基于大模型技术的商烟物流工控安全优化研究

廖东阳，周建钧，周翔明
（湖南省烟草公司永州市公司，湖南　永州　425000）

摘　要：针对商烟物流中心传统工控安全防护体系误报率高、策略僵化、运维不足及缺乏闭环等问题，以该中心工控系统为研究对象，融合大模型技术构建“感知－分析－决策－响应－优化”五层闭环防护体系，集成多源数据融合分析、智能策略动态配置等核心技术，设计四大功能模块。研究结果显示，优化后体系误报率降至4.8%，异常识别准确率达96.2%，安全事件响应时间缩短75%，业务中断时长与运维工作量显著减少，可有效抵御各类常见工控安全攻击。该体系适配商烟物流业务特性，具备可复制扩展性，为烟草行业工控安全防护升级提供切实可行的实践模板。

关键词：大模型；商烟物流中心；工控安全；闭环防护体系；多源数据融合；智能策略配置
中图分类号：TP309.2　　**文献标志码：**A　　**DOI：**10.19358/j.issn.2097－1788.2026.05.003

中文引用格式：廖东阳，周建钧，周翔明. 基于大模型技术的商烟物流工控安全优化研究[J]. 网络安全与数据治理，2026，45(5)：18－23.
英文引用格式：Liao Dongyang，Zhou Jianjun，Zhou Xiangming. Research on industrial control security optimization of commercial tobacco logistics based on large model technology[J]. Cyber Security and Data Governance，2026，45(5)：18－23.

Research on industrial control security optimization of commercial tobacco logistics based on large model technology

Liao Dongyang，Zhou Jianjun，Zhou Xiangming
（Hunan Tobacco Company Yongzhou Company，Yongzhou 425000，China）

Abstract：Aiming at the problems of high false alarm rate，rigid strategy，insufficient operation and maintenance，and lack of closed-loop in the traditional industrial control security protection system of the commercial tobacco logistics center，this article takes the industrial control system of the center as the research object，integrates large language model technology to construct a five layer closed-loop protection system of "perception-analysis-decision-response-optimization"，integrates core technologies such as multi-source data fusion analysis and intelligent strategy dynamic configuration，and designs four functional modules. The research results show that after optimization，the false alarm rate of the system has been reduced to 4.8%，the accuracy of anomaly recognition has reached 96.2%，the response time to security incidents has been shortened by 75%，the duration of business interruption and the workload of operation and maintenance have been significantly reduced，which can effectively resist various common industrial control security attacks. The system is adapted to the characteristics of commercial tobacco logistics business，has replicability and scalability，and provides a practical template for upgrading the industrial control security protection in the tobacco industry.

Key words：large language model；commercial tobacco logistics center；industrial control security；closed-loop protection system；multi-source data fusion；intelligent strategy configuration

0　引言

烟草行业作为国民经济支柱产业，商烟物流中心经自动化、智能化转型后关键业务效率显著提升，但工控系统与外部网络边界模糊，安全事件逐年增多[1]。传统防护体系难以应对复杂攻击与动态业务[2]，而大模型凭借多源数据处理、自主学习等优势，可精准识别未知威胁。本文将大模型与工控安全深度融合，构建“感知－分析－决策－响应－优化”闭环防护体系，破解传统防护缺陷，为行业防护升级提供支撑。

国外工控安全研究起步较早，已形成较为成熟的技术体系与标准规范，但早期基于传统机器学习的方法对未知攻击识别率不足70%[3－4]。国内烟草行业高

网络安全与数据治理

度重视工控安全，国家烟草专卖局“十四五”信息化规划明确要求构建全方位保障体系，但当前研究主要聚焦硬件防护与传统算法优化，存在防护逻辑固化、缺乏适配商烟物流特性的整体体系等短板[5-6]。

目前，大模型在工控安全中的应用呈单点突破、体系化不足等特征，未形成全生命周期防护方案[7-8]，且未适配商烟物流中心业务及工控特性，无法破解传统防护核心问题。

本文构建大模型融合的智能闭环防护体系，旨在降低安全事件误报率、优化安全策略、降低运维门槛，同时丰富行业理论体系、提供技术参考，为烟草行业工控安全升级提供可复制的实践模板。

