ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 46334—2025

网络关键设备安全检测方法 可编程逻辑控制器(PLC)

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

2025-10-05 发布　　2026-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：国家工业信息安全发展研究中心、机械工业仪器仪表综合技术经济研究所、中国电子技术标准化研究院、中控技术股份有限公司、中电智能科技有限公司、傲拓科技股份有限公司、三菱电机自动化(中国)有限公司、施耐德电气(中国)有限公司、公安部第三研究所、国家计算机网络应急技术处理协调中心、中国网络安全审查认证和市场监管大数据中心、中国信息通信研究院、国家信息技术安全研究中心、中国电子信息产业集团有限公司第六研究所、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、中国科学院信息工程研究所、宁波和利时信息安全研究院有限公司、西门子(中国)有限公司、罗克韦尔自动化(中国)有限公司、欧姆龙(上海)有限公司、欧姆龙自动化(中国)有限公司、北京通和实益电信科学技术研究所有限公司、南方电网科学研究院有限责任公司、中国人民解放军战略支援部队信息工程大学、广州大学、浙江大学、安天科技集团股份有限公司、北京华顺信安信息技术有限公司、烽台科技(北京)有限公司、中国电力科学研究院有限公司、北京中关村实验室、上海计算机软件技术开发中心、北京腾控科技有限公司、北京卓识网安技术股份有限公司。

本文件主要起草人：赵冉、王玉敏、姚相振、程曦、刘子贺、陆卫军、霍玉鲜、陈思宁、崔龙成、王勇、邹春明、张晓明、申永波、夏冀、郭春颖、曾珍珍、霍朝宾、周睿康、李琳、王翔宇、闫兆腾、刘盈、闫韬、潘亮、于海斌、丁一平、张博、袁玉东、许爱东、麻荣宽、尚文利、程鹏、王乃青、邓焕、龚亮华、贾玲、王智慧、王雅哲、张嘉玮、李鹏、王爱鹏、杜金燃、荆国利、楚兵、廖剑、裴渊斗、汪宇涛、贺敏超、车欣、章维、张亚薇、林浩、葛建新、韩娟、魏强、肖钰汾、王铁钢、刘韧、熊俊伟。

网络关键设备安全检测方法 可编程逻辑控制器(PLC)

1 范围

本文件描述了可编程逻辑控制器的安全功能检测方法和安全保障评估方法。

本文件适用于符合网络关键设备规定范围的可编程逻辑控制器的研发、测试等工作。

注:符合网络关键设备规定范围是指设备的性能指标或规格符合《网络关键设备和网络安全专用产品目录》中规定的范围。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 45406—2025 网络关键设备安全技术要求 可编程逻辑控制器(PLC)

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

可编程逻辑控制器 programmable logic controller;PLC

用于工业环境的数字式操作的电子系统。系统用可编程的存储器作为面向用户指令的内部寄存器,完成规定的功能,如逻辑、顺序、定时、计数、运算等,通过数字或模拟的I/O,控制各种类型的机械或过程。

[来源:GB/T 15969.1—2007,3.5,有修改]

3.2

预装软件 pre-installed software

设备出厂时安装或提供的、保障设备正常使用必需的软件。

注:可编程逻辑控制器的预装软件通常为设备固件。

[来源:GB 40050—2021,3.10,有修改]

3.3

读取 read

将可编程逻辑控制器中的预装软件、程序、状态参数等数据上传。

3.4

写入 write

将预装软件、程序、状态参数等数据下传至可编程逻辑控制器中。

3.5

漏洞 vulnerability

可能被威胁利用的资产或控制的弱点。