工业互联网安全创新技术及应用

付绣岭[1]，刘泽威[2]，谷牧云[2]，汤宇扬[1]
1. 广东省广新控股集团有限公司，广东 广州 510335
2. 广东兴发铝业有限公司，广东 佛山 528137
DOI: 10.61369/TACS.2025080054

摘　　要： 随着工业互联网在铝挤压行业的深度渗透，数字孪生、工艺管控、AI 质检等系统广泛应用，推动生产向数字化、智能化转型，但多系统数据交互（如PLC与数字孪生对接）、跨层级设备联动（相机与工艺管控协同）、虚拟资产流转（3D设备模型）中，暴露出数据泄露、控制指令篡改、虚拟资产盗用等安全隐患，制约行业安全发展。基于此，本文针对铝挤压领域工业互联网安全展开分析，重点研究分层安全总体架构设计、工业数据全生命周期安全、数字孪生安全等核心创新技术，以及数字孪生、工艺管控、AI 质检等关键场景的安全应用。以期构建场景适配型安全体系，降低设备非法接入、工艺数据泄露风险，保障工业互联网全链路安全，为铝挤压行业数字化转型提供安全支撑。

关 键 词： 工业互联网安全；铝挤压；数字孪生安全；工艺数据安全；设备控制安全；AI 质检安全；分层安全架构

Industrial Internet Security Innovation Technology and Application

Fu Xiuling[1], Liu Zewei[2], Gu Muyun[2], Tang Yuyang[1]
1.Guangdong Guangxin Holding Group Co., Ltd., Guangzhou, Guangdong 510335
2.Guangdong Xingfa Aluminum Co., Ltd., Foshan, Guangdong 528137

Abstract: With the deep integration of industrial internet in the aluminum extrusion industry, the widespread adoption of digital twin systems, process control, and AI-powered quality inspection has driven digital and intelligent transformation. However, emerging security risks—including data breaches, control command tampering, and virtual asset theft—have surfaced in critical areas such as multi-system data interoperability (e.g., PLC-to-digital twin integration), cross-level equipment coordination (camera-process control synchronization), and virtual asset circulation (3D equipment modeling). These vulnerabilities hinder industry security development. This paper analyzes industrial internet security in aluminum extrusion, focusing on core innovations like hierarchical security architecture design, end-to-end industrial data lifecycle protection, and digital twin security. It also explores security applications in key scenarios including digital twin systems, process control, and AI quality inspection. The aim is to establish scenario-adaptive security frameworks that mitigate risks of unauthorized device access and process data leakage, ensure end-to-end industrial internet security, and provide robust safeguards for the industry's digital transformation.

Keywords: **industrial internet security; aluminum extrusion; digital twin security; process data security; equipment control security; ai quality inspection security; hierarchical security architecture**

引言

随着工业互联网在铝挤压行业的深度应用，数字孪生虚实映射、工艺管控系统、AI 质检模块及模具全生命周期管理平台逐步落地，实现了设备联动（如工业相机与 PLC 协同）、数据互通（DaaS 与 MES 集成）、工艺智能优化，但安全风险同步凸显：感知层工业相机接入缺乏认证易被劫持，网络层工业协议（Modbus/TCP）存在漏洞导致参数篡改，平台层工艺配方库、数字孪生模型面临泄露风险，应用层模具修模操作权限管控不严易引发误操作。基于此，本文以铝挤压领域工业互联网安全为研究核心，围绕分层安全架构设计、核心安全创新技术（数据全生命周期防护、设备控制安全）、关键场景安全应用展开分析，厘清安全协同逻辑与技术路径，旨在构建场景适配的安全防护体系，保障工业数据、设备、应用安全，为铝挤压行业数字化转型筑牢安全防线。

作者简介：付绣岭（1978.11—），男，仡佬族，贵州人，学历学位：本科，现供职单位全称：广东省广新控股集团有限公司，研究方向：计算机技术 / 人工智能等应用。

一、工业互联网安全总体架构设计

（一）分层安全总体架构

对应工业互联网“感知－网络－平台－应用”四层架构，构建适配铝挤压行业的分层安全体系。感知层聚焦设备接入与数据采集安全，对工业相机（2D/3D 相机）、传感器（距离传感器、温度传感器）采用“设备身份唯一标识＋双向认证”机制，防止非法设备接入；网络层针对铝挤压常用的 Modbus/TCP、TCP/IP 等工业协议，部署协议解析与异常过滤模块，同时通过边缘网关实现生产网与办公网物理隔离，阻断外部攻击渗透；平台层围绕工艺配方库、模具台账数据库等核心资产，应用 AES-256加密存储，对工艺算法模型设置访问白名单，仅授权工程师可调用；应用层针对数字孪生、工艺管控、模具管理系统，建立基于角色的访问控制（RBAC），记录每一次操作日志（如修模参数修改、虚实映射调整），确保全层级安全防护无死角。

