

借助 ISA/IEC 62443 服务, 加强您的网络安全防护

为系统集成商和维护服务提供商提供网络安全解决方案

通过质量保证, 赢得客户的信任

随着工业 4.0 时代的到来, 标准通信协议的应用更加广泛, 连通性也进一步增强, 保护关键工业系统、自动化和控制系统, 使其防范网络安全威胁变得日益迫切。因此, 系统集成商和维护服务提供商必须能够有效降低责任风险, 并确保其制造商的安全水平满足品牌保护的要求。使系统集成和维护达到必要的安全标准, 对于管理供应链的复杂性和满足客户需求至关重要。

IEC 制定了 ISA/IEC 62443 国际标准系列, 旨在保护工业和控制系统防范安全威胁。该系列标准通过明确如何在多个行业中打造安全的电子化工厂、设施和系统, 来降低工业和设施通信网络的安全风险, 并建立自动化和控制系统。

对于工业控制系统 (ICS) 的集成商和控制系统的用户来说, 遵循 ISA/IEC 62443 标准系列是提升品牌保护和增强竞争优势的有效途径。

从组件制造商到系统集成商, 从资产所有者到最终用户, UL Solutions 可以为供应链中的众多参与者提供网络安全合规和咨询服务。

我们服务的行业



离散制造



流程工业



石油和天然气



可再生能源



汽车



发电 (电力)
和配电 (电网)



电气和电子设备



制药

行业面临的网络安全挑战

- 向客户展示安全确认。
- 理解并尽可能降低物联网 (IoT) 与运营技术 (OT) 基础设施的风险。
- 根据安全性对产品和系统进行差异化。
- 确认所需系统和产品的安全性。
- 与现有的未验证系统进行集成。

ISA/IEC 62443 标准系列				
流程工业与离散制造				
制造商		集成商/服务提供商		运营商/所有者
ISA/IEC 62443 4-1	ISA/IEC 62443 4-2	ISA/IEC 62443 3-3	ISA/IEC 62443 2-4	ISA/IEC 62443 2-1

我们的 ISA/IEC 62443 服务可以助力增强对流程和产品的严谨性和网络安全的信心。我们提供针对 ISA/IEC 62443 标准的多方位网络安全咨询、测试和认证服务，以满足您的安全需求。

ISA/IEC 62443 为系统集成商和维护服务提供商带来以下好处



更新和维护系统以达到所需的安全水平



降低责任风险



管理供应链复杂性与风险



根据特定行业的要求来满足客户需求

面向系统集成商和维护服务提供商的关键解决方案

市场介入

随着法规数量不断增加，要求日趋严格，您需要了解相关的法规或要求，知道如何实现合规并持续保持。UL Solutions 为工业应用提供网络安全和符合性评估的专业知识。我们支持您的组织在全球范围内进行市场激活和网络安全规划，助力您开启网络安全之旅。

培训

在我们的互动培训或专门设计的研讨会中，您将学习如何根据 ISA/IEC 62443 标准，针对您的工业控制与自动化系统所面临的安全问题，做出明智的决策。我们可依据您的具体需求，如系统架构设计、风险评估及网络安全政策制定，为您量身打造培训课程。研讨会将深入探讨行业优秀实践，并为您的流程和系统网络安全评估、认证需求及所需投资规划路线图。

技术要求与合规路线图制定研讨会

我们提供互动研讨会和座谈会，助力您将业务需求与技术要求相匹配，为您的系统绘制出一张网络安全路线图。这些会议还会制定合规性路线图，根据不同地区的特性，明确标准的适用性，以及如何在多系统及组件上进行高效实施。

运营技术 (OT) 风险评估

我们可以通过评估威胁可能性，来支持您的工业自动化和控制系统 (IACS) 的安全需求。我们将评估网络资产受损可能造成的严重后果，助力您更深入地拆解目标，以匹配客户对 OT 系统的成熟度需求。我们能够识别与设计的工业自动化和控制系统相关的风险，并由我们的 OT 网络安全专家提供多方位视角，包括基于 ISA/IEC 62443-3-2 的详细风险评估报告。OT 风险评估服务包括：

