ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37953—2019

信息安全技术　工业控制网络监测安全技术要求及测试评价方法

Information security technology—Security requirements and evaluation approaches for industrial control network monitor

2019-08-30 发布　　2020-03-01 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:中国电子技术标准化研究院、中国科学院沈阳自动化研究所、深圳赛西信息技术有限公司、北京工业大学、公安部第三研究所、浙江浙能台州第二发电有限责任公司、中国信息安全测评中心、上海三零卫士信息安全有限公司、上海交通大学、国家信息技术安全研究中心、和利时集团、北京启明星辰信息安全技术有限公司、烽台科技(北京)有限公司、国网浙江省电力有限公司电力科学研究院、华大半导体有限公司、中国电力工程顾问集团西南电力设计院有限公司、中国平安保险(集团)股份有限公司、北京匡恩网络科技有限责任公司。

本标准主要起草人:范科峰、周睿康、姚相振、李琳、刘贤刚、龚洁中、张大江、尚文利、赖英旭、顾健、陆臻、邹春明、夏克晁、朱青国、谢丰、邸丽清、戴忠华、赵剑明、仵大奎、谷大武、夏正敏、李冰、王戬、孟雅辉、龚亮华、魏钦志、罗志浩、兰天、张晋宾、于惊涛、毕思文。

引　言

随着工业化与信息化的深度融合，来自信息网络的安全威胁正逐步对工业控制系统造成极大的安全威胁，通用网络监测产品在面对工业控制系统的安全防护时显得力不从心，因此需要一种能应用于工业控制环境的网络监测产品对工业控制系统进行安全防护。

应用于工业控制环境的网络监测产品与通用网络监测产品的主要差异体现在：

——通用网络监测产品主要针对互联网通用协议进行分析和响应。应用于工业控制环境的网络监测产品除了能够分析部分互联网通用协议外，还具有对工业控制协议的深度解析能力，而无需对工业控制系统中不会使用的通用协议进行分析。

——应用于工业控制环境的网络监测产品可能有部分组件需部署在工业现场环境，因此比通用网络监测产品具有更高的环境适应能力。

——应用于工业控制环境的网络监测产品比通用网络监测产品具有更高的可用性、可靠性、稳定性。

信息安全技术　工业控制网络监测安全技术要求及测试评价方法

1　范围

本标准规定了工业控制网络监测产品的安全技术要求和测试评价方法。

本标准适用于工业控制网络监测产品的设计生产方对其设计、开发及测评等提供指导，同时也可为工业控制系统设计、建设和运维方开展工业控制系统安全防护工作提供指导。

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 2423.5—1995　电工电子产品环境试验　第2部分：试验方法　试验Ea和导则：冲击

GB/T 2423.8—1995　电工电子产品环境试验　第2部分：试验方法　试验Ed：自由跌落

GB/T 2423.10—2008　电工电子产品环境试验　第2部分：试验方法　试验Fc：振动(正弦)

GB/T 4208—2017　外壳防护等级(IP代码)

GB/T 17214.4—2005　工业过程测量和控制装置的工作条件　第4部分：腐蚀和侵蚀影响

GB/T 18336.1—2015　信息技术　安全技术　信息技术安全评估准则　第1部分：简介和一般模型

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

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 25069—2010、GB/T 32919—2016和GB/T 18336.1—2015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　industrial control system

多种工业生产中使用的控制系统。

注：包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)和其他较小的控制系统，如可编程逻辑控制器(PLC)，现已广泛应用在工业部门和关键基础设施中。

3.2

工业控制网络监测　industrial control network monitoring

部署于工业控制网络中，以实现针对工业控制网络中网络行为的安全事件监测、审计和管理等功能的技术。

注1：用于监测和分析工业控制网络中的数据报文，发现违反安全策略的行为、异常操作、工业控制设备被攻击的迹象，或工业生产受到影响的迹象。

注2：本标准所指“工业控制网络监测”即“工业控制网络监测产品”。工业控制网络监测产品是部署于工业控制网络中，用于实现工业控制网络监测功能的设备产品。