数字化转型背景下中小企业工控安全应用研究与对策

陈 栋

金华市中小企业数字化转型促进中心 浙江 杭州 310000

【摘　要】：在浙江省中小企业数字化转型梯度培育战略推进背景下，中小企业数字化转型与工控安全防护的矛盾日益凸显。本文基于对金华市中小企业的漏洞扫描、实地调研及重点企业自检自查数据，系统分析企业工控安全现状与核心问题。研究构建“战略-治理-技术-执行”四层工控安全框架，结合“中小企业数字化转型梯队建设要求，提出适配不同发展阶段的差异化安全建设标准。研究成果为金华市中小企业工控安全建设提供可落地的实践路径，也为区域工业安全与数字化转型协同发展提供决策参考。

【关键词】：工控安全；中小企业；数字化改造；梯队建设；漏洞防护

DOI:10.12417/3083-5526.25.03.001

1 引言

随着浙江省中小企业数字化梯度培育体系的深入推进，金华市中小企业数字化转型进入规模化发展阶段。数据显示，金华市 32% 的中小企业因 ICS 与办公网未实现有效隔离，而现有工控安全研究多聚焦单一技术或管理层面，未能与分级建设要求深度适配。在此背景下，系统剖析金华市中小企业工控安全核心问题，结合产业发展对比提出针对性解决方案，对筑牢区域工业安全防线、推动中小企业数字化转型可持续发展具有重要现实意义。

2 工控安全产业发展对比分析

2.1 研究意义

工控安全是中小企业数字化转型的核心保障，对产业链稳定与国家工业安全具有战略价值。从企业层面看，有效的工控安全防护可避免生产中断与资产损失，从产业链层面看，中小企业作为产业链供应链的重要环节，其安全漏洞易通过供应链传导引发连锁反应，从区域发展层面看，金华市中小企业作为制造业数字化转型的重要力量，其工控安全水平直接影响浙江省中小企业数字化转型培育成效，而企业 ICS 中进口组件占比高、自主可控技术体系未完全建立的现状，更凸显了加强工控安全建设的紧迫性。

2.2 省内外发展对比

国外工控安全产业已形成“标准引领 - 技术落地 - 协同防护” 的成熟体系[1]。美国以国家标准为核心锚点，针对离散制造、流程工业等细分领域，拆解出 “基础防护 - 高级监测 - 动态响应” 的阶梯式实施路径，明确 PLC 固件校验、DCS 漏洞修复等具体操作规范。技术研发层面，国内已形成一批创新成果，通过在不同安全区域部署工业防火墙、单向网闸，使企业病毒传播率下降 76%；

2.3 金华与省内工业强市对比

金华产业特色带来独特安全挑战。作为长三角重要制造业基地，金华机械制造、电子信息、食品加工等行业中小企业占比较多，此类企业 ICS 多为 “新旧设备混联” 架构，部分的设备服役年限超 8 年，厂商已停止提供固件更新与漏洞修复服务；且企业多为产业链配套环节，安全风险传导性突出，此外，本地工控安全服务生态薄弱，企业需依赖杭州、上海等地工控安全服务商，突发安全事件响应周期长达 3-5 天，难以满足应急处置需求。

3 金华市中小企业工控安全核心问题

3.1 设备部署基础薄弱

2025 年针对金华市电动工具、磁性材料、服装 3 个试点行业企业的超过 80 份标本的调研，数据显示，金华重点企业仅 30% 的企业部署防火墙，其中专业工业防火墙应用率不足 5%，80% 为传统 IT 防火墙，难以适配工控协议与场景需求；70% 的企业未配备工业入侵检测系统（IDS），仅 20% 采用数据加密技术保护敏感数据。同时，多数企业未实现生产网与办公网有效隔离，仅通过普通交换机简单划分网段，无法抵御跨网络攻击渗透。且设备运维存在显著短板，40% 的企业未定期更新设备特征库，35% 未开启安全认证功能，25% 的老旧 PLC 设备（服役超 8 年）因厂商停止支持无法修复漏洞，形成长期安全隐患。

3.2 安全制度呈现碎片化特征

安全制度呈现“碎片化”特征，与数字化水平工控安全体系保障要求差距显著。制度完整性不足，60%的企业未建立完善的工控安全管理制度，仅 40%明确了设备管理、数据安全等基础要求，缺乏介质管理、权限管控等专项制度，部分企业因无介质管理制度导致核心配方泄露；应急管理流于形式，30% 的企业未制定工控安全应急预案，已制定预案的企业中，75%

