工程与管理科学
Engineering and Management Science
第 8 卷◆第 2 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

工业控制系统网络安全防护研究

苏利
广西诺远科技有限公司　530022

DOI：10.32629/ems.v8i2.18518

［摘　要］工业控制系统作为关键基础设施的核心支撑，其安全稳定运行直接关系工业生产连续性与公共安全。随着 OT/IT 深度融合与数字化转型推进，系统面临协议原生缺陷、边界渗透、定向攻击与内部管理漏洞等多重安全挑战，传统防护模式已难以适配开放互联环境下的风险特征。本文聚焦工业控制系统网络安全的核心矛盾，深入剖析威胁传播机理与脆弱性根源，梳理不同层级安全风险的耦合关联，明确防护体系构建的核心逻辑与关键维度。研究结果为理解工控系统安全本质、优化防护架构提供理论支撑，对提升关键工业领域安全防护能力、保障国家基础设施安全具有重要实践价值。

［关键词］工业控制系统；网络；安全防护

引言

工业控制系统是现代工业生产的“神经中枢”，广泛应用于能源、化工、智能制造等关键领域，是推动工业现代化的核心技术支撑。然而，数字化、网络化转型在提升生产效率的同时，也打破了传统工控系统的封闭性，使原生安全缺陷被持续放大，OT/IT 融合引发的边界模糊、恶意代码专业化、人员操作失范等问题交织叠加，安全风险呈现跨域扩散、精准打击的复杂态势。当前，工控系统安全防护仍面临技术适配不足、风险认知不深、防护逻辑滞后等问题，难以应对新型网络威胁的冲击。因此，开展工控系统网络安全防护研究，厘清威胁与脆弱性的内在关联，构建科学有效的防护逻辑，对筑牢工业安全防线、保障国民经济平稳运行具有重要现实意义。

一、工业控制系统概述

工业控制系统（ICS）是支撑现代工业生产运行的核心技术体系，是融合硬件设备、软件系统与通信网络的复杂集成平台，被誉为工业生产的“神经中枢”。它通过对工业现场的设备状态、生产流程、环境参数进行实时监测、精准控制与智能调度，实现生产过程的自动化、高效化与安全化，广泛应用于能源、化工、冶金、智能制造、交通运输、水利水电等关键工业领域。其核心构成包括数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）、远程终端单元（RTU）等关键子系统，以及传感器、执行器、工业网络等基础硬件，形成“感知-传输-决策-控制”的闭环运行机制。在功能层面，工业控制系统不仅能替代人工完成高温、高压、高风险环境下的重复作业，降低人为误差与安全隐患，还能通过数据分析与算法优化，实现资源消耗最小化、生产效率最大化与产品质量稳定化。随着工业 4.0 与数字化转型的推进，传统工业控制系统正加速与工业互联网、人工智能、边缘计算等新技术融合，从封闭的本地控制模式向开放互联的智能化系统演进，具备了远程运维、预测性维护、柔性生产等新能力。作为国家关键基础设施的重要组成部分，工业控制系统的稳定性、安全性与智能化水平，直接关系到工业生产的连续性、国民经济的平稳运行以及公共安全，是衡量一个国家工业现代化水平的核心标志之一。

图一　工业控制系统核心构成与运行机制图

二、工业控制系统网络安全威胁与脆弱性分析

（一）协议与设备的原生脆弱性

工业控制系统的核心通信协议与硬件设备存在先天性安全缺陷，构成系统安全的底层隐患。多数传统工控协议设计时仅侧重实时性与兼容性，未纳入安全防护机制，Modbus、OPC 等主流协议采用明文传输模式，控制指令、工艺参数等敏感数据可被直接嗅探解析，且缺乏身份认证与数据完整性校验，攻击者可轻易篡改报文或伪造指令。同时，PLC、SCADA、RTU 等核心设备普遍存在“技术债务”，大量运行十年以上的老旧设备因担心影响生产连续性，长期未进行固件更新与漏洞修补，导致高危漏洞持续暴露。部分设备出厂时固化的默认密码、开放端口未被及时修改，成为攻击者无需复杂技术即可利用的入侵入口，这些原生缺陷在数字化转型中被持续放大，形成难以根治的安全短板。

