ICS 25.040
N 10

中华人民共和国国家标准

GB/T 40218—2021/IEC/TR 62443-3-1:2009

工业通信网络　网络和系统安全 工业自动化和控制系统信息安全技术

Industrial communication networks—Network and system security—Security technologies for industrial automation and control system

(IEC/TR 62443-3-1:2009,Industrial communication networks—Network and system security—Part 3-1: Security technologies for industrial automation and control system,IDT)

2021-05-21 发布　　2021-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 IEC/TR 62443-3-1:2009《工业通信网络　网络和系统安全　第 3-1 部分:工业自动化和控制系统信息安全技术》。

本标准做了下列编辑性修改:

——修改了标准名称;

——删除了与我国情况不符的脚注。

本标准由中国机械工业联合会提出。

本标准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。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、电力规划总院有限公司、中国核电工程有限公司、和利时科技集团有限公司、北京市自来水集团有限责任公司、浙江大学、华中科技大学、重庆邮电大学、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、西门子(中国)有限公司、施耐德电气(中国)有限公司、罗克韦尔自动化(中国)有限公司、中国科学院沈阳自动化研究所、北京启明星辰信息安全技术有限公司、北京国电智深控制技术有限公司、深圳万讯自控股份有限公司、中国电子科技集团公司第三十研究所、工业和信息化部电子第五研究所、西南大学、中国东方电气集团有限公司、北京四方继保自动化股份有限公司、国家工业信息安全发展研究中心、北京市轨道交通设计研究院有限公司、上海自动化仪表有限公司、重庆信安网络安全等级测评有限公司、公安部第三研究所、中国网络安全审查技术与认证中心、北京网御星云信息技术有限公司。

本标准主要起草人:王玉敏、梅恪、张晋宾、王彦君、华镕、孙静、张晨艳、冯冬芹、周纯杰、李锐、陈小淙、朱镜灵、魏旻、王浩、王弢、刘杰、成继勋、赵军凯、兰昆、尚文利、张为群、刘枫、刘志祥、袁晓舒、尚羽佳、郭永振、杜振华、张哲宇、肖衍、陆妹、丁长富、肖煦媛、高镜媚、闫韬、袁静、任卫红、甘杰夫、宋文刚。

引　言

保护工业自动化和控制系统(IACS)的计算机环境免受恶意代码入侵的需求在过去十年里越来越受到关注。IACS环境中越来越多地使用开放的系统、平台和协议,随着对外联合投资活动的提高、外部合作伙伴和外部资源的联合,都会带来更多的威胁和更高级的计算机攻击。随着这些威胁和脆弱性的增加,工业通信网络上遭受计算机攻击的风险也会相应地提高,因此对计算机和基于网络的信息共享和分析中心也需要加以保护。此外,智能设备和嵌入式系统的发展,计算机、网络设备和软件互连的增加,增强的外部连接以及网络入侵事故的快速增长,更多的智能攻击者和恶意的极易访问的软件,所有这些都增加了风险。

很多的电子安全技术和计算机入侵防范措施可能都适用于IACS环境。本标准列举了几类计算机信息安全技术和防范措施,并针对每一类具体讨论其所处理的脆弱性、部署的建议及其已知的优点和弱点。此外,也提供了使用各类安全技术的指南和针对以上所提及风险所要采取的防范技术。

本标准未对上述安全技术和防范措施进行比较,仅提供了使用这些技术和方法的建议和指南,以及在制定与IACS环境相关的现场或企业级信息安全策略、程序和规程中所需考虑的信息。

工作组将周期性更新技术要求以反映新的信息、计算机安全技术、应对措施和计算机风险降低方法。同时告诫读者在使用该标准中的推荐指南时,不确保其工业自动化或控制系统环境达到最佳的计算机安全状态。但是,本标准有助于识别和处理脆弱性,减少非预期的网络入侵。这些网络入侵可能会窃取机密信息,甚至造成人员和环境的伤害,或导致工业网络、控制系统及其监视和管理的工业和基础设施关键资产遭受破坏或失效。