陈栋（1983.9-），男，汉族，浙江，本科，研究方向为量子通信、工控安全。

未开展实质性应急演练，无法应对突发安全事件；人员管理机制缺失，80%的企业未配备专职工控安全工程师，第三方运维人员多缺乏 OT 环境操作资质，操作岗员工安全培训覆盖率仅 50%，默认口令使用、违规接入 USB 设备等行为频发。

3.3 漏洞风险防控占比较高

2025 年通过全方位漏洞排查，数据显示，跨站脚本攻击漏洞占比最高（45%），攻击者可通过构造恶意脚本注入网页窃取登录凭证与生产数据；数据传输存在严重缺陷，35% 的企业用户认证信息以明文形式传输，为中间人攻击提供可乘之机；工业控制系统层面，PLC 设备弱口令问题在各类型企业中均较突出，重点企业自检显示均未完成全面弱口令排查；高危端口未封闭、僵木蠕病毒未清理等问题在制造企业中尤为普遍，12%的企业因漏洞未及时修复导致生产数据泄露，直接影响正常生产运营。

4 分梯队工控安全建设指南

4.1 数字化水平 1.0 基础防护，基础合规型安全建设规范

数字化水平 1.0 基础防护作为数字化转型的起点，以 “边界隔离、基础防护、制度落地” 为核心，满足基础级安全标准。技术层面，部署工业防火墙实现生产网与办公网物理隔离，防火墙策略明确禁止办公终端访问 PLC 设备，仅允许授权数据传输。核心设备建立完整台账，记录型号、固件版本及补丁状态，老旧设备制定替换计划；开启设备身份认证功能，密码满足 “8 位以上字母 + 数字 + 特殊符号” 复杂度要求。工艺参数、生产配方等敏感数据采用国产密码算法（如 SM4）存储。同时，制定《工控安全管理制度》《设备安全管理办法》等基础制度，明确运维岗安全职责；完成“设备安全操作、弱口令风险识别、违规行为规避”等基础培训，考核合格后方可上岗。

4.2 数字化水平 2.0 增强防护，进阶提升型安全建设规范

数字化水平 2.0 增强防护作为数字化转型的核心阶段，以 “数据协同、动态防护、体系化管理” 为核心，满足增强级安全标准。技术层面，构建 “工业防火墙 ＋IDS＋ 安全隔离网关” 的多层防护体系，生产网按 “设备层 - 控制层 - 监控层” 划分网段，各网段间通过防火墙实现精细化访问控制；部署工业互联网安全监测平台，实时采集各网段流量数据，对 PLC 设备异常指令、数据批量导出等异常访问进行实时告警。建立数据全生命周期安全管理机制，采集阶段校验传感器数据完整性，传输阶段采用国密 SM4 算法加密，存储阶段实现敏感数据与非敏感数据分级存储，销毁阶段采用物理粉碎或多次覆写方式；搭建数据安全审计平台，对数据查询、修改、导出等操作进行全程追溯。工业主机安装工控专用杀毒软件，禁止安装非必要软件。部署轻量化安全运营平台（SOC），整合防火墙、IDS、审计日志等多源数据实现集中分析与可视化展示。治理层面，在数字化水平 1.0 制度基础上，补充《数据安全管理办法》《安全运营管理规范》，明确数据分级标准、安全运营流程及各部门安全职责，将漏洞修复率、安全事件发生率等指标纳入部门 KPI，考核结果与绩效挂钩，运维岗员工需掌握安全运营平台操作，管理岗员工需开展“安全战略与业务融合”培训，理解数字化水平 2.0 工控安全建设对生产效率的支撑作用，避免“重生产、轻安全”倾向。

4.3 数字化水平 3.0 以上重点防护，构建协同防护机制

数字化水平 3.0 重点防护作为数字化转型的高级形态，以 “智能防御、跨域协同、自主可控” 为核心，满足领航级安全标准。技术层面，全面部署零信任架构，采用 “身份多因素认证（MFA）+ 最小权限访问（PoLP）+ 实时行为验证” 机制，所有访问请求均需经过身份认证与权限校验；部署 AI 驱动的安全编排自动化响应（SOAR）平台，实现 “异常检测 - 端口阻断 - 漏洞溯源 - 补丁推送” 全流程自动化处置。部署动态脱敏系统，对客户信息、核心工艺等敏感数据按使用场景调整脱敏级别；搭建供应链安全监测平台，实时监控第三方组件漏洞更新情况，对存在高危漏洞的组件实现自动替换或补丁推送。治理层面，在数字化水平 2.0 制度基础上，新增《零信任安全管理规范》《供应链安全审计制度》，明确零信任架构落地流程、AI 安全模型训练规范、供应商安全准入标准及产业链协同防护职责；建立 “安全 - 业务” 协同决策机制，每年审议安全战略与业务发展的协同方案，组建专职工控安全团队，培育安全服务生态，对外输出安全解决方案，带动区域中小企业安全能力整体提升。