（二）OT/IT 融合引发的边界渗透风险

工业 4.0 推动的 OT 与 IT 深度融合，打破了传统工控系统的物理隔离边界，使安全风险呈现跨域扩散态势。为实现远程监控、数据共享与一体化管理，生产网与办公网、甚至互联网直接连通，但多数系统未进行科学的安全域划分，缺乏有效的边界访问控制策略。攻击者可利用企业 IT 网络的薄弱环节作为跳板，通过 VPN 漏洞、钓鱼攻击等方式突破边界防护，再横向移动至工控核心网络。此外，工业无线技术的广泛应用、移动运维终端的接入，进一步扩大了攻击面，无线通信信号易受窃听与中间人攻击，而缺乏严格准入控制的接入设备，可能成为携带恶意代码的“载体”，导致安全威胁从 IT 域快速渗透至 OT 域，引发生产系统瘫痪[1]。

（三）外部定向攻击与恶意代码威胁

工业控制系统作为关键基础设施的核心组成，已成为各类网络攻击组织的重点目标，攻击手段呈现专业化、精准化特征。攻击者针对能源、化工、智能制造等关键领域，开发专门针对工控设备的恶意代码，包括 PLC 蠕虫、工业勒索软件等，这些恶意代码可绕过传统 IT 安全防护工具，直接攻击控制设备的固件与控制逻辑。部分攻击采用“低门槛、高影响”的模式，通过公开网络搜索引擎扫描暴露的工控设备，利用已知漏洞或默认凭证发起攻击，篡改生产参数、触发虚假警报甚至中断生产流程。更有高级持续性威胁通过供应链植入恶意固件，或利用 AI 驱动的自动化工具生成畸形协议报文，短时间内瘫痪大量老旧设备，此类攻击不仅造成直接经济损失，更可能引发公共安全风险。

（四）内部管理与人员操作风险

内部管理漏洞与人员行为失范是工控系统安全的重要隐患，其隐蔽性强、防范难度大。多数企业未建立完善的安全管理制度，核心设备的操作权限划分模糊，最小权限原则未落实，存在多人共用账号、高权限账号长期不更换密码等问题。运维人员安全意识不足，违规使用移动存储介质、随意接入外部设备的行为频发，可能导致病毒感染或数据泄露。第三方运维人员在开展设备维护时，缺乏全程安全审计与行为监控，存在恶意操作或意外泄露敏感信息的风险。此外，操作人员的误操作也可能引发严重后果，如错误修改工艺参数、误发控制指令等，而缺乏实时操作监测与快速回滚机制，会导致小失误迅速扩大为生产安全事件，凸显内部管理与人员管控的重要性[2]。

三、工业控制系统网络安全防护体系设计

（一）底层安全加固：协议与设备全生命周期防护

底层安全加固是工控系统防护的根基，需针对协议原生缺陷与设备“技术债务”构建全生命周期防护机制。在协议安全方面，对 Modbus、OPC 等传统明文协议进行加密改造，采用 TLS1.2 及以上版本实现通信加密，结合 AES-256-GCM 算法保障数据传输完整性与保密性，同时通过协议网关部署功能码白名单，禁用高危写操作功能码，仅允许合法控制指令通行。针对设备安全，建立固件安全管理体系，在设备选型阶段优先选用通过安全认证的产品，部署前进行固件完整性校验，运行期间通过硬件安全模块（HSM）存储加密密钥与数字证书，防止固件被篡改[3]。

漏洞管理实施“评估-加固-验证”闭环流程，依托国家级漏洞共享平台实时获取漏洞信息，对老旧设备制定差异化加固方案，无法直接打补丁的设备通过网络隔离、流量过滤等补偿措施降低风险。同时关闭设备不必要的端口与服务，修改默认账号密码，采用 X.509 数字证书或预共享密钥（PSK）实现设备双向身份认证，从源头阻断利用原生脆弱性发起的攻击，确保底层硬件与通信协议的安全可控。

（二）边界防护升级：OT/IT 融合下的立体隔离体系

OT/IT 深度融合打破了工控系统传统隔离边界，边界渗透风险陡增，需构建“分区分域+精准管控”的立体防护体系。依据 Purdue 模型，可将工控网络清晰划分为设备层、控制层、监控层及企业层，通过工业防火墙、网闸等专用设备实现域间物理与逻辑双重隔离，严格限定跨域通信权限，从架构上阻断威胁横向扩散路径[4]。

