ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 45406-2025

Security technical requirements for critical network devices - Programmable logic controller (PLC)

网络关键设备安全技术要求 可编程逻辑控制器（PLC）

Issued on: March 28, 2025 **Implemented on: October 1, 2025**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.

This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260).

This document was drafted by: National Industrial Information Security Development Research Center, China Electronics Technology Standardization Institute, Machinery Industry Instrument Representatives include the Institute of Comprehensive Technology and Economics, the Third Research Institute of the Ministry of Public Security, the National Computer Network Emergency Response Technical Processing Coordination Center, and the China Network Security Review Center.

Certification and Market Supervision Big Data Center, China Academy of Information and Communications Technology, National Information Technology Security Research Center, China Electronic Information Industry The Sixth Research Institute of the Group Co., Ltd., China Software Evaluation Center (Software and Integrated Circuit Promotion Center of the Ministry of Industry and Information Technology), Chinese Academy of Sciences Information Engineering Research Institute, Zhongkong Technology Co., Ltd., Ningbo Hollysys Information Security Research Institute Co., Ltd., China Electronics Intelligent Technology Co., Ltd.

Co., Ltd., AoTuo Technology Co., Ltd., Mitsubishi Electric Automation (China) Co., Ltd., Schneider Electric (China) Co., Ltd., Siemens (China Co., Ltd., Rockwell Automation (China) Co., Ltd., Omron (Shanghai) Co., Ltd., Omron Automation (China) Co., Ltd.

Beijing Tonghe Shiyi Telecommunications Science and Technology Research Institute Co., Ltd., China Southern Power Grid Research Institute Co., Ltd., Zhejiang University, Antiy Technology Group Co., Ltd., Beijing Winut Technology Co., Ltd., Beijing Huashun Xinan Information Technology Co., Ltd., Venusstar Information Technology Group Co., Ltd., Fengtai Technology (Beijing) Co., Ltd., China Electric Power Research Institute Co., Ltd., Beijing Zhongguancun Laboratory, Shanghai Computer software technology development center.

The main drafters of this document are: Zhang Ge, Zhao Ran, Yao Xiangzhen, Wang Yumin, Zhang Yong, Zou Chunming, Zhang Xiaoming, Shen Yongbo, Xia Ji, Liu Zihe, Zhang Zhibing, Zeng Zhenzhen, Huo Chaobin, Zhou Ruikang, Li Lin, Wang Xiangyu, Yan Zhaoteng, Lu Weijun, Liu Ying, Huo Yuxian, Chen Sining, Cui Longcheng, Wang Yong, Yan Tao, He Hua, Yu Haibin, Ding Yiping, Zhang Bo, Yuan Yudong, Xu Aidong, Cheng Peng, Wang Naiqing, Zhang Dongqi, Deng Huan, Yuan Zhen, Gong Lianghua, Yan Minhui, Wang Yazhe, Zhang Jiawei, Li Peng, Wang Aipeng, Zhang Yunan, Wang Fangli, Jing Guoli, Chu Bing, Liao Jian, Pei Yuandou, Wang Yutao, He Minchao, Che Xin, Zhang Wei, Chunying Guo, Hao Lin, Jianxin Ge, and Juan Han.

Security technical requirements for key network equipment Programmable Logic Controller (PLC)

1 Scope

This document specifies the security function requirements and security assurance requirements for programmable logic controllers of network critical equipment.

This document is applicable to the research and development, testing, etc. of programmable logic controllers, which are key network equipment.

Note. Critical network equipment refers to equipment whose performance indicators or specifications meet the scope specified in the "Catalogue of Critical Network Equipment and Special Network Security Products".

2 Normative references

GB/T 25069-2022

GB 40050-2021

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

3.1 [Source. GB/T 15969.1-2007, 3.5, modified]

Use programmable memory as internal register for user instructions to complete specified functions (such as logic, sequence, timing, counting, operation, etc.) An electronic system used for digital operation of industrial control that controls various types of machinery or processes through digital or analog I/O.

3.2 Pre-installed software

Software installed or provided when the device leaves the factory to ensure normal use of the device.

Note. The pre-installed software for a PLC is usually the device firmware.

[Source. GB 40050-2021, 3.10, modified]

3.3 reading

The process of uploading pre-installed software, programs, status parameters and other data in the programmable logic controller.

3.4 writing

The process of transferring pre-installed software, programs, status parameters and other

data to the programmable logic controller.

3.5 Vulnerability

Weaknesses in assets or controls that could be exploited by a threat. [Source. GB 40050-2021, 3.3]