ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 42456—2023/IEC 62443-4-2:2019

工业自动化和控制系统信息安全 IACS组件的安全技术要求

Security for industrial automation and control systems—Technical security requirements for IACS components

（IEC 62443-4-2:2019,Security for industrial automation and control systems—Part4-2:Technical security requirements for IACS components,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 62443-4-2:2019《工业自动化和控制系统信息安全　第4-2部分:IACS组件的安全技术要求》。

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信息安全　IACS组件的安全技术要求》。

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专利的责任。

本文件由中国机械工业联合会提出。

本文件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、成都启明星辰信息安全技术有限公司、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、中国软件测评中心(工业和信息化部软件与集成电路促进中心)、菲尼克斯亚太电气(南京)有限公司。

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、王锐、杨金华、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、潘学龙。

引　言

0.1　概述

IEC 62443 是应用于工业自动化和控制系统安全的系列标准，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/TS 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)、GB/T 42445—2023《工业自动化和控制系统安全　IACS环境下的补丁管理》(IEC/TR 62443-2-3:2015，IDT)、GB/T 42457—2023《工业自动化和控制系统信息安全　产品安全开发生命周期要求》(IEC 62443-4-1:2018，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。

工业自动化和控制系统(IACS)组织越来越多地使用便宜、高效和高度自动化的商用现成(COTS)网络设备。出于合理的商业原因，控制系统也越来越多地与非IACS网络相互连接。这些设备、开放的网络技术以及增加的连通性都给控制系统的软硬件提供了日益增加的遭受网络攻击的机会。该弱点可能导致部署的控制系统中的健康、安全和环境(HSE)、财务和/或声誉的系列后果。

利用商业信息技术(IT)网络安全解决方案来解决IACS安全问题的组织，可能尚未完全理解这一决定的结果。同时，许多商业IT应用和安全解决方案可以应用于IACS，因此需要以适当的方式应用这些解决方案以消除无意的后果。出于这个原因，定义系统要求的方法综合考虑功能要求和风险评估，通常也包括对操作问题的认识。

IACS安全对策包括应急程序，宜避免造成必要的服务和功能缺失的可能性(通常利用的IT安全对策确实有这个潜在可能性)。IACS安全目标集中在控制系统的可用性、工厂保护、工厂操作(即使在降级模式下)和对时间要求严格的系统响应。IT安全目标通常并不同等重视这些因素；他们可能更关心保护信息而不是物理资产。不管工厂集成的程度如何，这些不同的目标都需要明确地表述为安全目标。根据IEC 62443-2-1的要求，风险评估的一个关键步骤宜是确定哪些服务和功能对于运营是真正必要的(例如，在某些设施中，工程支持可能被确定为非基本服务或功能)。与必要服务或功能不宜受到不利影响不同，在某些情况下，信息安全措施可能会导致的暂时丢失非必要服务或功能是可以接受的。

本文件为组成IACS的组件提供网络安全要求，特别是嵌入式设备、网络组件、主机组件和软件应用。附录A描述了IACS常用设备的分类。本文件的要求参考IEC 62443-3-3描述的IACS系统安全要求。本文件的目的是指定安全功能，使组件能够在给定的安全等级(SL)下集成到系统环境中。附录B中的表格汇总了本文件定义的要求和增强要求的SL。

IEC 62443系列标准的主要目标是提供一个灵活的框架，有助于解决IACS当前和未来的脆弱性，并以系统的、可防御的方式应用必要的缓解措施。IEC 62443的目的是构建适应企业IT系统需求的企业安全扩展，并将其与IACS所需的高完整性和可用性的独特要求相结合，这点十分重要。

0.2　目的和目标读者

本文件在IACS社区的目标读者是资产所有者、系统集成商、产品供应商以及合适的合规部门。合

规部门包括具有法定权力的政府机构和监管机构,可以进行审计以验证其是否遵守法律法规。

系统集成商将使用本文件来协助他们采购构成IACS解决方案的控制系统组件。本文件将帮助系统集成商对他们正在采购的单个组件明确提出适当的安全能力水平。系统集成商参考的主要标准是IEC 62443-2-1、IEC 62443-3-2和IEC 62443-3-3,它们提供安全管理系统的组织和操作要求,并指导系统集成商完成定义安全区的过程和定义这些区域的目标安全能力水平(SL-T)。一旦定义了每个区域的SL-T,提供必要功能的组件能够实现每个区域的SL-T。

产品供应商将使用本文件来理解具有特定SL-C要求的控制系统组件的要求。组件可能本身不提供安全能力,但可能与更高级别的实体集成设计,从而受益于该实体的能力——例如,嵌入式设备本身可能不具备维持用户目录的能力,而是可能被集成进具备鉴别和授权服务的系统,因此仍然满足提供个人用户鉴别、授权和管理能力的要求。本文件将指导产品供应商可以分配哪些要求以及哪些要求需要在组件中内置。根据IEC 62443-4-1的实践8的规定,产品供应商将提供如何正确地将组件集成到系统以符合特定SL-T的文件。

本文件中的组件要求(CR)参考IEC 62443-3-3中的系统要求(SR)。IEC 62443-3-3中的要求被称为SR,它是从IEC 62443-1-1中定义的总体基本要求(FR)中导出的。CR还可以包括一组增强要求(RE)。CR和RE的组合将决定组件能够实现的目标安全等级。

本文件为四种类型的组件提供了要求:软件应用、嵌入式设备、主机设备和网络设备。因此,每种组件的CR将被指定如下:

- 软件应用要求(SAR);
- 嵌入式设备要求(EDR);
- 主机设备要求(HDR);
- 网络设备要求(NDR)。

本文件的大部分要求对于四种类型组件是相同的,因此简称为CR。当有独特的组件特定要求时,通用要求将声明该要求是组件特定的,并且位于本文件的组件特定要求条款中。

图1示出了本文件编写时IEC 62443系列标准的图形描述。

图 1　IEC 62443 标准体系

工业自动化和控制系统信息安全 IACS 组件的安全技术要求

1 范围

本文件提供了与 IEC TS 62443-1-1 中描述的七个基本要求(FR)相关的详细的技术控制系统组件要求(CR),包括定义控制系统能力安全等级和其组件 SL-C(组件)的要求。

按照 IEC TS 62443-1-1 的规定,总共有七个 FR:

a) 标识和鉴别控制(IAC),

b) 使用控制(UC),

c) 系统完整性(SI),

d) 数据保密性(DC),

e) 受限数据流(RDF),

f) 事件的及时响应(TRE),

g) 资源可用性(RA)。

这七个要求(FR)是定义控制系统安全能力级别的基础。本文件的主要目标是定义控制系统组件的安全能力水平,而 SL(SL-T)或如何实现 SL(SL-A),不在本文件规定的范围。

注 1:全面实现控制系统的 SL 目标,还需参见 IEC 62443-2-1 规定的一系列非技术性、程序相关的 CR 的能力。如果不做特别说明,本文件中的"安全"指的是"信息安全"。

注 2:本文件提及的商标及商品名称仅为方便用户使用。此信息不构成 IEC 对所提及产品的认可。

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。

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)

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 62443-3-3 工业通信网络 网络和系统安全 第 3-3 部分:系统安全要求和安全等级(Industrial communicaiton networks—Network and system security—Part 3-3:System security requirements and security levels)

IEC 62443-4-1 工业自动化和控制系统信息安全 产品安全开发生命周期要求(Security for industrial automation and control systems—Part 4-1: Secure product development lifecycle requirements)

注:GB/T 42457—2023 工业自动化和控制系统信息安全 产品安全开发生命周期要求(IEC 62443-4-1:2018,