ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 44861—2024/IEC 62443-3-2:2020

工业自动化和控制系统安全 系统设计的安全风险评估

Security for industrial automation and control systems—Security risk assessment for system design

（IEC 62443-3-2:2020,Security for industrial automation and control systems—Part 3-2: Security risk assessment for system design,IDT）

2024-10-26 发布　　2025-05-01 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 62443-3-2:2020《工业自动化和控制系统安全　第3-2部分:系统设计的安全风险评估》。

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　系统设计的安全风险评估》。

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:机械工业仪器仪表综合技术经济研究所、北京天地和兴科技有限公司、重庆信安网络安全测评有限公司、电力规划总院有限公司、中国工程物理研究院动力部、东方电气集团科学技术研究院有限公司、国能智深控制技术有限公司、北京市自来水集团有限责任公司、施耐德电气(中国)有限公司、罗克韦尔自动化(中国)有限公司、国网辽宁省电力有限公司电力科学研究院、国网辽宁省电力有限公司大连供电公司、华北电力大学、淄博市标准化研究院、深圳市奥图威尔科技有限公司、北京机械工业自动化研究所有限公司、北京市自来水集团大通供水技术有限公司、华北电力科学研究院有限责任公司、国网思极网安科技(北京)有限公司、北京卓识网安技术股份有限公司、中国电力科学研究院有限公司、国网北京市电力公司电力科学研究院、国家电网有限公司信息通信分公司、国网山东省电力公司潍坊供电公司、北京电安信科技有限公司、广东电网有限责任公司、中国电子科技集团公司第三十研究所。

本文件主要起草人:尚羽佳、李凯斌、周彦晖、张一彬、周沫燃、张晋宾、王玉敏、李云、张晨艳、杨书评、朱镜灵、高镜媚、王勇、胡博、杨超、李桐、孙峰、孙跃、唐聪、高涛、杨波、程平、翟婉波、张强、龚钢军、陆俊、何剑、刘韧、屠竞哲、杨德龙、高阳、王立永、陈亮、王怀宇、李志宏、孙华忠、张琪、李燕平、施又丹、王海城、周泽龙、李祉岐、兰昆。

引　言

之所以没有简单的方法来保证工业自动化和控制系统(IACS)的安全,是因为安全是一个风险管理问题。由于面临的威胁、产生这些威胁的可能性、系统中固有的脆弱性以及系统被破坏时的后果不同,使得每一个 IACS 都会给组织带来不同的风险。此外,不同组织对风险的容忍度都不同。

本文件旨在指导组织评估特定 IACS 的风险,识别并应用安全对策,将风险降低到可承受的水平。

本文件中的关键概念是区域和管道的应用,定义见 GB/T 40211。

本文件的使用者包括资产所有者、系统集成商、产品供应商、服务提供商和合规管理机构等。

本文件通过目标安全等级(SL-T)与能力安全等级(SL-C)达成一致来为确定安全对抗措施提供依据。

工业自动化和控制系统安全 系统设计的安全风险评估

1 范围

本文件规定了以下方面的要求：

a) 确定工业自动化和控制系统(IACS)的被评估系统(SUC)；

b) 划分 SUC 的区域和管道；

c) 评估每个区域和管道的风险；

d) 建立每个区域和管道的目标安全等级 (SL-T)；

e) 文档化安全要求。

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)

3 术语、定义、缩略语和约定

3.1 术语和定义

下列术语和定义适用于本文件。

ISO 和 IEC 维护的用于标准化的术语数据库网址如下：

——ISO 在线浏览平台：https://www.iso.org/obp；

——IEC 电工百科：https://www.electropedia.org/。

3.1.1

通道 channel

资产之间的特定逻辑或物理的通信链路。

注：通道有助于建立连接。

3.1.2

合规管理机构 compliance authority

有权确定管理文件中规定的安全评估的充分性或实施的有效性的实体机构。

注：合规管理机构的例子包括政府机构、监管机构、外部和内部审计机构。

3.1.3

管道 conduit

连接两个及以上区域、具有相同安全要求的通信信道的逻辑分组。