 DOI: https://doi.org/10.12345/bdai.v6i5.32050

Industrial control network security risk assessment and hierarchical protection strategy optimization

Jiawei Li Zhixiu Gao

Jinan Sanze Information Security Evaluation Co., Ltd., Jinan, Shandong, 250101, China

Abstract

With the continuous advancement of industrial automation, Industrial Control Systems (ICS) have become deeply embedded in national critical infrastructure, serving as a core driver for the stable operation of modern manufacturing and energy systems. However, their widespread application has also brought numerous cybersecurity risks. This paper focuses on cybersecurity risk assessment for industrial control systems, conducting a comprehensive and systematic analysis. On one hand, it details typical security threats currently faced by ICS networks, such as malware attacks and data breaches, along with existing vulnerabilities like system flaws and improper configurations. On the other hand, by integrating the framework of the graded protection system, it explores adaptive optimization strategies for industrial environments. The aim is to build a cybersecurity defense system better suited to industrial scenarios, enhance ICS network resilience against risks, and ensure the secure and stable operation of national critical infrastructure.

Keywords

Industrial Control Systems; Cybersecurity; Risk Assessment; Graded Protection; Strategy Optimization

工业控制网络安全风险评估及等级保护策略优化

李佳蔚 高志修

济南三泽信息安全测评有限公司，中国·山东 济南 250101

摘 要

在工业自动化水平持续攀升的当下，工业控制系统（ICS）深度嵌入国家关键基础设施，已然成为现代制造业与能源系统稳定运行的核心驱动力。然而，其广泛的应用也带来了诸多网络安全隐患。本文聚焦工业控制系统网络安全风险评估，展开全面且系统的分析。一方面，详细梳理了当前ICS网络面临的典型安全威胁，如恶意软件攻击、数据泄露等，以及存在的脆弱点，像系统漏洞、配置不当等。另一方面，结合等级保护制度框架，深入探讨其在工业环境中的适应性优化策略，旨在构建更贴合工业场景的网络安全防护体系，提升ICS网络应对风险的能力，保障国家关键基础设施的安全稳定运行。

关键词

工业控制系统；网络安全；风险评估；等级保护；策略优化

1 引言

随着新一轮工业革命的持续推进，工业控制系统（Industrial Control System, ICS）作为智能制造、智慧电网、城市基础设施运行的核心枢纽，正朝着高度网络化、信息化与智能化方向发展。特别是在“工业互联网”“智能工厂”“数字孪生”等新兴技术的广泛应用背景下，工业控制网络的边界逐渐模糊，开放性与复杂性显著增强，从而为网络攻击者提供了更多潜在入口。

本文在深入分析工业控制系统网络特征与风险源构成的基础上，构建适应工业场景的多维度风险评估模型，进一步结合我国网络安全等级保护制度，提出具有可实施性的优化策略建议，以期为工业控制网络安全治理提供理论参考与实践支撑。

【作者简介】李佳蔚（1992–），女，中国辽宁营口人，本科，工程师，从事网络安全研究。

2 工业控制网络安全风险识别与评估现状

在工业数字化与智能制造加速推进的背景下，工业控制系统（Industrial Control Systems，简称 ICS）已成为国家关键基础设施的重要组成部分，广泛应用于能源、电力、交通、制造、水利等多个领域。ICS 通过对工业现场的实时监测与精细控制，实现生产效率提升与资源优化配置。然而，其网络架构的开放性与系统耦合性的增强，也使其面临日益严峻的网络安全挑战。深入剖析工业控制系统的结构特征、安全风险源及现有评估方法的适用性，对于构建高韧性、可持续的工业网络安全体系具有重大现实意义。

2.1 工业控制系统网络的结构特征与安全挑战

工业控制系统网络结构呈现多层级、多协议、高耦合

特征。一般分为现场感知层、控制执行层、调度监控层和企业管理层。现场感知层采集生产数据，控制执行层借助 PLC、DCS 等控制设备，调度监控层通过 SCADA 系统、HMI 等集中监控调度，企业管理层集成 MES、ERP 等实现决策管理。这种“纵向整合、横向互联”架构虽保障了信息高效流动，却带来新安全挑战。任一层受攻击，影响会垂直或水平扩散，造成“多点触发、系统连锁”破坏。

ICS 系统多采用专有通信协议，因重功能与实时性，缺乏身份认证和加密机制，难抵御网络威胁。老旧设备无法支持现代加密与补丁更新，安全防护薄弱。运维人员网络安全意识与培训滞后，易出现配置不当等问题。而且设备供应链管理缺乏完整安全评估流程，第三方组件存在隐患，进一步扩大了攻击面。

2.2 典型安全威胁与风险源分析

随着攻击技术演化与攻击目标转向工业系统，工业控制网络所面临的威胁类型日益复杂，呈现出精确化、隐蔽化、长期化的趋势。综合现实攻击案例与行业报告，当前 ICS 主要面临以下几类典型威胁：