1　商烟物流中心工控安全现状与痛点分析

商烟物流中心工控系统采用设备层－控制层－管理层三层架构，支撑卷烟入库、分拣、配送全流程自动化作业[9]。设备层执行物理作业，控制层负责设备控制与数据采集，管理层统筹业务管理、指令下发及数据交互。系统通过工控专网与企业信息网互联互通，虽经网闸、防火墙隔离，但受业务需求限制，仍需保留固定通信接口，导致边界防护压力大，成为安全威胁的主要入口。

现有防护体系以工业防火墙、审计系统、入侵检测等硬件产品为核心，依托“边界隔离＋特征匹配＋机器学习”构建防护逻辑。但存在四大核心痛点[10-11]：一是误报率高，缺乏动态优化与场景化训练机制，泛化能力不足，误报率达32%，无效告警干扰生产；二是策略僵化，采用“一刀切”配置，与业务流脱节，设备调整时策略更新滞后，多产品协同性差，存在防护盲区与规则冲突；三是运维能力存在短板，运维人员多从信息化岗位转岗而来，缺乏工控协议解析、新型攻击处置及溯源能力；四是无闭环机制，防护组件数据分散形成信息孤岛，缺乏关联分析与事件效果跟踪机制，同类安全事件反复爆发。

2　基于大模型技术的工控安全防护体系架构设计

2.1　整体架构设计

防护体系采用“感知－分析－决策－响应－优化”五层闭环架构，各层通过数据总线实现互联互通，形成全流程、智能化防护闭环。整体架构如图1所示。

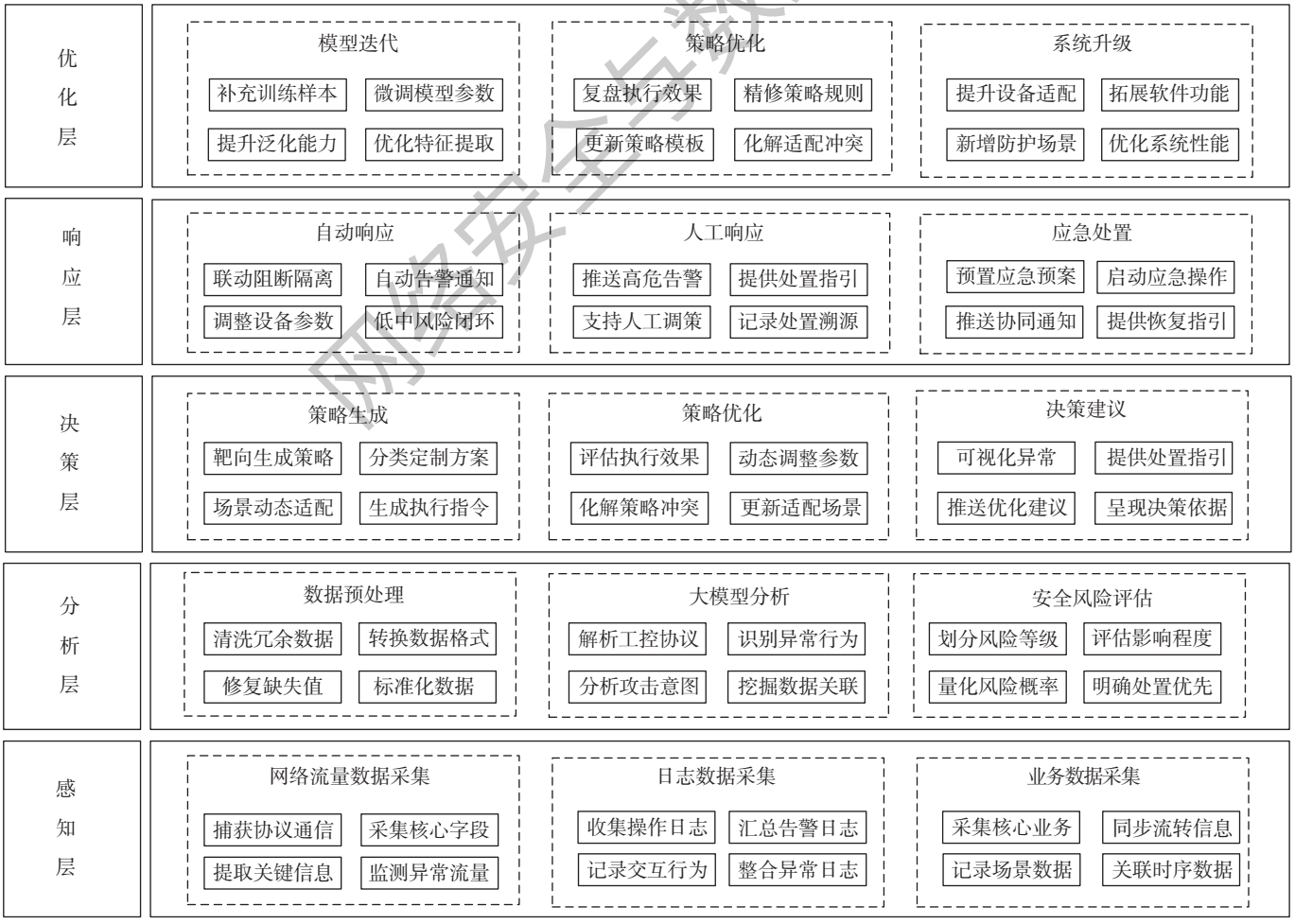

图1　整体架构图

网络安全与数据治理

2.1.1 感知层

作为数据采集核心，感知层为分析层提供基础数据支撑，采集商烟物流中心工控系统四类数据：通过工控专网核心节点流量采集器获取含数据包、协议功能码的网络流量数据；采集设备运行状态数据；汇总管理系统与安全设备的日志数据；收集订单量、分拣效率等业务数据以关联安全与业务。采集方式采用无损旁路部署，并支持动态调整采集频率，以平衡数据实时性与系统资源占用。

2.1.2 分析层

分析层是系统的智能分析引擎，基于大模型深度处理感知层数据，实现异常识别、风险评估与攻击溯源：数据预处理模块清洗转换数据为结构化格式；大模型分析引擎解析工控协议、识别异常并分析攻击意图；风险评估模块按行业标准对异常定级，为决策层提供依据。

