 DOI: https://doi.org/10.12349/iser.v7i2.9254

The security interconnection mechanism and implementation scheme of industrial control networks and public networks

Yu Zhang

Guizhou Tobacco Company, Guiyang Branch, Guiyang, Guizhou, 550002, China

Abstract

With the advancement of industrial intelligence, industrial control networks are breaking away from the closed structure through public networks such as the Internet and 5G, enabling efficient applications such as remote operation and data sharing. However, the fundamental differences in architecture and transmission characteristics between the two have given rise to four major security risks: boundary penetration, protocol flaws, equipment operation and data leakage, which seriously threaten production stability and the security of national critical infrastructure. Therefore, this paper builds a "five-in-one" security interconnection mechanism of "boundary isolation + identity authentication + protocol protection + data encryption + behavior auditing", constructing a full-chain protection system from five core dimensions. At the same time, it designs a three-layer implementation scheme of "edge-end-cloud", through boundary protection deployment, equipment protocol modification, security platform establishment and management system support, to form "technology + management" dual guarantees. Practical applications have shown that this mechanism and scheme are in line with the requirements of industrial scenarios and can effectively solve the core security problems of interconnection.

Keywords

Industrial control network; Public network; Security interconnection; Boundary protection; Protocol parsing

工业控制网络与公共网络的安全互联机制及实现方案

张煜

贵州省烟草公司贵阳市公司，中国 · 贵州 贵阳 550002

摘　要

随着工业智能化推进，工业控制网络正通过互联网、5G等公共网络打破封闭格局，实现远程运维、数据共享等高效应用。但两者在体系架构、传输特性等方面的本质差异，催生了边界渗透、协议缺陷、设备运维及数据泄露四大安全风险，严重威胁生产稳定与国家关键基础设施安全。为此，本文搭建“边界隔离+身份认证+协议防护+数据加密+行为审计”的“五位一体”安全互联机制，从五大核心维度构建全链条防护体系。同时设计“端－边－云”三层实现方案，通过边界防护部署、设备协议改造、安全平台搭建及管理制度配套，形成“技术+管理”的双重保障。实际应用表明，该机制与方案贴合工业场景需求，能有效破解互联核心安全难题。

关键词

工业控制网络；公共网络；安全互联；边界防护；协议解析

1 引言

新一代信息技术与制造业深度融合，工业控制系统正逐步跳出传统封闭运行框架。它借助互联网、5G 网络等公共网络，实现跨地域远程运维、数据共享分析及云端协同管控等新型应用。这一互联模式为工业企业带来诸多利好，既能提升生产效率、优化运维成本，还能推动决策向智能化升级[1]。不过，这也让工控网络暴露在公共网络的复杂威胁中，彻底打破了传统工控系统“物理隔离即安全”的防护逻辑。实际应用中，工控设备固有漏洞、协议安全缺陷、边界防护薄弱、第三方运维隐患等问题愈发凸显，严重威胁国家关键基础设施安全与工业生产稳定。构建科学完善的安全互联机制、设计适配工业场景的实现方案，已是工业互联网发展的迫切需求。因此，本文将对工业控制网络与公共网络的安全互联机制及实现方案展开分析。

【作者简介】张煜（1987–），中国贵州贵阳人，硕士，工程师，从事网络安全研究。

2 工业控制网络与公共网络的特性差异及互联风险

2.1 核心特性差异

工业控制网络与公共网络在设计目标、体系架构、传输内容上有着本质不同，这种设计差异直接埋下了互联安全的隐患。从体系架构来看，工控网络多采用纵向高度集成的分层架构，覆盖现场控制层、监督控制层、生产执行层。主

站与终端节点是严格的主从关系，节点功能单一，对稳定性的要求却极高。公共网络则相反，采用扁平对等架构，节点具备通用计算能力，支持动态接入和数据交互，架构设计优先保障灵活性而非稳定性。再看传输特性，工控网络核心传输遥测、遥信、遥控、遥调“四遥信息”——即设备状态监测、指令下发等关键数据，对实时性、可用性要求严苛，允许适度丢包但绝禁恶意篡改。公共网络以文本、图像等通用数据传输为主，侧重提升传输效率和带宽利用率，对实时性要求相对宽松，核心防护重点是防范数据泄露与窃取。设备及生命周期层面差异也明显。工控设备生命周期长达 5 至 10 年，软硬件升级难度大，默认口令、未修复漏洞等问题普遍存在。公共网络设备迭代周期短，可定期更新安全补丁、优化防护策略，安全适配能力更强。

