

ICS 25.040

CCS N 10



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

**GB/T 46933.1-2025**

---

**Safety and security integration of smart factories - Part 1:  
General requirements**

智能工厂安全一体化 第1部分：一般要求

**Issued on: December 31, 2025**

**Implemented on: July 1, 2026**

---

**Issued by: State Administration for Market Regulation;  
Standardization Administration of the PRC**

## Table of Contents

|     |                                                                                        |
|-----|----------------------------------------------------------------------------------------|
| 1   | Scope                                                                                  |
| 2   | Normative references                                                                   |
| 3   | Terms and Definitions                                                                  |
| 4   | System Evaluation Requirements                                                         |
| 5   | Objects of integrated security                                                         |
| 6   | Integrated security lifecycle                                                          |
| 7.1 | General Requirements                                                                   |
| 7.2 | Security Policy and Strategy                                                           |
| 7.3 | Organizational Requirements                                                            |
| 7.4 | Personnel                                                                              |
| 7.5 | Change Management                                                                      |
| 7.6 | Centralized Security Management                                                        |
| 10  | Safety Integration Requirements Allocation and Design                                  |
| 14  | Table C.1 Status of the Interaction Between Functional Safety and Information Security |

## Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1. Structure and Drafting Rules of Standardization Documents". Drafting. This document is Part 1 of GB/T 46933 "Integrated Safety in Smart Factories". GB/T 46933 has already published the following parts.

1. General Requirements;

2. Risk Assessment Requirements;

3. System Co-design Requirements;

4. System Evaluation Requirements. Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed by the China Machinery Industry Federation. This document is under the jurisdiction of the National Technical Committee on Standardization of Industrial Process Measurement, Control and Automation (SAC/TC124). This document was drafted by: the Mechanical Industry Instrumentation Comprehensive Technology and Economic Research Institute, Supcon Technology Co., Ltd., and the State

Petroleum & Chemical Corporation. Gas Pipeline Network Group Co., Ltd. Oil and Gas Control Center, Huazhong University of Science and Technology, Beijing Zhiwang Digital Technology Co., Ltd., Shanghai Energy Construction Engineering Design Design & Research Co., Ltd., China Electric Power Planning & Engineering Institute, China Power Engineering Consulting Group North China Electric Power Design Institute Co., Ltd., Beijing Qimingxingchen Information Security Technology Co., Ltd., Beijing Anwen Youdao Technology Co., Ltd., Ningbo Hollysys Information Security Research Institute Co., Ltd., China Petrochemical Corporation Qingdao Refining & Chemical Co., Ltd., Xi'an Electric Baoji Electric Co., Ltd., Ningbo Juhua Chemical Technology Co., Ltd., Cixi Dahua Electric Co., Ltd. Limited Company. The main drafters of this document are. Wang Linkun, Xiong Wenze, Liu Yao, Lu Weijun, Zhu Jie, Lü Feng, Zhang Jinbin, Ma Xinxin, Yuan Zhen, and Zhou Youzheng. Sun Ruoyu, Zhou Chunjie, Shi Xueling, Sun Yongkang, Fan Yongfeng, Qiu Kun, Mei Ke, Meng Zouqing, Wang Yumin, Liu Ying, Chen Xin, Gao Longbo, Wang Yong, Hong Pengda Ren Zhigang, Xu Lin, Yu Wenguang, Shuai Bing, Zhang Yabin, Guo Miao, Zhou Li, Nie Zhongwen, Zhou Qiang, Wang Lihua, Li Qiujuan, Diao Yu, Jin Ling, Feng Dongqin Pan Dongbo, Liu Yingjie, Zhu Xiaopeng, Qiao Jingyu, Li Lei, Xiao Songqing, Liu Peizhi, Zhu Minglu, Wang Yang, Sun Ai.