在工业控制网与办公网、互联网的连接节点，部署具备工业协议解析能力的深度包检测设备，精准识别 Modbus、OPC 等协议中的畸形报文与异常流量，同时果断阻断 HTTP、FTP 等高风险通用服务的非法访问请求，筑牢边界第一道防线。针对无线接入与远程访问场景，工业无线网络需关闭 SSID 广播，采用 WPA3 加密及设备身份认证机制，防范信号窃听与违规接入。远程运维必须通过 IPsecVPN 构建专属安全通道，结合双因子认证与最小权限授权机制，严格管控访问范围与操作时长，所有远程操作均需全程日志审计。引入零信任架构打破“内部可信”误区，对所有接入设备与用户实施持续身份验证和权限评估，践行“永不信任、始终验证”原则，有效遏制威胁跨域渗透，保障 OT/IT 融合环境下的边界安全。

（三）主动防御构建：智能检测与威胁精准管控

面对专业化、精准化的外部攻击，需建立“监测-识别-响应-溯源”的主动防御体系，提升威胁发现与处置能力。部署具备工业协议深度解析能力的入侵检测系统（IIDS），结合基于行为分析与机器学习的检测模型，自动识别批量修改参数、非工作时间异常操作等攻击行为，实现对已知威胁与零日攻击的精准检测。针对恶意代码威胁，在主机端部署工业专用防病毒软件与应用白名单系统，仅允许授权软件运行，同时定期对 PLC 配置文件、控制逻辑进行备份，防范勒索软件加密破坏。

构建威胁情报驱动的防御机制，整合行业攻击特征库与自身安全日志数据，通过安全运营中心（SOC）进行集中分析，提前预判攻击趋势。在网络边界部署工业蜜罐系统，诱捕攻击行为并提取攻击特征，实现威胁情报闭环更新。针对关键业务系统采用拜占庭容错（BFT）协议或三模冗余（TMR）架构，确保部分节点被攻陷时系统仍能正常运行，同时通过安全编排自动化与响应（SOAR）技术，实现攻击告警、流量阻断、设备隔离等操作的自动化响应，缩短攻击处置时间[5]。

（四）管理体系完善：人员与全流程安全管控

夯实内部管理是筑牢工控系统安全防线的核心，需构建“人员-流程-供应链”全维度防护体系。制度层面，要建立健全工控安全管理制度，明确资产管理责任主体，通过普查梳理含 PLC、SCADA 服务器等核心资产清单并分级保护。账户权限实行精细化管控，遵循最小权限原则，按岗位分配操作权限，及时禁用过期及冗余权限，每季度开展权限审计，防范权限滥用与泄露风险。

人员管理实施分层培训，为运维人员强化漏洞修复、应急处置等技能，对一线操作人员侧重安全规范与风险识别培训。规范移动存储介质使用，执行“专人管、先审批、必查杀”流程；参数修改、设备启停等敏感操作严格双人复核，确保过程可追溯。第三方运维需在协议中明确安全责任，运维前核查资质，运维中全程监控留痕，操作后立即回收临时权限，杜绝权限遗留问题。应急响应体系需闭环管理，制定三级应急预案，明确上报流程、责任分工与资源调配机制，每半年开展实战演练，模拟勒索软件攻击等场景提升处置能力。供应链安全延伸至全环节，设备采购、软件开发等环节均签订安全协议，明确供应商责任；自主研发软件需通过静态代码分析、渗透测试等检测，确保从源头到运维全生命周期安全可控，彻底堵住内部风险漏洞。

结语

综上所述，工业控制系统网络安全防护是一项覆盖技术、管理、生态的系统性工程，其核心在于平衡开放互联与安全可控的内在需求。本文通过对工控系统安全威胁与脆弱性的深度剖析，明确了防护体系需围绕底层加固、边界管控、主动防御与管理优化形成协同合力。研究表明，只有立足工控系统“实时性、可用性优先”的核心特征，精准匹配风险场景与防护手段，才能实现安全与生产的动态平衡。未来，随着人工智能、零信任等新技术的深度应用，工控系统安全防护将向智能化、自适应方向演进。持续深化相关研究，完善防护理论与实践体系，对推动工业数字化转型安全落地、保障关键基础设施可持续运行具有长远意义。

[参考文献]

[1]石永杰，于慧超，吕峰，等.工业控制系统网络安全的主动防御技术研究与实践[J].信息技术与网络安全,2020,39（4）：13-18.

[2]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.

[3]赖金志.基于 PDCA 循环的工业控制系统网络安全管理研究与实践[J].电脑与电信，2021（11）：12-15.

[4]辛耀中.重要工业控制系统网络安全防护体系[J].信康安全研究，2022，8（6）：2-10.

[5]蒲永杰.工业控制系统网络安全防护措施的研究[J].设备管理与维修，2022（11）：1-5.