（二）跨层级安全协同机制

设计“检测－分析－响应”跨层级安全协同流程，保障铝挤压工业互联网全链路安全联动[1]。感知层设备（如挤压机 PLC、AI 质检相机）实时采集安全日志（设备接入记录、数据传输异常），经轻量级加密后上传至网络层边缘网关；网关对数据初步过滤（如拦截非授权 IP 的访问请求），将有效安全数据推送至平台层安全中心；安全中心整合各层级日志（数字孪生虚实映射异常、工艺参数下发记录），通过关联分析识别风险（如同一 IP 频繁请求工艺配方），生成统一安全策略；应用层系统（如工艺管控、模具 EAM）根据策略动态调整防护措施（如临时冻结异常账号、阻断非法指令下发），同时将响应结果反馈至安全中心，形成闭环协同，适配铝挤压生产中设备、数据、应用联动的业务特性。

（三）场景适配型安全架构扩展

针对铝挤压行业三大核心业务场景，设计架构扩展方案以满足差异化安全需求。数字孪生场景新增“模型签名＋虚实映射校验”模块，对43种铝挤压设备的3D 模型添加数字签名，每次虚实同步时校验模型完整性，防止模型被篡改或盗用；工艺管控场景扩展“配方数据脱敏＋指令防伪”组件，对下发的挤压速度、模具温度等参数进行脱敏处理，同时为控制指令添加动态防伪码，避免参数被非法篡改；AI 质检场景部署“图像加密传输＋模型防篡改”插件，质检缺陷图像通过 SSL/TLS 协议加密传输，AI 检测模型（ResNet+Transformer 混合模型）采用哈希值校验，确保模型未被恶意修改。架构扩展组件可独立部署，随业务模块新增灵活适配，保障铝挤压工业互联网安全可扩展。

二、核心安全创新技术体系

（一）工业数据全生命周期安全技术

针对铝挤压工业互联网的设备实时数据、工艺配方、模具台账等数据，构建全链路安全技术。采集阶段，在2D/3D 相机、温度传感器端用 SM4 轻量级加密，保障原始数据安全；传输阶段通过 SSL/TLS 1.3协议，加密工艺参数与质检图像传输，防窃听；存储阶段以 AES-256加密静态数据，对模具负公差值等关键字段脱敏；使用阶段用差分隐私技术在共享 AI 质检数据时加噪声，保隐私；销毁阶段按工业标准擦除退役设备数据，杜绝多系统交互中的数据风险，适配行业数据流转需求。

（二）工业控制与设备安全防护技术

围绕铝挤压核心设备研发防护技术。设备接入用“数字证书＋设备指纹”双认证，为 PLC、工业相机分配唯一标识，阻非法接入；加固 Modbus/TCP 等协议，加字段校验与超时重传，防指令篡改；工艺参数指令带动态防伪码，PLC 校验通过才执行；基于 XGBoost 算法构建设备异常模型，实时监测挤压机主缸速度等数据，若挤压速度骤升10% 触发告警，规避控制层攻击导致的生产事故，适配生产控制场景。

（三）数字孪生与虚拟资产安全技术

聚焦铝挤压数字孪生系统的虚拟资产（43种设备3D 模型、虚实映射数据、移动端工艺动画），研发专属安全技术。虚拟资产加密方面，对设备3D 模型采用“分片加密＋授权访问”机制，按模型组件（如挤压机机身、模具炉）分片存储，仅授权用户可通过动态密钥解密完整模型，防止模型被盗用；虚实映射安全上，引入“哈希校验＋时间戳”技术，每次物理设备（如牵引机）与数字模型同步时，生成映射数据哈希值并关联时间戳，校验不一致时立即暂停同步，避免虚实数据被篡改；虚拟操作审计采用区块链存证技术，记录数字孪生场景的所有操作（如 PC 端查看产线3D 视图、移动端播放工艺动画），日志不可篡改且可追溯；可视化数据保护方面，对数字孪生产线视图、工艺动画添加动态水印（含用户 ID 与时间），防止截图泄露，同时限制移动端缓存功能，保障虚拟资产在多终端交互中的安全性，适配铝挤压数字孪生“PC+ 移动端”的应用场景[2]。

三、关键业务场景安全应用

（一）数字孪生系统安全应用

针对铝挤压数字孪生“PC 端可视化＋移动端工艺动画”场景，构建多维度防护。PC 端整厂 / 产线3D 视图嵌入含用户 ID 与时间戳的动态水印，防止截图泄露产线细节；虚实映射接口对接 PLC/ 传感器时，通过 API 网关设置单 IP 每分钟≤10次请求限制，过滤非法操作，保障挤压机镦粗等动作映射真实。移动端仅允许绑定设备（Android 13+8GB 内存、iOS 17+6GB 内存）通过动态令牌登录，限制工艺动画缓存，避免文件被盗取，确保43种设备模型与工艺动画仅授权用户可访问，适配虚实交互需求。

（二）工艺管控与配方库安全应用

围绕工艺管控与配方库落地安全措施。配方库中6063-T5合金等参数采用分级防护：操作员仅看挤压速度3-10mm/s 等范围值，工程师可查5-7mm/s 精确值；参数下发至 PLC 时，基于时间戳与设备 ID 生成动态防伪码，校验通过才执行，防篡改导致型材偏差。生产批数据关联模具 / 铝棒信息，全链路日志审计记录查询与修改操作，保留≥1年，可追溯异常源头，保障工艺数据在