Traditional factories generally adopt GB/T 20438 (all parts) and application-specific standards [such as GB/T 21109 (all parts)]. Functional safety is achieved using GB/T 16855 (all parts) and GB 28526, while industrial control information security is achieved using standards such as GB/T 35673. Technically, relatively independent electrical and electronic programmable electronic or mechanical protection systems are generally used, and different systems are usually isolated or have limited separation. The connection between functional safety systems and information security protection is relatively independent. With the development of smart factories, more and more intelligent and information technologies are being applied to industrial control systems, and smart factories... The devices/systems within and between each level have achieved deeper interconnectivity, improving the efficiency of industrial operators and reducing costs, but... This also increases the complexity of the system, bringing new challenges to traditional production operation risk control. on the one hand, traditional functional safety technical measures... (Such as safety instrumented systems) face more complex application environments (such as information security threats like hacker attacks and malware, and the failure of artificial intelligence AI). (For example, the ability to control hazards, etc.) has weakened; on the other hand, the increase in external influencing factors and the enhanced correlation between various units have made the original risk reduction capabilities weaker. The applicability of risk protection theories has decreased; finally, the interaction and integration among different security protection measures has led to a surge in potential conflicts and contradictions between them. Therefore, smart factories need to adopt an integrated safety approach to achieve comprehensive safety protection throughout the entire lifecycle. GB/T 46933, "Integrated Safety in Smart Factories," aims to guide smart factories in establishing an integrated

safety lifecycle and to address risk assessment. The requirements for system evaluation, collaborative design, and system assessment are proposed and consist of four parts.

- 1.General Requirements. The purpose is to outline the overall requirements for the integrated security lifecycle, and to achieve integrated security. Basic principles;
- 2.Risk Assessment Requirements. The purpose is to outline the procedures and requirements for conducting integrated safety risk assessments;
- 3.System Collaborative Design Requirements. The aim is to address the manufacturing execution layer, process monitoring layer, and field control layer of a smart factory. The system requires collaborative design with the field equipment layer;
- 4.System Evaluation Requirements. The purpose is to propose methods and requirements for conducting integrated security capability evaluations. Smart factory safety integration Part

## 1 Scope

GB/T 46933.1-2025 is the Chinese national standard covering treating machine safety and cybersecurity as one problem - the general requirements that the other parts build on, the responsibilities, the lifecycle and the principle that a security measure must not defeat a safety function and vice versa. Part 1 of the series, first edition, with Parts 2, 3 and 4 published together. It was issued on 31 December 2025 and has been in force since 1 July 2026, as a first edition. The document is under the responsibility of the China Machinery Industry Federation. This page is published from the official record of the 2025 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

This document specifies the objects, full lifecycle management, concept and objective definition, risk assessment, and requirement allocation for integrated safety in smart factories. Requirements for each stage of design, validation, operation and maintenance, modification and alteration, decommissioning and retirement. This document applies to the risk assessment, design, and implementation of integrated safety in smart factories.

## 2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included. For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies. This document.

GB/T 20438 (all parts) Functional safety of electrical/electronic/programmable electronic

safety-related systems

GB/T 22239 Information Security Technology - Basic Requirements for Network Security Level Protection

GB/T 30976.1 Information security of industrial control systems - Part

### 3 Terms and Definitions

The following terms and definitions apply to this document.

3.1 smart factory By deeply integrating automated measurement and control technology, information technology, and intelligent technology with the entire production process and all its elements, the production operation process is monitored. The entire chain of planning, management, diagnosis, and optimization enables digital design, intelligent production, networked management, and smart services, building a flexible and highly efficient system. A factory with an efficient, green, and safe production and operation system.

3.2 The process of controlling risks within a tolerable range by coordinating risk assessment, designing and comprehensively using various risk reduction measures.

3.3 Safety integrity level A discrete level (one of four possible levels), corresponding to a range of security integrity values. Security integrity level 4 is the highest. Security integrity level 1 is the lowest.