ICS 25.040
CCS N 10

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 46933.3-2025

Safety and security integration of smart factories - Part 3: System collaborative design requirements

智能工厂安全一体化 第3部分：系统协同设计要求

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

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 3 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., Beijing Anwen Youdao Technology Co., Ltd. Limited Liability Company, Ningbo Hollysys Information Security Research Institute Co., Ltd., Sinopec Qingdao Refining & Chemical Co., Ltd., Xi'an Electric Baoji Electric Co., Ltd. Limited Liability Company, Shanghai Energy Construction Engineering Design & Research Co., Ltd., Changzhou Borui Power Automation Equipment Co., Ltd., Guangdong Xinguang Intelligent Systems Limited Liability Company, Saifite Engineering Technology Group Co., Ltd., Shenzhen Today International Software Technology Co., Ltd., Jiangxi Baiying High-Tech Co., Ltd. Limited Liability Company, Cixi Dahua Electric Appliance Co., Ltd. The main drafters of this document are. Xiong Wenze, Zhu Jie, Lu Weijun, Liu Yao, Zhou Youzheng, Sun Ruoyu, Shen Liang, Sun Yongkang, Zhou Chunjie, and Zhang Jinbin. Fan Yongfeng, Ma Xinxin, Mei Ke, Qiu Kun, Liu Ying, Chen Xin, Gao Longbo, Zhou Li, Nie Zhongwen, Liu Liang, Wang Yuhao, Fu Mingtao, Sun Chuanwu, Wang Heping Wu Fengming, Wang Lihua, Ren Zhigang, Hong Pengda, Qiao Jingyu, Wu Haifeng, Zhang Kai, Xu Lin, Yu Wenguang, Zhang Zhaoyun, Hao Xin, Wu Lei, Shuai Bing, Zhang Yabin Guo Miao, 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 is implemented using standards such as GB/T 35673 (all parts). Information security. Technically, it generally uses relatively independent electrical and electronic programmable electronic or mechanical protection systems, and different systems are usually isolated from each other. With limited or isolated connections, functional safety systems and information security protections are also set up relatively independently. 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 estimation, collaborative design, and evaluation verification 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. The use of information or network technologies has exposed more risks and vulnerabilities in traditional functional safety-related systems, making them more susceptible to internal/external threats. External attacks, such as communications attacks, can increase system load and prevent timely response to dangerous events involving the controlled object (EUC). Unauthorized external access and modification may alter important system configuration parameters and system firmware, causing system malfunction or vulnerability to external manipulation. Therefore, information security risks must also be considered and information security protection designs must be implemented in the design of functional safety-related systems. However, information security protection design cannot be considered in isolation during system design; the synergy between the two security measures must be taken into account. One side... The increasing external information security risks lead to increased risks for EUC and EUC control systems, placing higher demands on security functions. On the other hand, inappropriate information security protection design may negatively impact system functional security, including the execution of security functions. And the realization of security and integrity capabilities, for example. using encryption algorithms in data communication can effectively protect against the risk of information leakage, but... The decryption process will increase data processing time, and the functional safety response time will not meet expectations; the information security design increases the system's complexity. Complexity, and failure in this part, can also lead to system malfunctions, affecting production efficiency and causing financial losses to users. Therefore, without security... However, when considering all factors, a safety design may actually introduce additional risks. In conclusion, smart factories need to comprehensively consider the synergy between functional safety-related systems and information security protection facilities to ensure mutual protection. Effective integration and reduced conflict mean implementing a collaborative design for an integrated security system. Smart factory safety integration Part

1 Scope

GB/T 46933.3-2025 is the Chinese national standard covering designing the safety and security systems together - the shared architecture and zoning, the interfaces between the safety instrumented functions and the security controls, and the conflicts that have to be resolved on paper rather than discovered in service. Part 3 of the series, first edition. 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 system collaborative design architecture, system collaborative design objectives and principles, and system collaborative design requirements for integrated security. This document is applicable to users, designers, system evaluation parties, and safety regulatory agencies in smart factories for integrated safety design. confirm.

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 16855.1 Mechanical safety - Safety control systems - Part

3 Terms and Definitions

The terms and definitions defined in GB/T 46933.1 apply to this document.

4.Abbreviations The following abbreviations apply to this document. DoS. Denial of Service