- 方法概述。
- OT 环境的脆弱性概述。
- 工厂现有状态与安全要求之间的差距分析。
- 针对暴露风险等级的缓解计划。
- 评估现有对策，并提出额外的建议。
- 制定或优化安全程序的路线图。

为 IACS 构建控制系统网络安全管理系统 (CSMS)

我们可以助力您的组织构建 IACS 网络安全管理系统，并按照 ISA/IEC 62443-2-1 要求进行完善。

此服务包含多项内容，主要可分为四大类：

- 风险分析。
- 利用 CSMS 应对风险。
- 监控并改进 CSMS。
- ISO/IEC 27001 和 ISA/IEC 62443-2-1 之间的对应关系。

差距分析

我们将进行一次多方位审核，基于组织的成熟度目标或系统的安全水平，针对 ISA/IEC 62443-2-4 和 ISA/IEC 62443-3-3 要求，评估当前状态与期望状态之间的差异。结果将在差距分析报告中提供，您可以对报告进行定制以便将测试包含在内。

文档审核与支持

我们可以提供以 ISA/IEC 62443 为导向的文档审核，助力您确认所需的成熟度或安全水平。首先，我们会采用四级评价体系来评估所定义流程和技术文档的就绪度情况。然后，我们可以提出与安全相关的文档变更，以支持基本要求和增强功能。最后，在您向审计员提交项目文档前后，我们的团队将提供以下活动的咨询服务：

- 撰写符合性声明的建议。
- 符合性证据。
- 最终文档审核。
- 支持团队弥补差距。
- 助力团队做好准备，应对现场审计问答。

认证

我们可以对系统集成商和维护服务提供商进行评估和认证，以增强工厂所有者和运营商的信心。我们提供不同的评估和认证选项，以助力高效且可持续地满足您的需求。

监督与检查

我们的监督和检查服务可助力验证您是否采取足够的安全措施，以维持您的认证状态。检查结束后，您将获得一份报告，报告中的结果可助力您确定正确的行动方案，以展示成熟度和安全水平达到既定目标。

对于服务提供商和系统集成商而言，符合 ISA/IEC 62443 标准的认证可助力您向广泛的目标市场和客户展示您的安全合规性。

UL Solutions 已依据 IEC 17065 和 IEC 17025 获得 ANAB 认证，可实施 ISASecure 认证流程，并按照 ISA/IEC 62443 标准为工业网络安全认证提供符合 ISASecure 体系的符合性评估。因此，我们有能力作为 ISASecure 认证机构 (CB) 开展网络安全评估。

同时，我们也是 ISA/IEC 62443 下 CB 体系的 CB 测试实验室 (CBTL)。我们的专家能够在 IEC 62443 体系下，针对 ISA/IEC 62443 标准提供网络安全评估与认证服务。CB 体系包括 ISA/IEC 62443 框架中的一些子标准，专门用于评估和认证。

除了 IEC 62443 和 ISASecure 体系，UL Solutions 还推出了网络安全保障计划 (CAP)，并通过该计划颁发由 UL Solutions 签发的 ISA/IEC 62443 认证证书。

最后，我们能够根据您的特定需求进行评估，包括产品特性、预期使用中的网络安全问题、运营商与系统集成商之间的合同要求，也可以基于联邦、州或地区的监管要求，助力制定更稳健的网络安全策略。我们还可以提供其他培训和咨询服务，为安全产品开发、智能生态系统的网络安全以及供应链风险管理提供助力。

如需有关 UL Solutions ISA/IEC 62443 网络安全服务的更多信息，请访问 UL.com/IEC62443。



Safety. Science. Transformation.™

© 2024 UL LLC 保留所有权利
IMS23CS1206271
039.02.0823.EN.CYBzhCN