本标准提供了对当前许多类型的电子计算机安全技术、缓解措施和工具的评价和评估,这些用于保护IACS环境以防不利的计算机入侵和攻击。本标准中介绍了各类技术、方法和工具,并提供了对这些内容的开发、实现、运行、维护、工程实施/管理和其他服务的讨论。本标准也提供了适用于生产商、供货商和终端用户的信息安全实践者、设施和工厂的指南,以便在技术选择上和应对措施上用于保护自动化的IACS(及其相关的工业网络)免受电子(计算机)攻击。

本标准中给出的指南并不能确保IACS已经达到最佳的计算机信息安全。但是,这些指南有助于识别和指出脆弱性,并且能够减少未预期入侵的风险以防保密信息的泄露或者造成控制系统和其自动控制的关键资产的损坏或失效。更关注的是,当自动化控制系统或其相关工业网络发生计算机泄密时,这些指南的使用能够帮助减少对任何人员或环境损害的风险。

本标准中的网络安全指南是通用/一般性的,视人员知识在工业自动化系统中的应用而定/并且应根据适用的、特定的工业自动化系统人员知识,正确适用于每一个控制系统和网络。本指南标识了对于提供网络安全控制系统而言,典型的、重要的活动行为。但是上述活动行为并不总是与系统功能的有效运行或维护相兼容。指南包括了针对特定控制系统的适用的信息安全的建议和推荐。然而,选择和部署那些特定用于给定控制系统及其相关的工业网络的信息安全活动和实践是系统拥有者的责任。

随着控制系统脆弱性经验的获得,特定网络信息安全实施的成熟以及新的基于控制的网络信息安全技术的使用,本标准将逐渐修改并完善。这样,在本标准的主体结构保持相对稳定的同时,其应用和解决方案也将逐步完善。

工业通信网络　网络和系统安全
工业自动化和控制系统信息安全技术

1　范围

本标准提供了对当前各种网络信息安全工具、缓解对抗措施和技术的评估。这些技术可有效地用在基于现代电子的IACS中，以调整和监视数量众多的工业和关键基础设施。本标准描述了几种类型的以控制系统为中心的网络信息安全技术、这些种类中可用的产品类别、在自动化IACS环境中使用这些产品的利弊、相对于预期的威胁和已知的网络脆弱性，更重要的是，对于使用这些网络信息安全技术产品和/或对抗措施的初步建议和指南。

本标准应用的IACS网络安全概念是最大可能地涵盖所有行业和关键基础设施中的组件、工厂、设施以及系统。IACS包括但不限于：

- 硬件（如历史数据服务器）和软件系统（如操作平台、配置、应用），例如分布式控制系统（DCS）、可编程序控制器（PLC）、监测控制和数据采集（SCADA）系统、网络化电子传感系统以及监视、诊断和评估系统。包含此硬件和软件范围的是重要的工业网络及任何相连的或相关的关键信息技术（IT）设备和对成功运行整个控制系统的链路。就这点而言，此范围也包括但不限于：防火墙、服务器、路由器、交换机、网关、现场总线系统、入侵检测系统、智能电子/终端设备、远程终端单元（RTU），以及有线和无线远程调制解调器。
- 用于连续的、批处理的、分散的或组合过程的相关内部的、人员的、网络或机器的接口，用来提供控制、数据记录、诊断、（功能）安全、监视、维护、质量保证、法规符合性、审计和其他类型的操作功能。

类似地，网络信息安全技术和对抗措施的概念也广泛用于本标准，并包括但不限于如下技术：

- 鉴别和授权；
- 过滤、阻塞和访问控制；
- 加密；
- 数据确认；
- 审计；
- 测量；
- 监视和检测工具；
- 操作系统。

此外，非网络信息安全技术，即物理安全控制，对于网络信息安全的某些方面来说是必不可少的要求，并在本标准中进行了讨论。

本标准的目的是分类和定义网络信息安全技术、对抗措施和目前可用的工具，为后续标准提供一个通用基础。本标准的每项技术从以下几方面进行讨论：

- 技术、工具和/或对抗措施所针对的信息安全脆弱性；
- 典型部署；
- 已知问题和弱点；
- 在IACS环境中使用的评估；
- 未来方向；
- 建议和指南；