2.1.3 决策层

决策层依据分析层结果生成并优化防护策略：策略生成模块针对不同异常与风险等级制定专属策略；策略优化模块持续评估执行效果，动态调整参数；决策建议模块向运维人员提供可视化异常详情、处置步骤等，辅助人工决策。

2.1.4 响应层

响应层执行决策层策略，实现安全事件快速处置：自动响应模块联动安全设备，处置低、中风险事件；人工响应模块向运维人员推送高风险告警并提供指引，支持人工介入；应急处置模块启动预案，降低重大事件的业务损失。

2.1.5 优化层

优化层通过分析运行与处置数据，实现体系持续迭代：模型迭代模块补充样本、微调参数，提升识别能力；策略优化模块优化规则，降低误报与漏报率；系统升级模块更新软硬件，拓展防护边界以适配新设备与新型攻击类型，形成防护闭环。

2.2 核心技术支撑

2.2.1 工控场景专用大模型训练

采用通用大模型 + 领域适配层 + 任务层三级架构，选用 ChatGLM-6B 作为基础大模型，选型依据如下[12]：

（1）协议特征提取适配性：在工业协议（如 Modbus、Profinet）的结构化解析任务中，ChatGLM-6B 的 F1 值较 LLaMA 2（7B）提升了 12.3%[13]，表明其能够精准提取协议功能码、寄存器地址等关键特征，更适配商烟物流工控系统多协议交互场景。

（2）长文本处理效率：针对工控系统日志、流量会话等长文本数据，ChatGLM-6B 的处理速度较 GPT-3.5 Turbo 提升 40%[13-14]，且本地部署无网络延迟，满足工控安全实时性要求。

（3）小样本适配能力：通过 LoRA 微调技术，ChatGLM-6B 仅需 500 条商烟物流工控场景标注数据即可实现领域适配，较 BERT-base 模型所需样本量减少 60%[15]，大幅降低训练成本。

（4）部署灵活性：ChatGLM-6B 支持 INT4/INT8 量化部署，在普通 x86 服务器即可稳定运行，无需高端 GPU 硬件，适配商烟物流中心现有 IT 基础设施。