2.2 主要互联安全风险

工控网络与公共网络互联主要存在四大安全风险如图 1 所示。

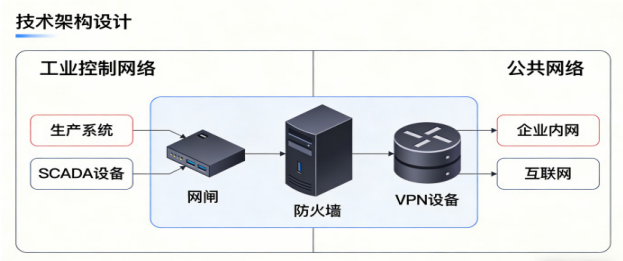

图 1 工控网络与公共网络互联安全风险示意图

2.2.1 边界渗透风险

工业控制网络与公共网络互联后，边界就成了攻击者的首要目标。不少企业因数据交互便捷，要么不部署有效边界防护设备，要么用传统 IT 防火墙替代工业专用款，根本挡不住针对工控协议的攻击。攻击者可先通过公共网络入侵企业管理网，进而横向渗透至工控网络——比如借助 MES 系统攻击 OPC 服务器，篡改生产参数引发设备异常。

2.2.2 协议安全缺陷风险

主流工控协议设计之初以功能实现为核心，未将安全性纳入首要考量，存在明文传输、缺乏身份认证、功能码易滥用等固有缺陷。Modbus 协议采用明文传输模式，无内置加密与身份认证机制，攻击者可通过 Wireshark 等抓包工具直接截获设备状态数据与控制指令，甚至利用功能码滥用漏洞——如未经授权使用功能码 06、16 篡改生产参数。某水处理厂曾因 Modbus 协议未做防护，被攻击者篡改水泵转速指令，导致供水压力异常。OPC 协议基于 Windows 平台开发，继承了 Windows 系统的漏洞隐患，且客户端常使用 admin/admin、root/root 等通用账号密码，极易引发越权访问。此外，OPC 协议的数据传输未做默认加密，攻击者可通过中间人攻击截获生产配方、工艺参数等核心数据。据国家工业信息安全漏洞库（CNVD）统计，2024 年上半年涉及 OPC 协议的漏洞报告达 87 起，其中高危漏洞占比 42%。

3 工业控制网络与公共网络的安全互联机制构建

工业控制网络与公共网络的安全互联机制构建，如图 2 所示。

图 2 “端 – 边 – 云”三层安全互联总体架构图

3.1 边界隔离机制

边界隔离是工控与公共网络安全互联的基础，实际防护中需采用“纵向隔离 + 横向分区”的双重策略，以此搭建起多层次的边界防护体系。纵向防护上，要在工控网络与公共网络、企业管理网之间部署工业网闸、工业防火墙等专用防护设备，彻底切断网络间的直接连接，依靠专有数据块“摆渡”完成数据交换，同时严禁公共网络直接访问工控核心设备。横向管控方面，需按业务重要性将工控网络划分成核心控制区、监控区等不同安全区域，落实分区分域管控，严格限制区域间的数据流向与访问权限。而面对无线互联的特殊场景，还需制定严格接入控制策略，关闭 SSID 广播、做无线设备双向身份认证，通过工业级 VPN 构建加密链路，限制接入设备权限，防范非法接入与信号截获攻击。

3.2 身份认证与权限管控机制

要搭建覆盖设备、用户、应用三层面的全维度身份认证体系，从根源上确保互联主体可信。面向设备端，为工控设备、网关、服务器等分配唯一身份标识，设备接入网络时完成双向认证，直接禁止未授权设备接入。针对用户群体，采用“账号密码 + 双因子认证”模式，对管理员、运维人员等实施分级授权，严格遵循最小授权原则，禁用冗余默认账户，及时清理过期账户。聚焦跨网络应用，对 OPC、MES 等应用做精细化权限管控，细化操作权限粒度，限定访问与数据操作范围，防范越权访问与恶意操作。除此之外，还需建立权限动态调整机制，根据业务需求、人员岗位变动及时更新权限配置。

3.3 协议安全防护机制

面对工控协议先天设计短板，可搭建“协议解析 + 过滤审计 + 漏洞防护”全流程防护体系（如图 3 所示）。优先部署工业协议安全网关，借助深度协议解析技术对 Modbus、IEC104 等主流协议做四维检测，过滤非法报文与异常指令，比如校验报文头格式、拦截未授权功能码 [2]。针对 OPC 这类高危协议，要升级至 OPCUA 标准，用 AES-256 加密和 X.509 证书认证替代通用账号密码，再配专用网关实现协议隔离。漏洞管理方面，定期用 Nessus 等工具扫

描，同步 CNVD 漏洞库信息；可修复漏洞选停机时段打补丁，老旧设备就用工控 IPS 旁路防护，像某电厂曾靠这招阻断 CVE-2023-38148 漏洞攻击，拦截率达 98%。