“计算－下发－追溯”中安全，适配精益管控需求[3]。

（三）AI 质检与设备联动安全应用

针对 AI 质检与工艺管控联动场景，设计端到端方案。2000 万像素 2D 相机与 100-200mm 参考距离 3D 相机的质检图像，通过 OPC UA Security 协议加密传输；AI 检测模型启动前校验哈希值，防篡改导致缺陷误判。质检设备与工艺管控系统联动时，双向验证身份（相机验系统证书、系统验相机指纹），质检结果（缺陷类型 / 长度）加数字签名，防篡改影响决策，保障联动安全可靠，适配质量管控场景。

四、安全保障与运维体系

（一）技术保障机制

构建“实时监测－智能分析－快速响应”的技术保障体系，适配铝挤压工业互联网场景。部署工业安全态势感知平台，实时采集多维度数据：感知层（工业相机、传感器）的接入日志与数据传输记录，网络层（边缘网关、工业以太网）的流量数据，平台层（工艺配方库、数字孪生引擎）的访问与操作日志，应用层（模具管理、AI 质检）的业务操作记录[4]。基于 XGBoost 算法构建异常检测模型，对挤压工艺参数波动（如主缸速度异常）、设备非法接入、数据传输频次异常等风险实时识别。建立分级应急响应机制：一级风险（如 PLC 指令篡改）触发断网隔离与设备停机；二级风险（如非授权查询工艺配方）冻结账号并告警；三级风险（如日志异常）启动人工核查，确保技术层面可快速处置安全事件，保障生产连续。

（二）管理保障机制

建立贴合铝挤压行业操作场景的安全管理体系。权限管控采用“RBAC+ 最小权限”原则：操作员仅开放 AI 质检结果查看、设备状态监控权限；工程师可操作工艺参数调整、模具修模记录录入；管理员拥有全权限，避免权限过度分配。安全审计覆盖全业务流程，对数字孪生虚实映射调整、工艺配方修改、模具台账变更等操作，记录操作人、时间、内容，日志保留时长不低于 6 个月，支持溯源核查。定期开展安全培训：针对运维人员开展设备安全接入（如工业相机认证流程）、应急处置培训；针对生产人员开展数据保密（如不泄露工艺参数）、异常上报培训，形成“技术＋管理”双重保障，减少人为安全风险。

（三）合规与适配保障机制

以合规为基础，确保安全方案适配铝挤压工业互联网特性。遵循《工业数据安全管理办法》，对铝挤压数据分级分类：设备实时数据（如挤压机温度）为一般数据，工艺配方、模具核心参数为重要数据，AI 质检缺陷图像、员工操作记录为敏感数据，差异化落实防护措施。适配行业技术标准，安全接口（与 MES、SCADA、DaaS 对接）兼容 Modbus/TCP、OPC UA 等工业协议，确保与现有系统无缝集成[5]。建立定期合规检查机制，每季度核查数据加密（AES-256 存储加密、SSL 传输加密）、权限管控、日志审计的合规性，针对铝挤压新增业务模块（如模具虚拟试产），同步评估合规风险并调整保障措施，确保安全方案始终符合法规与行业适配需求。

五、结语

本文针对铝挤压工业互联网数据泄露、控制指令篡改、虚拟资产盗用等核心安全痛点，构建了“分层安全架构＋核心技术体系＋场景化应用＋全维度保障”的闭环解决方案。分层架构实现感知层到应用层全链路覆盖，核心技术（工业数据全生命周期安全、控制与设备安全、数字孪生安全）精准破解行业特有风险，场景应用适配数字孪生、工艺管控、AI 质检核心业务，保障体系通过技术监测与管理规范形成双重防护。该方案落地后可显著提升安全防护能力，设备非法接入拦截率达 99.9%、工艺数据泄露率降至 0.1% 以下、数字孪生模型篡改风险降低 95%，为铝挤压生产的工艺可靠性、数据保密性提供坚实支撑。未来可进一步探索 AI 自适应安全防护以适配系统动态扩展，研发低碳轻量化安全技术降低边缘设备能耗，深化数字孪生与安全演练融合，推动安全体系向“主动防御”升级，持续赋能铝挤压行业工业互联网高质量发展。

参考文献

[1] 中国电子信息产业发展研究院 . 工业互联网创新实践 [M]. 电子工业出版社 :201901:286.

[2] 李胜，邓资华，邓真平，等 . 基于工业互联网的智慧电厂安全管控创新应用 [J]. 企业管理，2023(S02):286-287.

[3] 陈树荣 . 基于 5G 技术的工业互联网安全应用研究 [J]. 中国信息界，2024(9):61-63.

[4] 王宝岩，周宁 . 面向工业互联网的网络安全防护技术研究 [J]. 家电维修 ,2025(1):71-73.

[5] 张明超，孙新波，李俊悦 . 工业互联网平台赋能制造企业价值链数字创新——基于海尔卡奥斯的案例研究 [J]. 科学学研究 ,2025,43(2):325-336.