最具代表性的案例为 Stuxnet 蠕虫，它通过 USB 等可移动介质植入目标系统，利用 Windows 与西门子 PLC 系统的多个零日漏洞，进行精确的物理层设备破坏。这种结合 IT 漏洞与 OT 协议的“跨域攻击”极具隐蔽性与破坏力。

工控环境中的账户管理往往松散，权限设置不合理，运维人员可能使用默认口令、共享账户等做法，使攻击者容易窃取或冒用权限。此外，操作失误（如误配置、防火墙规则错误）也可能引发服务中断或数据丢失。

随着远程运维与 VPN 接入的普及，攻击者可利用 RDP、远程桌面服务等方式绕过边界防护，实施控制渗透。同时，通过利用工业设备供应商的固件更新系统、后门程序等路径，也能隐蔽地植入恶意代码，形成供应链攻击。

攻击者通过截获或篡改控制指令，诱使设备产生误动作，如误启动、停止关键流程设备，严重时可能导致爆炸、泄漏等事故，直接危及人员安全与环境稳定。

这些风险不仅针对信息资产，更可能波及实体工业系统，引发“数字攻击—物理破坏”的复合型危害，对国家关键基础设施构成极大威胁。

2.3 现有风险评估模型的适用性分析

工业控制系统安全防护依赖科学风险评估机制来识别薄弱环节与制定策略。当下常用评估方法有静态漏洞扫描，能检测设备和服务已知漏洞；攻击路径分析，借助攻击图建模模拟潜在攻击路径评估被攻破可能；资产优先级评估，依资产业务重要性与可替代性确定防护优先级。但这些方法在工业控制系统环境有局限，对动态行为适应性差，传统静态模型难反映系统不同状态下的脆弱点与攻击面变化；缺乏系统依赖关系建模，无法捕捉设备间复杂依赖结构；忽略业务连续性与韧性评估，难以指导长期安全策略制定。所以，要构建更具针对性的风险评估框架，需多维度整合技术漏洞等因素，具备动态建模能力支持系统行为模拟，以业务驱动导向量化风险对生产与安全目标的影响。像引入“网络 - 物理 - 组织”三层集成建模机制，输出动态风险态势图，助力决策者精准部署防护资源，实现安全防护转变。

3 等级保护制度下工业控制网络的适应性挑战

3.1 我国网络安全等级保护制度框架概述

网络安全等级保护制度是我国关键信息基础设施防护的基本制度依据。自《中华人民共和国网络安全法》实施以来，等级保护 2.0 体系逐步完善，其核心在于将信息系统按安全保护等级分为一至五级，依据“谁运营、谁负责”的原则，落实技术防护与管理措施。

该制度为工业控制系统提供了基础性的安全治理标准框架，但其原始设计更侧重于信息系统，在面对控制网络时存在一定适配性偏差。例如，部分通用安全策略（如强制终端隔离、密码策略）在工业现场中难以直接落地，需结合控制系统运行特性加以调整。

3.2 等级保护制度在工业系统中的实施困境

工业控制系统等级保护在实际执行中面临诸多难题。一方面，安全等级划分不够明晰，因其涵盖物理设备、数据通信和信息系统等多个层级，系统边界难以精准界定，对应的等级也就无法明确。另一方面，策略落地困难重重，像安装杀毒软件等技术措施，在嵌入式控制器里无法兼容。此外，现有的测评指标适配性欠佳，多侧重信息系统通用指标，缺乏对工业控制相关特性的评估。

3.3 工业控制环境下的等级保护优化需求

为增强等级保护制度对工业控制系统（ICS）的适配与实效，需制度、标准、执行层面协同发力。制度上，贴合 ICS“控制优先、实时敏感、物理耦合”特性，明确差异化安全管理要求；标准方面，探索“通用 + 行业扩展 + 场景细化”分层路径，定制测评指标与技术规范；执行中，强化测评流程实操性，配套专业工具与试验平台，推动制度落地，提升保障能力。

4 工业控制网络安全风险评估模型构建

4.1 资产梳理与关联分析：奠定评估模型基础架构

工业控制系统涵盖众多资产，从硬件设备如 PLC 控制器、传感器、执行器，到软件系统包括操作系统、控制程序、通信协议等。全面且精准地识别这些资产是构建风险评估模型的首要任务。通过自动化工具与人工排查相结合的方式，详细记录资产的型号、版本、位置、功能等关键信息。

构建资产关联图谱至关重要，它能清晰呈现资产之间的依赖关系和交互逻辑。例如，某个传感器采集的数据会传输给特定的 PLC 控制器进行处理，而控制器的输出又会影

响执行器的动作。明确这些关联后，当某一资产出现安全风险时，就能迅速判断可能波及的范围，为后续的风险评估提供全面的数据支撑，确保模型能准确反映系统的实际安全状况。

4.2 威胁情报融合与攻击模拟：精准刻画潜在安全威胁

整合多源威胁情报是提升评估模型准确性的关键。收集来自安全厂商、行业报告、开源社区等的威胁信息，涵盖已知的漏洞、恶意软件特征、攻击手法等。将这些情报与工业控制系统的资产信息进行匹配，筛选出对系统有潜在威胁的内容。