图 3 协议安全防护技术流程图

3.4 数据安全传输机制

要围绕工控数据采集、传输、存储、使用全生命周期，搭建专属的数据安全防护体系。传输环节，用商用密码算法加密工控数据，结合 IPsec、SSL 构建加密传输通道，保障公网传输的机密性与完整性；实时控制数据需优化加密算法，适配毫秒级时延要求，避免干扰生产流程。数据分类分级上，先梳理工控数据资产，区分核心与重要数据实施差异化防护，核心生产数据必须境内存储，确需出境的依法开展安全评估；存储环节则采用加密存储、冗余备份技术，定期开展备份恢复测试，保障数据可用性。

4 安全互联实现方案设计

4.1 方案总体架构

采用“端 - 边 - 云”三层架构实现工控与公共网络的安全互联，现场端聚焦设备安全接入，边缘层负责边界防护与数据预处理，云端做集中管控与智能分析，各层级协同联动，搭建全链条安全防护体系。现场端改造 PLC、传感器等工控设备，关闭冗余接口服务，设唯一身份标识，装终端防护软件，严禁违规接公网。边缘层部署工业网闸、防火墙等设备，实现边界隔离、协议解析等功能，过滤异常数据与攻击报文。云端搭建工控 SOC，集成设备管理等功能，实时监控安全状态、预警风险。

4.2 关键环节实现路径

4.2.1 边界防护系统部署

在工控网络与企业管理网间部署工业网闸，采用“2+1”硬件架构实现物理隔离，仅允许授权生产数据按规则摆渡传输，保障毫秒级时延适配工控实时性需求。企业管理网与公共网络间，部署工业防火墙与 VPN 设备，防火墙配置工控协议防护规则拦截攻击，远程运维需经 VPN 加密通道接入，完成“账号密码 + 硬件令牌”双认证，严格限定访问范围与授权时长，操作全程审计。5G 无线场景部署工业级 5G 网关，支持 SIM 卡认证与 AES-256 加密，关闭冗余服务，通过网络切片隔离工控与公共业务，配置时延≤ 20ms、丢包率＜ 0.01% 的 QoS 参数，契合工业生产传输要求。

4.2.2 工控设备与协议安全改造

对工控设备开展安全加固，修改默认口令、关闭冗余接口与服务，安装设备安全管理插件，实时监测设备运行状态和漏洞情况 [3]。部署工业协议安全网关，解析过滤 Modbus、IEC104 等协议，拦截非法功能码与异常报文，封装 OPC 协议实现身份认证与加密传输。引入应用软件白名单技术，限定授权软件在工控主机运行，定期病毒查杀、补丁更新，防范勒索软件等恶意程序感染。

4.2.3 安全运营平台搭建

搭建工控安全运营中心（SOC），集成核心模块。资产盘点采用“主动扫描 + 被动监听”，动态生成设备型号、协议版本清单。漏洞管理关联 CNVD 工控漏洞库，实现扫描、评估、修复闭环。嵌入 AI 异常检测模型，精准识别协议异常、参数篡改等风险。集中存储审计日志，支持多维度检索追溯，联动应急响应模块快速处置安全事件。

4.2.4 管理制度体系建设

配套建立完善的工控安全管理制度，覆盖资产管理、配置管理、供应链安全等多方面。明确资产管理责任部门，建立工控资产清单并定期核查。规范账户与口令管理，定期更新口令，对权限实施分级管控。与供应商签订安全协议、明晰权责，选用经安全认证的工控软硬件；强化运维人员培训考核，第三方运维全程旁站监督审计，严禁私自操作核心设备。

5 结语

工控与公共网络的安全互联，是工业智能化发展的必然走向，只是这一过程的安全防护，要兼顾工业生产的实时性、可用性，以及网络安全的机密性、完整性。本文搭建的“五位一体”安全互联机制，从边界隔离、身份认证等五大维度形成全链条防护，设计的一体化实现方案贴合工业实际应用场景，能有效破解互联过程中的核心安全难题。未来，AI、数字孪生、6G 等技术持续发展，工控与公共网络的融合会更深入，安全风险也将呈现复杂化、智能化特征。后续可深挖 AI 驱动的自适应安全防护技术，实现攻击行为的精准识别与主动防御；也可探索数字孪生与工控安全的深度融合，构建虚拟仿真防护体系，提前预判互联风险，为工业互联网安全发展筑牢技术支撑。同时还需强化行业标准体系建设与跨领域协同，打造“技术 + 管理 + 标准”的立体化安全保障体系，切实筑牢国家关键基础设施的安全防线。

参考文献

[1] 王庚辰,姜庆超,颜学峰.基于深度学习的工控系统网络攻击多分类检测[J/OL].华东理工大学学报(自然科学版),1-11[2026-01-21].

[2] 淮文军,刘树立,高士伟,等.工业网络控制系统故障诊断与智能运维研究[J].电脑编程技巧与维护,2025,(11):173-176.

[3] 桂松涛.石油企业工业控制系统网络安全体系建设研究[J].信息系统工程,2025,(10):99-102.