ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37941—2019

信息安全技术　工业控制系统网络审计产品安全技术要求

Information security technology—Security technical requirements of industrial control system network audit products

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:公安部第三研究所、公安部网络安全保卫局、珠海市鸿瑞软件技术有限公司、北京天地和兴科技有限公司、上海三零卫士信息安全有限公司、北京神州绿盟信息安全科技股份有限公司、中国信息安全研究院有限公司、北京天融信网络安全技术有限公司、中国电子技术标准化研究院、济南华汉电气科技有限公司、北京和利时系统工程有限公司、上海电力学院。

本标准主要起草人:邹春明、沈清泓、刘瑞、陆臻、陆磊、范春玲、田原、孟双、俞优、顾健、康天娇、王勇、刘智勇、陈敏超、金光宇、倪华、叶晓虎、王晓鹏、周文奇、雷晓锋、范科峰、姚相振、李琳、周睿康、朱毅明、杨晨。

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，通用安全审计产品在面对工业控制系统的安全防护时显得力不从心，因此急需要一种能应用于工业控制环境的安全审计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安全审计产品与通用安全审计产品的主要差异体现在：

——通用安全审计产品主要针对应用于互联网的通用协议进行分析和记录。用于工业控制环境的安全审计产品除了能够分析部分互联网的通用协议外，还应具有对工业控制协议的深度解释能力，而无需对电子邮件等工业控制系统中不会使用的通用协议。

——用于工业控制环境的安全审计产品可能有部分组件部署在工业现场环境，因此比通用安全审计产品需具有更高的环境适应能力。

——工业控制环境中，通常流量相对较小，流量类型相对固定，对可靠性要求更高，用于工业控制环境的安全审计产品能够支持全流量审计，并要求支持采用基于白名单方式对审计信息进行分析。

信息安全技术　工业控制系统网络审计产品安全技术要求

1　范围

本标准规定了工业控制系统网络审计产品的安全技术要求，包括安全功能要求、自身安全要求和安全保障要求。

本标准适用于工业控制系统网络审计产品的设计、生产和测试。

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 4824—2013　工业、科学和医疗(ISM)射频设备　骚扰特性　限值和测量方法

GB/T 9254—2008　信息技术设备的无线电骚扰限值和测量方法

GB/T 13729—2002　远动终端设备

GB/T 15153.1—1998　远动设备及系统　第2部分：工作条件　第1篇：电源和电磁兼容性

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 17626.2—2018　电磁兼容　试验和测量技术　静电放电抗扰度试验

GB/T 17626.3—2016　电磁兼容　试验和测量技术　射频电磁场辐射抗扰度试验

GB/T 17626.4—2018　电磁兼容　试验和测量技术　电快速瞬变脉冲群抗扰度试验

GB/T 17626.5—2008　电磁兼容　试验和测量技术　浪涌(冲击)抗扰度试验

GB/T 17626.6—2017　电磁兼容　试验和测量技术　射频场感应的传导骚扰抗扰度

GB/T 17626.8—2006　电磁兼容　试验和测量技术　工频磁场抗扰度试验

GB/T 17626.10—2017　电磁兼容　试验和测量技术　阻尼振荡磁场抗扰度试验

GB/T 17626.11—2008　电磁兼容　试验和测量技术　电压暂降、短时中断和电压变化的抗扰度试验

GB/T 17626.12—2013　电磁兼容　试验和测量技术　振铃波抗扰度试验

GB/T 17626.16—2007　电磁兼容　试验和测量技术　0 Hz～150 kHz共模传导骚扰抗扰度试验

GB/T 17626.17—2005　电磁兼容　试验和测量技术　直流电源输入端口纹波抗扰度试验

GB/T 17626.18—2016　电磁兼容　试验和测量技术　阻尼振荡波抗扰度试验

GB/T 17626.29—2006　电磁兼容　试验和测量技术　直流电源输入端口电压暂降、短时中断和电压变化的抗扰度试验

GB/T 20945—2013　信息安全技术　信息系统安全审计产品技术要求和测试评价方法

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