5 数字化改造背景下中小企业工控安全应用研究

基于调研发现的问题与企业梯队化需求，构建“战略-治理-技术-执行”四层工控安全解决方案，实现与数字化水平分级建设的深度适配。

5.1 锚定梯队建设目标

以金华市中小企业数字化转型阶段为依据，明确不同梯队安全战略定位。数字化水平 1.0 阶段，将“生产网络边界隔离、核心设备基础防护”纳入建设目标，确保符合等保 2.0 基础要求；数字化水平 2.0 阶段，设定“漏洞修复率≥90%、安全事件响应时间≤2 小时”等量化指标，实现生产经营数据安全共享；数字化水平 3.0 阶段，以“生产连续性 99.9%、核心数据泄漏率为 0”为目标，构建自适应安全防护体系，支撑“十场景”建设需求。

5.2 完善制度保障体系

建立董事会牵头的安全治理架构，明确安全管理部门、业务部门、运维团队的权责边界。制定分级制度规范，数字化水平 1.0 需完善设备管理、介质管控等基础制度；数字化水平 2.0 需补充应急预案、风险评估等专项制度；数字化水平 3.0 需建

立全生命周期安全管理制度。构建分层培训体系，操作岗重点培训弱口令修改、USB 设备管控等实操技能，运维岗强化漏洞修复、应急处置能力，管理岗提升安全战略认知。

5.3 构建梯队化防护架构

采用“基础防护+进阶升级”的技术路径，适配不同企业发展阶段[2]。部署工业防火墙、单向网闸等基础设备，实现生产网与办公网物理隔离，采用数据加密技术保护工艺参数[3]；基于机器学习算法分析 ICS 日志与设备状态数据，构建动态风险评估模型，提升威胁识别精度；数字化水平 3.0 落地零信任架构，实现身份多因素认证、最小权限访问与实时行为验证，集成 WAF、态势感知等设备，形成“数据接入→安全防护→威胁分析→人机协同→响应处置”的全链路闭环。

5.4 强化落地保障能力

搭建自动化响应机制，数字化水平 1.0 建立漏洞排查台账，每季度开展安全检查；数字化水平 2.0 部署态势感知、安全运营等平台，实现“异常检测-端口阻断-告警上报-漏洞溯源”标准化处置；数字化水平 3.0 构建跨企业协同响应体系，接入区域威胁情报共享平台。

6 结论

金华市中小企业工控安全的核心在于安全建设与梯队化数字化转型不同步，设备部署基础薄弱、漏洞风险防控不足等问题突出，通过构建 “战略 - 治理 - 技术 - 执行” 四层解决方案，针对企业不同数字化阶段制定差异化安全建设规范，明确设备部署、数据保护、应急处置等强制性要求，将工控安全纳入专项资金支持项目、数字化改造试点项目、各级企业申报与评定核心指标；数字化水平 1.0 阶段，明确工业防火墙部署、生产网隔离等基础要求；数字化水平 2.0 阶段，增加安全运营平台建设、动态风险评估等进阶指标；数字化水平 3.0 阶段，补充零信任架构应用、跨企业协同防护等高阶标准，形成“基础达标-进阶提升-卓越引领”的阶梯式建设路径，为中小企业数字化转型筑牢。

参考文献：

[1] 张耀元，原通文，韩立新，工业控制系统安全挑战与对策研究综述 1671-0711（2025）05（下）-0266-03

[2] 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，

[3] 周玉锁 基于深度学习的工控网络安全立体化防御体系研究 1008-1739(2025)01-0045-05

[4] 郝琪伟,谭文娟,佘林娟.国有企业年轻干部梯队建设的优化路径研究[J].知识经济,2025,(29):91-94.

[5] 王英州.工业控制系统异常场景重建与分析方法研究[D].哈尔滨工业大学,2025.