采用本地训练 + 模型联邦更新模式，确保原始数据不脱离工控专网，从而有效规避数据泄露风险。

2.2.2 多源数据融合分析技术

采用联邦学习、数据脱敏、数据关联建模技术：联邦学习实现跨域安全分析，避免数据集中存储的隐私风险；数据脱敏处理日志敏感信息，平衡安全性与可用性；建立多源数据关联模型，挖掘数据潜在联系，精准识别异常。

2.2.3 智能策略动态配置技术

基于强化学习算法，实现策略动态调整、多设备策略协同优化、自适应学习，避免规则冲突与防护盲区，优化策略针对性与有效性。

3 核心功能模块设计与实现

3.1 大模型训练与优化模块

3.1.1 训练数据预处理

对采集的多源数据进行清洗、脱敏、标注处理，具体流程如下：（1）数据清洗：去除重复数据、无效数据，采用插值法修复缺失数据，确保数据完整性；（2）数据脱敏：对敏感信息进行处理，避免敏感信息泄露；（3）数据标注：采用人工标注与自动标注相结合的方式，对异常数据进行标注；（4）数据划分：按比例将标注后的数据划分为训练集、验证集与测试集，分别用于模型训练、超参数调整与性能评估。

3.1.2 模型架构设计

模型采用“通用大模型 + 领域适配层 + 任务层”的三级架构，具体设计如下：通用大模型层基于 ChatGLM-6B，提供基础能力；领域适配层引入烟草行业工控安全知识图谱，实现场景适配；任务层针对异常识别、策略生成、运维辅助设计专用网络结构。采用小批量梯度下降算法训练模型，通过学习率衰减策略避免过拟合。

3.1.3 模型性能评估与优化

通过准确率、召回率、误报率、漏报率等指标评

网络安全与数据治理

估模型性能。为提升模型性能，采用以下优化措施：补充攻击样本以增强数据多样性；调整超参数（优化学习率、增加训练轮次、引入早停策略）；引入多头注意力机制，进一步提升模型性能。

3.2 异常行为智能识别模块

3.2.1 识别维度设计

结合商烟物流工控系统的三层架构与收货、存储、分拣、配送四大核心业务流程，设计多维度异常识别体系，全面覆盖网络层、设备层、应用层、业务层的异常行为：（1）网络层异常：包括异常流量、非法端口访问、协议异常、IP 地址伪造；（2）设备层异常：包括设备运行参数异常、固件异常升级、默认账户密码未修改、设备离线；（3）应用层异常：包括各类管理系统异常登录、订单数据篡改、分拣任务异常中断；（4）业务层异常：包括分拣效率突降、订单处理延迟、库存数据异常波动、配送路径偏离。

3.2.2 识别算法实现

基于大模型的异常行为识别算法流程如下：（1）数据输入：接收感知层采集的多源数据，经过预处理模块转换为结构化数据后输入大模型；（2）特征提取：大模型自动提取数据中的关键特征；（3）模式匹配：将提取的特征与模型训练库中的正常模式、异常模式进行比对，计算特征相似度；（4）异常判定：根据相似度结果，结合风险等级评估规则，判定是否为异常行为，同时输出异常类型、风险等级、影响范围等信息。

3.3 安全策略智能配置模块

3.3.1 策略生成逻辑

安全策略智能配置模块基于大模型的决策能力，根据异常行为的类型、风险等级、影响范围，生成针对性的防护策略，具体生成逻辑如下：（1）低风险等级：生成告警通知 + 持续监测策略，通过可视化平台向运维人员发送告警，持续监测后自动闭环；（2）中风险等级：生成调整设备参数 + 限制相关操作权限策略，自动调整设备运行阈值，临时限制异常操作权限，同时通知运维人员核查；（3）高风险等级：生成阻断攻击 IP + 锁定账户 + 告警通知策略，通过工业防火墙阻断攻击源，锁定异常账户，向运维人员发送紧急告警；（4）高高风险等级：生成隔离受感染设备 + 启动应急预案 + 数据恢复策略，自动隔离受感染设备，启动预设应急方案，调用数据备份进行恢复。

