ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 42445—2023/IEC TR 62443-2-3:2015

工业自动化和控制系统安全 IACS环境下的补丁管理

Security for industrial automation and control systems—Patch management in the IACS environment

（IEC TR 62443-2-3:2015,Security for industrial automation and control systems—Part 2-3:Patch management in the IACS environment,IDT）

2023-03-17 发布　　2023-10-01 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。

本文件等同采用IEC TR 62443-2-3:2015《工业自动化和控制系统安全　第2-3部分:IACS环境下的补丁管理》。文件类型由IEC的技术报告调整为我国的国家标准。

本文件做了下列最小限度的编辑性改动:

——为与现有标准协调,将标准名称改为《工业自动化和控制系统安全　IACS环境下的补丁管理》。

本文件由中国机械工业联合会提出。

本文件由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:东方电气集团科学技术研究院有限公司、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、施耐德电气(中国)有限公司、西门子(中国)有限公司、北京四方继保自动化股份有限公司、北京国能智深控制技术有限公司、华北电力大学、重庆信安网络安全等级测评有限公司、国电投芜湖发电有限责任公司、中国石油天然气股份有限公司塔里木油田分公司、重庆邮电大学、西南大学、中国科学院沈阳自动化研究所、华中科技大学、中国电子科技集团公司第三十研究所、上海工业自动化仪表研究院有限公司、工业和信息化部电子第五研究所、国家工业信息安全发展研究中心、罗克韦尔(上海)有限公司、上海电器科学研究所(集团)有限公司、和利时科技集团有限公司、工业和信息化部计算机与微电子发展研究中心(中国软件测评中心)、西安空间无线电技术研究所。

本文件主要起草人:袁晓舒、王玉敏、尚羽佳、张晋宾、王勇、闫韬、杜振华、朱镜灵、龚钢军、周彦晖、程家荣、杨其展、魏旻、刘枫、赵剑明、周纯杰、兰昆、刘慧芳、刘杰、赵冉、高镜媚、任悦、刘盈、郭永振、王爱鹏、桑梓、王英、翟婉波、杨小倩、张焱、徐进、王佳、胡博、杨超。

引　言

IEC 62443 是应用于工业自动化和控制系统安全的系列国际标准，目前我国已采用该系列标准发布了 GB/T 33007—2016《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》(IEC 62443-2-1:2010，IDT)、GB/T 35673—2017《工业通信网络 网络和系统安全 系统安全要求和安全等级》(IEC 62443-3-3:2013，IDT)、GB/T 40211—2021《工业通信网络 网络和系统安全 术语、概述和模型》(IEC 62443-1-1:2009，IDT)、GB/T 40218—2021《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》(IEC TR 62443-3-1:2009，IDT)、GB/T 40682—2021《工业自动化和控制系统网络安全　第 2-4 部分：IACS 服务提供商的安全程序要求》(IEC 62443-2-4:2015，IDT)和本文件，这些标准共同构成应用于工业自动化和控制系统安全的系列国家标准。

网络安全是现代组织中的一个日益重要的话题。许多信息技术(IT)和商业组织多年来一直持续关注网络安全，并按国际标准化组织(ISO)和国际电工委员会(IEC)的 ISO/IEC 27001 和 ISO/IEC 27002 来建立信息安全管理系统(ISMS)。这些管理系统为组织提供了一个保护其资产免受网络攻击的方法。

目前，工业自动化和控制系统(IACS)供应商和所有者在其日常活动中使用为商业系统开发的商用现成(COTS)技术。由于 COTS 系统被更广泛地了解和使用，它在 IACS 中的应用也提高了 IACS 设备受到网络攻击的机会。对于 IACS 安全新的研究也发现了许多设备的脆弱点。对工业系统的成功攻击可能导致健康、安全和环境(HSE)后果。

组织可能在不了解后果的情况下，尝试使用商业网络安全策略来解决 IACS 的安全。虽然其中的许多解决方案可以应用于 IACS，但它们需要以正确的方式应用以消除意外的后果。

本文件解决了 IACS 网络安全的补丁管理问题。补丁管理是一个网络安全整体策略的一部分，它通过安装补丁来增加网络安全性，其中补丁也被称为软件更新、软件升级、固件升级、服务包、修补程序、基本输入输出系统(BIOS)更新以及其他可解决缺陷、可操作性、可靠性和网络安全脆弱性的数字电子程序更新。本文件介绍了资产所有者和 IACS 产品供应商对于 IACS 补丁管理方面的许多问题和行业关注点，以及不良的补丁管理对 IACS 的可靠性和/或可操作性的影响。

工业自动化和控制系统安全 IACS环境下的补丁管理

1 范围

本文件描述了对已经建立并正在维护工业自动化和控制系统(IACS)补丁管理计划的资产所有者和IACS产品供应商的要求。

本文件推荐了一种定义好的格式,涉及资产所有者和IACS产品供应商分发安全补丁信息,并定义了IACS产品供应商对于补丁信息的开发和资产所有者对于补丁的部署和安装等一些相关活动。所定义的交换格式和活动主要用于安全相关的补丁。交换格式和活动被定义用于安全相关的补丁,但也可能应用于与安全无关的补丁或更新。

本文件不区分为操作系统(OS)、应用程序或设备补丁,也不区分提供基础架构组件或IACS应用程序的产品供应商,而是为适用于IACS的所有补丁提供指导。此外,补丁类型可以是用于解决缺陷、可靠性问题、可操作性问题或安全脆弱性。

注1:发现和披露影响IACS的安全脆弱性是本文件范围之外的一般性问题,本文件不提供这方面的道德标准和处理方法的指导。如果不做特殊说明,本文件中的"安全"都是指"信息安全"。

注2:本文件没有提供从发现脆弱性到创建脆弱性补丁期间如何缓解脆弱性的指导。减轻安全风险的多种补偿措施是IACS安全管理体系(IACS-SMS)的一部分,若需要这方面内容的指导,请参阅本文件附录B的B.4.5、B.4.6和B.8.5以及IEC 62443系列标准的其他部分。

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。

IEC TS 62443-1-1 工业通信网络 网络和系统安全 第1-1部分:术语、概念和模型(Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models)

注:GB/T 40211—2021 工业通信网络 网络和系统安全 术语、概念和模型(IEC TS 62443-1-1:2009,IDT)

IEC 62443-2-1 工业通信网络 网络和系统安全 第2-1部分:建立工业自动化和控制系统安全程序(Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program)

注:GB/T 33007 工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序(IEC 62443-2-1:2010,IDT)

3 术语、定义、缩略语和缩写

3.1 术语和定义

IEC TS 62443-1-1和IEC 62443-2-1界定的以及下列术语和定义适用于本文件。