ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 46334-2025

Security testing methods for critical network devices - Programmable logic controller (PLC)

网络关键设备安全检测方法 可编程逻辑控制器（PLC）

Issued on: October 5, 2025 **Implemented on: May 1, 2026**

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

Table of Contents

1.Scope 1
2 Normative References 1
3.Terms and Definitions 1
4.Abbreviations 2
5.Test Environment 2
6.Safety Function Testing Methods 3
6.1 Equipment Identification Safety 3
6.2 Redundancy, Backup Recovery, and Anomaly Detection 3
6.3 Vulnerability and Malicious Program Prevention 4
6.4 Security of Pre-installed Software Startup and Updates 4
6.5 User Identification and Authentication 5
6.7 Log Audit Security 7
6.8 Communication security 8
6.9 Data Security 8
7.1 Supply Chain Security 9
7.2 Design and Development 9
7.3 Production and Delivery 10
11 References 12

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. 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 National Industrial Information Security Development Research Center, the Machinery Industry Instrumentation Comprehensive Technology and Economic Research Institute, and China... China Electronics Technology Standardization Institute, Supcon Technology Co., Ltd., China Electronics Intelligent Technology Co., Ltd., Aotuo Technology Co., Ltd., Mitsubishi

Electrical Automation (China) Co., Ltd., Schneider Electric (China) Co., Ltd., the Third Research Institute of the Ministry of Public Security, and the National Computer Network Emergency Response Technical Team/Coordination Center. Technology Processing Coordination Center, China Cybersecurity Review and Certification and Market Supervision Big Data Center, China Academy of Information and Communications Technology, National Information Technology Security Research Center, the Sixth Research Institute of China Electronics Corporation, and the China Software Testing Center (Ministry of Industry and Information Technology Software) (in collaboration with the Integrated Circuit Promotion Center), Institute of Information Engineering, Chinese Academy of Sciences, Ningbo Hollysys Information Security Research Institute Co., Ltd., and Siemens) Rockwell Automation (China) Co., Ltd., Omron (Shanghai) Co., Ltd., Omron Automation (China) Co., Ltd. The company, Beijing Tonghe Shiyi Telecommunications Science and Technology Research Institute Co., Ltd., China Southern Power Grid Science Research Institute Co., Ltd., and the People's Liberation Army Military Strategic Support Force Information Engineering University, Guangzhou University, Zhejiang University, Antiy Labs Group Co., Ltd., Beijing Huashun Xin'an Information Technology Co., Ltd. Technology Co., Ltd., Fiberhome Technologies (Beijing) Co., Ltd., China Electric Power Research Institute Co., Ltd., Beijing Zhongguancun Laboratory, Shanghai Computer Software Technology Development Center, Beijing Tenkong Technology Co., Ltd., and Beijing Zhuoshi Network Security Technology Co., Ltd. The main drafters of this document are. Zhao Ran, Wang Yumin, Yao Xiangzhen, Cheng Xi, Liu Zihe, Lu Weijun, Huo Yuxian, Chen Sining, Cui Longcheng, and Wang Yong. Zou Chunming, Zhang Xiaoming, Shen Yongbo, Xia Ji, Guo Chunying, Zeng Zhenzhen, Huo Chaobin, Zhou Ruikang, Li Lin, Wang Xiangyu, Yan Zhaoteng, Liu Ying, Yan Tao, Pan Liang Yu Haibin, Ding Yiping, Zhang Bo, Yuan Yudong, Xu Aidong, Ma Rongkuan, Shang Wenli, Cheng Peng, Wang Naiqing, Deng Huan, Gong Lianghua, Jia Ling, Wang Zhihui Wang Yazhe, Zhang Jiawei, Li Peng, Wang Aipeng, Du Jinran, Jing Guoli, Chu Bing, Liao Jian, Pei Yuandou, Wang Yutao, He Minchao, Che Xin, Zhang Wei, Zhang Yawei Lin Hao, Ge Jianxin, Han Juan, Wei Qiang, Xiao Yufen, Wang Tiegang, Liu Ren, Xiong Junwei. Security testing methods for critical network equipment Programmable Logic Controller (PLC)

1 Scope

GB/T 46334-2025 is the Chinese national standard covering security testing a PLC - the authentication and the protocol robustness under malformed traffic, the firmware integrity and the update path, the program upload and download controls, the logging, and the behaviour under a denial of service against a device that controls a process. First edition, in force from 1 May 2026. Issued on 5 October 2025, it has been in force since 1 May 2026.

This document describes the methods for testing the safety functions of programmable logic controllers and for evaluating their safety assurance. This document applies to the research, development, testing, and other work related to programmable logic controllers

that meet the requirements of network critical equipment.

Note. Meeting the scope of network critical equipment refers to the equipment's performance indicators or specifications conforming to the provisions of the "Catalogue of Network Critical Equipment and Network Security Dedicated Products". The range.

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 25069 Information Security Technical Terminology

GB/T 45406-2025 Security Technical Requirements for Critical Network Equipment - Programmable Logic Controllers (PLCs)

3 Terms and Definitions

The terms and definitions defined in GB/T 25069 and the following terms and definitions apply to this document.

3.1 Electronic systems for digital operation in industrial environments. The system uses programmable memory as internal registers for user-instruction-oriented operation. Devices perform specified functions, such as logic, sequencing, timing, counting, and arithmetic, and control various types of machinery or equipment through digital or analog I/O. process. [Source: GB/T 15969.1-2007, 3.5, with modifications]

3.2 Pre-installed software Software installed or provided at the time of manufacture that is necessary to ensure the normal operation of the equipment.

Note. The pre-installed software of a programmable logic controller is usually the device firmware. [Source: GB 40050-2021, 3.10, with modifications]

3.3 Read Upload the pre-installed software, programs, status parameters, and other data from the programmable logic controller.

3.4 Write The pre-installed software, programs, status parameters and other data are downloaded to the programmable logic controller.

3.5 Vulnerability Vulnerabilities in assets or controls that could be threatened or exploited.