工业控制系统网络安全防护体系建设研究

周铭浩
航宇救生装备有限公司　湖北　襄阳　441003

摘　要：本文深入研究了工业控制系统（ICS）网络安全防护体系的建设。文章首先概述了ICS的基本组成及在工业生产中的重要性，并分析ICS面临的物理入侵、远程攻击、恶意软件和数据泄露等主要网络安全威胁。提出ICS网络安全设计的四大原则，包括分割网络、路由与过滤、认证与访问控制以及安全更新与漏洞修复。基于这些原则，文章构建了ICS网络安全防护体系，具体涉及网络隔离技术、加密技术的应用、入侵检测系统与防火墙、安全审计与日志记录以及应急响应机制。通过这些措施，旨在提高ICS的网络安全防护能力，确保工业生产的安全与稳定。

关键词：工业控制系统；网络安全；防护体系

1 工业控制系统概述

工业控制系统（ICS，Industrial Control Systems）是现代工业生产与运营的核心，它们集成了计算机技术、自动化技术、通信技术和信息技术，以实现对工业设备的远程监控、控制、数据采集与分析等功能。ICS广泛应用于制造业、能源、交通、水利、农业等多个领域，对于提高生产效率、优化资源配置、保障运行安全具有重要意义。ICS通常由三个主要层次组成：现场控制层、监控层和管理层。现场控制层包括传感器、执行器、可编程逻辑控制器（PLC）等现场设备，它们负责实时采集生产过程中的数据，并根据预设的控制逻辑执行相应的操作。监控层则通过人机界面（HMI）、数据服务器等设备，对现场设备进行集中监控、报警管理和数据分析，为操作人员提供直观的生产状态信息和故障预警。管理层则关注于生产计划的制定、资源调度、成本控制等高级管理功能，通过企业级信息系统与ICS的集成，实现生产流程的全面优化[1]。随着工业自动化和智能化的不断发展，ICS正逐渐从传统的封闭式系统向开放式、网络化系统转变。因此，加强ICS的网络安全防护，构建安全可靠的工业网络环境，已成为当前工业界和学术界共同关注的焦点。

2 工业控制系统网络安全威胁分析

2.1 物理入侵的威胁

物理入侵是指攻击者通过物理手段直接访问或破坏工业控制系统的硬件设备和网络基础设施。这种威胁可能源自未经授权的访问、盗窃、破坏或恶意篡改等行为。攻击者一旦成功入侵，便可能获得对控制系统的直接控制权，进而干扰或破坏生产流程。例如，攻击者可以通过插入恶意硬件、篡改系统配置或破坏关键设备来实施破坏。物理入侵的防范需要强化物理安全措施，如设置门禁系统、安装监控摄像头、实施严格的访问控制等，以确保只有授权人员能够接近和操作控制系统。

2.2 远程攻击的威胁

远程攻击是指攻击者利用网络通信协议、系统漏洞或未受保护的端口，从远程位置对工业控制系统发起攻击。这种威胁可能源自网络钓鱼、恶意软件传播、漏洞利用等手段。攻击者通过远程攻击可以获取系统控制权、窃取敏感数据或注入恶意指令，进而干扰生产运行、造成设备损坏或引发安全事故。防范远程攻击需要强化网络通信安全，如配置防火墙、入侵检测系统（IDS）、实施访问控制列表（ACL）等，以确保网络通信的机密性、完整性和可用性。

2.3 恶意软件的威胁

恶意软件是指具有恶意意图的软件程序，它们可以通过多种途径（如电子邮件、网络下载、U盘等）感染工业控制系统的设备。一旦恶意软件侵入系统，它们可能会执行恶意操作，如破坏数据文件、篡改系统配置、窃取敏感信息等。此外，恶意软件还可能作为跳板，允许攻击者进一步渗透系统，实施更复杂的攻击。防范恶意软件需要采取多层次的安全措施，如安装可靠的防病毒软件、禁用不必要的服务和端口、限制软件安装权限等，以减少恶意软件的入侵风险[2]。

2.4 数据泄露的威胁

数据泄露是指工业控制系统中的敏感数据被未经授权的人员获取或泄露给外部实体。这些敏感数据可能包括生产数据、设备参数、用户信息等。数据泄露不仅可能导致知识产权损失和隐私泄露，还可能为攻击者提供有价值的情报，用于实施进一步的攻击。防范数据泄露需要强化数据加密、访问控制和审计机制。例如，对敏感数据进行加密存储和传输，实施严格的访问控制策略，以及

