ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36470—2018

信息安全技术　工业控制系统现场测控设备通用安全功能要求

Information security technology—Common security functional requirements for data acquisition and control field devices of industrial control systems

2018-06-07 发布　　2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:全球能源互联网研究院有限公司、中国电力科学研究院有限公司、北京和利时系统工程有限公司、北京四方继保自动化股份有限公司、华北电力大学、国电南瑞科技股份有限公司、沈阳电业电气安装有限公司、中国信息安全测评中心、北京江南天安科技有限公司、中国电子技术标准化研究院、国家信息技术安全研究中心。

本标准主要起草人:梁潇、高昆仑、王弢、任雁铭、李焕、郑晓崑、徐茹枝、殷尧、郑洁、王迪、赵保华、安宁钰、王志皓、赵婷、詹雄、李凌、张姗、谢丰、陈冠直、李冰、刘鸿运、范科峰、李琳。

引　言

现场测控设备是工业控制系统的基本功能执行设备，直接对工业生产过程进行监视与控制，对于生产的安全稳定运行至关重要。

随着信息通信技术在工业控制系统中的应用，现场设备的智能化程度逐渐增加，网络化和处理能力的增加使得这些设备所面临的信息安全风险较传统现场设备面临的风险种类更多，范围更大，层次更为深入，一旦遭受攻击，将直接导致设备所辖区域内甚至连锁性的生产事故，因此其信息安全不仅与生产安全和经济安全密不可分，而且电力、化工、天然气等重要基础设施的现场安全水平直接关系到国计民生、社会稳定与公众利益。

为提高现场设备的信息安全能力，本标准提出针对现场测控设备的通用安全功能要求，用于设备的安全设计、开发、测试与评估。使用者应根据实际或计划使用环境的安全风险分析结果，选择设备应满足的安全功能要求。

信息安全技术　工业控制系统现场测控设备通用安全功能要求

1　范围

本标准规定了工业控制系统现场测控设备的用户标识与鉴别、使用控制、数据完整性、数据保密性、数据流限制、资源可用性6类通用的安全功能要求。

本标准适用于指导设备的安全设计、开发、测试与评估。

涉及设备功能实现原理、工业控制系统整体管理和运行以及信息安全外围技术的内容不在本标准范围之内。例如：

——本标准不涵盖与设备自身安全功能与实现没有直接关联的行政性管理和运行安全要求，如组织管理和人员管理等。对于影响技术实施的口令策略和配置程序等管理措施，将包含在要求的描述中，不作关于管理和运行内容的强调；

——本标准不涵盖与设备自身信息安全功能与实现没有直接关联的电磁辐射等物理安全方面的内容，对于影响信息安全技术防护效果的物理安全访问控制等措施，将包含在要求的描述中，不作关于物理安全内容的强调；

——本标准不对传统工业控制系统中机电式、液压式和气动式等不涉及信息技术实现原理的设备的信息安全功能进行要求；

——本标准不覆盖传感器、变送器、调节器、开关/断路器等生产过程设备。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分：安全体系结构

GB/T 25069—2010　信息安全技术　术语

GB/T 32919—2016　信息安全技术　工业控制系统安全控制应用指南

3　术语和定义

GB/T 9387.2—1995、GB/T 25069—2010和GB/T 32919—2016界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统现场测控设备　data acquisition and control field devices of industrial control systems

工业控制系统中，位于现场，具有以下生产相关全部或部分功能的一种独立实体设备：

——从传感器、变送器、调节器或开关等过程设备接收采集数据；

——进行逻辑与控制计算；

——向调节器或开关等过程执行设备发送控制指令。

设备与其他同类设备、系统主站或应用进行采集数据与控制指令等数字或模拟信号通信。

典型工业控制系统现场测控设备的功能与构成参见附录A。