基于攻击图（Attack Graph）算法开展攻击模拟，以图形化的方式展示攻击者可能利用的漏洞和采取的路径。从系统的初始入口点出发，结合资产的脆弱性和威胁情报，逐步推导攻击者可能达到的目标节点。通过模拟不同的攻击场景，能够全面了解系统面临的潜在威胁，提前发现可能被攻击者利用的薄弱环节，为制定针对性的防护策略提供依据。

4.3 脆弱性深度评估与量化：确定风险关键影响因素

对工业控制系统资产进行深入的脆弱性评估是模型构建的核心环节。采用专业的漏洞扫描工具对硬件设备和软件系统进行全面检测，发现存在的安全漏洞。同时，结合人工审计的方式，对系统的配置、权限管理、访问控制等方面进行细致检查，识别可能存在的安全风险。

对检测到的脆弱性进行量化评估，考虑漏洞的严重程度、利用难度、影响范围等因素，为每个脆弱性赋予相应的风险值。通过量化评估，能够清晰地比较不同脆弱性对系统安全的影响程度，确定哪些是需要优先处理的关键问题，使风险评估更加科学、客观，为后续的风险处置提供明确的指导。

4.4 风险综合计算与可视化呈现：构建闭环安全治理机制

综合资产、威胁、脆弱性等多方面因素，运用合适的风险计算方法，如层次分析法、模糊综合评价法等，计算工业控制系统的整体安全风险值。将计算结果与预设的风险等级标准进行对比，确定系统当前所处的风险等级。

通过可视化技术将风险评估结果以直观的图表、报表等形式呈现出来，使企业管理者和技术人员能够快速了解系统的安全状况。基于评估结果，制定针对性的安全加固措施，如修复漏洞、优化配置、加强访问控制等。同时，建立持续监测和定期评估的机制，根据系统变化和新的威胁情报及时更新评估模型，形成闭环的安全治理机制，不断提升工业控制系统的安全防护能力。

5 等级保护策略在工业控制系统中的优化应用

为了实现等级保护在工业控制系统中的有效落地，应从以下几个维度开展优化设计：

通过物理隔离与逻辑划分相结合方式，实现办公区与控制区、管理层与现场层的网络分区；引入零信任架构原则，实施最小权限访问控制，强化边界防护、终端接入与行为监测能力，阻断横向攻击路径。

针对控制系统对可用性与连续性的高要求，应在关键节点部署冗余控制单元、备份通信链路与多路径容灾机制，提升系统容错能力。同时引入基于策略的自动化故障转移与业务恢复系统，确保安全事件发生时的快速响应与恢复。

构建面向 Modbus、OPC、S7 等工业协议的深度解析引擎，实现对指令层级的异常检测与行为分析。结合态势感知系统部署安全事件监测平台，提升对异常行为的检测、追踪与取证能力，为后续溯源与响应提供支持。

6 结语

工业控制系统作为国家关键基础设施的重要组成部分，其网络安全问题已成为影响国家安全与社会稳定的重要因素。传统 IT 安全理念与工具难以直接适用于工业控制场景，构建面向工业特性的风险评估体系与等级保护优化策略已迫在眉睫。本文在系统梳理工业控制网络特征与典型安全威胁基础上，构建了多维度动态风险评估模型，并结合我国等级保护制度提出了优化路径建议。研究表明，基于资产分级、路径建模与行为识别的综合评估机制，能够显著提升风险识别的精准度；而差异化、行业化的等级保护策略体系，是提升工业控制网络安全治理能力的制度保障。

未来，应进一步加强标准体系建设与跨部门协同，推动安全技术与工控系统融合创新，构建“动态感知、防御联动、持续优化”的智能防御体系，助力我国工业系统迈向本质安全的新时代。

参考文献

[1] 林宝晶,刘江.聚焦专项领域“铁三角”，打造网络安全一体化[J].军民两用技术与产品,2024,(12):44-53.

[2] 伍浩松,杨鹏.英国智库发布民用核设施网络安全报告[J].中国核工业,2024,(12):17-19.

[3] 奈姆·艾力赫瑞克,张禹.网络安全维护与隐私权保护的平衡性建构研究——基于数字时代法律与道德的双重考量[J].数字法学评论,2024,(02):223-251.

[4] 高松涛.新时代病毒防护技术在计算机网络安全中的运用[J].木工机床,2024,(04):35-39.

[5] 朱远.面向融合媒体的网络安全保障体系研究[J].现代电视技术,2024,(12):80-83.