定期审计系统日志以发现潜在的数据泄露风险。

3 工业控制系统网络安全设计原则

3.1 分割网络原则

分割网络原则，又称网络隔离原则，是工业控制系统网络安全设计的基础。该原则要求将网络划分为不同的安全区域，每个区域根据其功能、数据敏感性和安全需求进行隔离。通过这种方式，可以降低网络攻击的风险，并限制攻击者在系统中的横向移动。在分割网络原则的指导下，工业控制系统通常被划分为多个逻辑或物理上的隔离区域，包括生产控制区、数据采集与监视区、企业管理区等。生产控制区通常是最关键和敏感的区域，包含直接控制工业设备的PLC、传感器和执行器等。这个区域应受到严格的访问控制和物理保护，以避免未经授权的访问。数据采集与监视区则负责收集生产数据并生成报告，该区域需要确保数据的完整性和机密性。企业管理区则负责企业的日常运营和管理，虽然这个区域可能不包含直接控制设备的系统，但仍然需要防范数据泄露和网络攻击；为了实现有效的网络隔离，工业控制系统通常采用防火墙、DMZ（非军事区）、VLAN（虚拟局域网）等技术。防火墙用于限制不同安全区域之间的通信，阻止潜在的恶意流量。DMZ提供了一个缓冲区，允许外部用户访问某些服务而不会直接暴露内部系统。VLAN则通过逻辑上划分网络，实现不同设备之间的隔离，从而降低安全威胁。

3.2 路由与过滤原则

路由与过滤原则要求在网络中实施精细的路由控制和流量过滤，以确保只有合法的、经过验证的流量能够进入工业控制系统。这一原则有助于防止恶意流量渗透系统，保护系统的完整性和安全性。为了实现路由与过滤原则，工业控制系统应配置先进的路由器和交换机，这些设备具备强大的流量管理、过滤和日志记录功能。通过配置ACL（访问控制列表），可以限制特定IP地址、端口或协议的流量通过。另外，还可以部署入侵检测和防御系统（IDS/IPS），这些系统能够实时监测网络流量，识别并阻止潜在的攻击行为。除了基于ACL和IDS/IPS的流量过滤，工业控制系统还可以利用深度包检测（DPI）技术。DPI技术能够分析网络流量的内容，识别出潜在的恶意软件、病毒或钓鱼攻击，从而进一步保护系统免受攻击。

3.3 认证与访问控制原则

认证与访问控制原则是工业控制系统网络安全设计的核心。该原则要求所有访问系统的用户和设备都必须经过身份验证，并根据其权限级别进行访问控制。通过这种方式，可以确保只有经过授权的用户才能访问系统资源，从而降低数据泄露和恶意操作的风险。为了实现认证与访问控制原则，工业控制系统应采用强密码策略、多因素认证技术（如指纹识别、智能卡等）以及基于角色的访问控制（RBAC）模型。强密码策略要求用户定期更换密码，并限制密码的复杂性和重复性[3]。多因素认证技术则提供了额外的安全层，增加了攻击者破解系统的难度。RBAC模型则根据用户的角色和职责分配访问权限，实现了细粒度的访问控制。工业控制系统还应实施定期的审计和审查，以确保访问控制策略的有效性和合规性。审计日志应记录所有访问尝试、成功或失败的登录尝试以及系统配置的更改，以便及时发现和调查潜在的安全事件。

3.4 安全更新与漏洞修复原则

安全更新与漏洞修复原则是工业控制系统网络安全设计的最后一道防线。该原则要求系统运营商定期更新软件和固件，以修复已知的安全漏洞和弱点。通过实施这一原则，可以确保系统始终具备最新的安全补丁和防护措施，从而有效抵御网络攻击。为了实现安全更新与漏洞修复原则，工业控制系统应建立一套完善的更新管理流程。该流程应包括识别需要更新的软件组件、测试更新补丁的兼容性和安全性、制定更新计划和时间表以及执行更新操作。在更新过程中，应确保系统的可用性不会受到严重影响，并采取适当的备份和恢复策略以防止数据丢失。除了定期更新软件和固件外，工业控制系统还应采用漏洞扫描技术；通过定期运行漏洞扫描工具，系统运营商可以及时发现并修复潜在的安全隐患。

4 工业控制系统网络安全防护体系构建

4.1 网络隔离技术

网络隔离技术是工业控制系统网络安全防护的基础。通过将ICS划分为不同的安全区域，并采取相应的隔离措施，可以显著降低安全威胁的扩散风险。网络隔离技术主要包括物理隔离和逻辑隔离。物理隔离是通过物理手段将ICS与其他网络完全断开连接，以确保系统的独立性。这种技术适用于对安全性要求极高的场景，如关键基础设施的控制网络。然而，物理隔离可能限制了系统的可扩展性和灵活性，因此在现代ICS中，逻辑隔离成为更常见的选择。逻辑隔离利用防火墙、DMZ（非军事区）和VLAN（虚拟局域网）等技术，在逻辑上将ICS划分为不同的安全区域，并对各区域之间的通信进行严格的控制和过滤。防火墙是逻辑隔离的核心设备，它可以基于源地址、目标地址、协议类型、端口号等多种因素，控制不同安全区域之间的流量。DMZ提供一个缓冲

