

# 工业自动化与控制系统（IACS）的网络安全管理

## 概述：工业和监管环境中的运营技术（OT）安全

工业自动化与控制系统（IACS）是现代生产、工艺和基础设施格局的核心组成部分。持续的数字化、物联网技术的应用、远程维护理念以及信息技术（IT）与运营技术（OT）日益融合，都在不断提升效率和透明度，但同时也显著扩大了攻击面和网络风险。

在工业环境中，尤其关注控制和过程数据的可用性、完整性和机密性等安全目标。安全事件会对生产能力、产品质量、环境和人身安全以及公司的经济稳定性和声誉产生直接影响。同时，监管要求以及客户和合作伙伴的需求也日益增加对结构化、可验证的运营技术（Operational Technology, OT）安全水平的需求。

IEC 62443-2-1:2024（2.0版）标准是工业自动化和控制系统运营商（资产所有者）的核心国际标准。

它为系统安全计划（SP）的政策、流程和组织措施制定了要求，以确保国际船级社协会（IACS）运营中的网络安全。在当前版本中，“网络安全管理系统”（CSMS）一词被特意替换为“安全计划”，以便更好地与现有的信息安全管理（ISMS）系统保持一致，并确保重叠部分的一致整合。

该标准明确考虑了工业厂房的长生命周期，并通过基于风险的措施和补偿措施来解决遗留系统的安全处理问题。工业自动化（OT）安全的技术、组织、人员和物理方面均以综合方式加以考虑，并在整个工厂和运营生命周期中进行控制。

根据IEC 62443-2-1标准认证，TÜV NORD 确认安全方案已得到有效实施，且运营技术（Operational Technology, OT）网络安全已系统化、以风险为导向、正式且透明地融入了公司管理。



## IEC 62443-2-1认证的主要特点

- 工业自动化和控制系统安全计划开发和运营的国际公认标准
- 基于风险、面向生命周期的IACS网络风险管理方法
- 清晰的治理结构，明确界定角色和职责（例如，资产所有者、运营技术（OT）运营、维护、服务提供商）
- 整合组织、技术和流程相关的安全措施
- 持续改进流程（如PDCA方法）以可持续地增强网络韧性
- 与现有管理体系，特别是符合ISO/IEC 27001的信息安全管理体系（ISMS）具有良好的兼容性（例如，综合审核、联合治理结构以及文档和风险管理方面的协同作用）

## 认证的目标群体

IEC 62443-2-1认证面向各种行业、规模和成熟度水平的工业控制和自动化环境中的组织。

## 典型的目标群体是以下组织：

- 运营工业、工艺或能源设施  
（例如，制造业、化工、石油与天然气、能源供应、供水/废水处理、交通运输、建筑技术）
- 运营关键基础设施或高可用性生产环境，其中运营技术（Operational Technology, OT）中断会对安全、供应或交付能力产生重大影响
- 已经按照ISO/IEC 27001标准运营信息安全管理体系（ISMS），并希望以符合标准且可验证的方式保护其运营技术（OT）系统
- 必须满足客户、原始设备制造商（OEM）或运营商对于结构化运营技术（OT）安全管理的要求（例如，作为供应合同、运营合同或服务合同的一部分）
- 希望在整个IACS（国际船级社协会）生命周期中，增强其网络韧性、设备可用性和业务连续性

该标准既适用于已建立管理体系（如ISO 9001、ISO/IEC 27001）的组织，也适用于首次希望全面、系统地引入运营技术（Operational Technology, OT）安全性的公司。

## 您通过5个步骤即可获得IEC 62443-2-1认证

根据IEC 62443-2-1的认证流程遵循管理体系审核的成熟结构，并根据组织的规模、复杂性和风险状况进行调整。



询价与报价



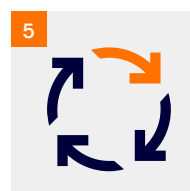
第一阶段审核—  
准备情况评估



第二阶段审核—  
认证审核



认证决定与证书



监督与再认证

## 我们的专业技能助力您取得成功

TÜV NORD 是国际公认且值得信赖的检测与认证服务合作伙伴。我们的专家和审核员具备深厚的专业知识，且通常都担任长期职位。这确保了我们在服务客户时能够保持独立性和中立性，并提供持续性的服务。这给您带来的好处显而易见：我们的审核员将陪伴并支持贵公司的发展，为您提供客观的反馈意见。



Contact

TÜV NORD  
中国上海市静安区康宁路  
288弄5号楼

T +86 21-33196200

[www.tuv-nord.com/cn](http://www.tuv-nord.com/cn)

[gc-mkt@tuv-nord.de](mailto:gc-mkt@tuv-nord.de)