Identification of Applicability...	22
5.6 SM-4.Security Expertise...	22
5.7 SM-5.Process Scoping...	23
5.8 SM-6.File Integrity...	23
5.9 SM-7.Development Environment Security...	23
5.10 SM-8.Controls for Private Keys...	24
5.11 SM-9.Security Requirements for Externally Provided Components...	24
5.12 SM-10.Custom Developed Components from Third-party Suppliers...	25
5.13 SM-11.Assessing and Addressing Security-related Issues...	26
5.14 SM-12.Process Verification...	26
5.15 SM-13.Continuous Improvement...	27
6 Practice 2 - Specification of Security Requirements...	28
6.1 Purpose...	28
6.2 SR-1.Product Security Context...	28
6.3 SR-2.Threat Model...	29
6.4 SR-3.Product Security Requirements...	30

6.5 SR-4.Product Security Requirements Content...	31
6.6 SR-5.Security Requirements Review...	31
7 Practice 3 - Secure by Design...	32
7.1 Purpose...	32
7.2 SD-1.Secure Design Principles...	32
7.3 SD-2.Defense In-depth Design...	34
7.4 SD-3.Security Design Review...	35
7.5 SD-4.Secure Design Best Practices...	36
8 Practice 4 - Secure Implementation...	37
8.1 Purpose...	37

Foreword

This document was drafted in accordance with the rules provided in GB/T 1.1-2020 Directives

for Standardization - Part 1.Rules for the Structure and Drafting of Standardizing Documents.

This document identically adopts IEC 62443-4-1.2018 Security for Industrial Automation and

Control Systems - Part 4-1.Secure Product Development Lifecycle Requirements.

This document makes the following minimal editorial modification.

---In order to coordinate with the existing standards, the title of the Standard is modified into Security for Industrial Automation and Control Systems - Secure Product Development Lifecycle Requirements.

This document was proposed by China Machinery Industry Federation.

This document shall be under the jurisdiction of National Technical Committee 124 on Industrial Process Measurement, Control and Automation of Standardization Administration of

China (SAC/TC 124).

The drafting organizations of this document. Beijing Winicssec Technologies Co., Ltd.; Instrumentation Technology and Economy Institute; Electric Power Planning & Engineering Institute; Schneider Electric (China) Co., Ltd.; SIEMENS (China) Co., Ltd.; Beijing Sifang

Automation Co., Ltd.; Beijing CHN Energy Zhishen Control Technologies Co., Ltd.; North China Electric Power University; Chongqing Xin'an Network Security Classified Testing and Evaluation Co., Ltd.; Chongqing University of Posts and Telecommunications; Southwest University; Huazhong University of Science & Technology; The 30th Research Institute of China Electronics Technology Group Corporation; China Techenergy Co., Ltd.; Liaoning Datang International New Energy Co., Ltd.; Maintenance Branch of State Grid Liaoning Electric Power Supply Co., Ltd.; CRRC Zhuzhou, Locomotive Co., Ltd.; Southwest Jiaotong University Richsun Technologies Co., Ltd.; Traffic Control Technology Co., Ltd.; Hangzhou Dianzi University; China First Automobile Group Co., Ltd.; Xi'an Thermal Power Research Institute Co., Ltd.; Shanghai Institute of Process Automation & Instrumentation; The Fifth Research Institute of Electronics, Ministry of Industry and Information Technology; China Industrial Control Systems Cyber Emergency Response Team; Rockwell Automation (Shanghai) Co., Ltd.; Shanghai Electrical Apparatus Research Institute (Group) Co., Ltd.; HollySys Technology Group Co., Ltd.; Xi'an Space Radio Technology Research Institute.

1 Scope

This document specifies process requirements for the secure development of products used in

industrial automation and control systems. It defines a secure development lifecycle (SDL) for

the purpose of developing and maintaining secure products. This lifecycle includes security requirements definition, secure design, secure implementation (including coding guidelines),

verification and validation, defect management, patch management and product end-of-life.

These requirements can be applied to new or existing processes for developing, maintaining

and retiring hardware, software or firmware for new or existing products. These requirements

apply to the developer and maintainer of the product, but not to the integrator or user of the product. A summary list of the requirements in this document can be found in Appendix B.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of dated references, only the version with

the specified date applies to this document. In terms of references without a specified date, the

latest version (including all the modifications) is applicable to this document.

IEC 62443-2-4 Security for Industrial Automation and Control Systems - Part 2-4. Security Program Requirements for IACS Service Providers

NOTE. GB/T 40682-2021 Security for Industrial Automation and Control System - Security Program

Requirements for IACS Service Providers (IEC 62443-2-4.2015, IDT)

IEC TR 62443-1-2 Security for Industrial Automation and Control Systems - Part 1-2. Master Glossary of Terms and Abbreviations

3 Terms, Definitions, Abbreviated Terms, Acronyms and

Conventions

The terminology databases for ISO and IEC can be accessed at the following URLs.

.....