区，允许外部用户访问ICS提供的特定服务，而不会直接暴露内部系统。VLAN则通过逻辑上划分网络，实现了不同设备之间的隔离，降低了潜在的安全威胁。

4.2 加密技术的应用

加密技术是保障ICS数据安全的重要手段。通过采用适当的加密算法和协议，可以对ICS中的敏感数据进行加密处理，以防止数据在传输和存储过程中被窃取或篡改。在ICS中，加密技术的应用主要包括传输层加密和存储层加密。传输层加密通过在数据传输过程中使用SSL/TLS等加密协议，确保数据在网络中的安全传输。这种加密方式可以防止攻击者通过窃听、中间人攻击等手段获取敏感数据。存储层加密则是对存储在硬盘、数据库等存储设备上的数据进行加密处理，以防止数据在存储过程中被非法访问。

4.3 入侵检测系统与防火墙

入侵检测系统和防火墙是ICS网络安全防护的重要组成部分。它们能够实时监测和防御外部攻击和内部恶意行为，确保系统的安全性和稳定性。防火墙作为ICS的第一道防线，能够基于预定义的规则库，对进出ICS的流量进行过滤和控制。然而，防火墙的局限性在于它只能基于已知的攻击模式和特征进行防御，对于未知的或变形的攻击可能无法有效识别。因此，入侵检测系统成为防火墙的重要补充。入侵检测系统通过实时监测ICS中的网络流量和系统日志，能够识别并报告潜在的攻击行为。它可以根据预设的安全策略，对异常流量和恶意行为进行报警、阻断或记录。同时，入侵检测系统还可以与防火墙等其他安全设备进行联动，实现对攻击的协同防御。

4.4 安全审计与日志记录

安全审计与日志记录是ICS网络安全防护的重要组成部分。通过定期对系统进行安全审计和记录详细的日志信息，可以发现潜在的安全威胁和漏洞，并为后续的安全分析和事件调查提供依据[4]。安全审计包括对ICS的配置、用户行为、数据完整性等多个方面进行审查。通过审查系统的配置，可以发现潜在的安全配置错误和漏洞；通过审查用户行为，可以发现异常操作和潜在的安全风险；通过审查数据的完整性，可以验证数据的真实性和完整性；日志记录则需要记录ICS中的所有重要安全事件和日志信息。这些日志信息包括用户登录尝试、系统配置更改、异常操作等。通过记录这些信息，可以追踪和分析系统的运行状况，及时发现并处理潜在的安全威胁。

4.5 应急响应机制

在发生安全事件时，能够迅速启动应急响应流程，采取有效的措施进行处置，以减少安全事件对ICS的影响。应急响应机制包括应急响应计划、应急响应团队和应急响应流程三个方面。应急响应计划是ICS网络安全防护的重要组成部分，它规定了在不同安全事件下应采取的应对措施和流程。应急响应团队则由专业的安全人员组成，负责在发生安全事件时迅速启动应急响应计划并进行处置。应急响应流程则包括事件发现、事件分析、措施实施和事件恢复等多个阶段。

结束语

综上所述，工业控制系统网络安全防护体系的建设对于保障工业生产的安全与稳定具有重要意义。在深入研究ICS面临的主要网络安全威胁基础上，提出了有效的网络安全设计原则和防护体系构建措施。随着技术的不断发展和网络攻击手段的不断演变，ICS网络安全防护工作仍需持续加强和创新。未来，将继续关注ICS网络安全领域的最新动态和技术发展，为构建更加安全、可靠的工业网络环境贡献力量。

参考文献

[1]苏红生.刘燕江,李高桥,李明.工业控制系统网络安全防护体系建设研究[J].自动化仪表,2024,45(02):111-115.

[2]李永毅.工业控制系统网络安全防护建设探讨[J].通讯世界,2020,27(03):84-85.

[3]苏红生,刘燕江,李高桥,等.工业控制系统网络安全防护体系建设研究[J].自动化仪表,2024,45(2):111-115.DOI:10.16086/j.cnki.issn1000-0380.2022100036.

[4]徐伟,孔坚,毛庆梅,等.工业控制系统安全现状及应对策略[J].网络安全技术与应用.2021,(9).DOI:10.3969/j.issn.1009-6833.2021.09.066.