3.3.2 策略动态优化

策略生成后，模块通过以下方式实现动态优化：（1）实时监控策略执行效果：持续监测策略执行后的异常复发率、业务影响程度；（2）结合业务场景调整：根据业务动态变化调整策略参数；（3）基于历史数据迭代：分析历史策略的执行效果数据，优化策略规则。

3.4 智能运维响应模块

3.4.1 可视化运维平台

开发可视化运维平台作为运维人员与防护体系的交互入口，平台采用 B/S 架构，支持多终端访问，核心功能包括：（1）实时监控：以多种图表形式展示工控系统运行状态、网络流量、设备状态、安全事件告警等信息，支持多维度筛选与钻取；（2）告警管理：对安全告警进行分类展示，标注告警级别、处理状态，支持一键处理，并记录处理日志；（3）事件处置：提供安全事件的详细分析报告；（4）策略管理：支持对防护策略的查看、编辑、启用/禁用操作，展示策略执行效果数据；（5）报表统计：自动生成不同周期的安全运行报表，为管理层决策提供依据。

3.4.2 智能辅助运维功能

针对运维人员专业不足的问题，模块提供以下智能辅助功能：（1）知识库查询：内置工控安全知识库，涵盖各类专业内容，支持关键词检索；（2）故障诊断辅助：运维人员输入设备故障现象，大模型自动匹配可能的原因与处置步骤，提供可视化操作指引；（3）远程协助接口：支持与安全厂商专家系统对接，实现远程故障排查与技术支持。

4 实践验证

4.1 实践环境

在某商烟物流中心部署防护体系，该中心日均处理订单 5 000 单以上，工控系统含终端设备 200 余台、控制器 50 余台、数据采集与监控系统 3 套、业务管理系统 4 套，工控专网带宽 1 000 Mb/s。

防护体系采用“物理部署 + 虚拟化部署结合”模式：工业防火墙、流量采集器等硬件物理部署于网络边界与核心节点；大模型分析引擎、可视化运维平台等软件虚拟化部署，基于云计算资源灵活扩展。

该模式优势体现在物理部署可保障核心设备独立运行与低延迟，虚拟化部署则能提升弹性扩展能力并降低硬件成本。但是，也带来了运维复杂性增加、安全边界模糊、资源调度协同难度提升等挑战。

针对上述挑战，拟采取以下应对措施：建立统一运维管理平台；强化虚拟化环境安全防护；采用 SDN 技术实现网络协同调度。

网络安全与数据治理

4.2 测试指标与方法

4.2.1 测试指标

选取误报率、异常识别准确率、安全事件响应时间、业务中断时长、运维工作量、故障诊断建议采纳率、平均诊断时间缩短比例七项核心指标，全面评估体系的性能优势。

4.2.2 测试方法

采用对比测试 + 模拟攻击测试的方法验证体系性能。

对比测试：将优化体系与传统防护体系在同一环境下分别运行 3 个月，统计各项指标数据，对比分析优化体系的性能优势。传统防护体系保持原有配置不变，优化体系按设计方案部署运行，确保测试环境的一致性与可比性。

模拟攻击测试：邀请专业安全团队发起四类常见工控安全攻击，包括 PLC 暴力破解攻击、Modbus 协议异常调用、DDoS 攻击、订单数据篡改攻击，分别测试两套体系的识别与处置效果，评估优化体系的实战防护能力。

针对智能辅助运维功能，额外选取 30 例商烟物流中心历史故障案例，由 5 名运维人员分别采用传统排查模式与优化体系智能辅助模式进行故障诊断，记录诊断时间与建议采纳情况，量化评估功能价值。

4.3 实践结果与分析

4.3.1 对比测试结果

对比测试数据如表 1 所示，优化体系在各项核心指标上均实现显著提升。

表 1 传统防护体系与优化体系性能对比

测试指标	传统防御体系	优化体系	提升幅度
误报率	32.0%	4.8%	-85.0%
异常识别准确率	65.0%	96.2%	+48.0%
安全时间响应时间	60 min	15 min	-75.0%
业务终端时长	8 h	2 h	-75.0%
运维工作量	1 200 条	280 条	-76.7%
故障诊断建议采纳率	/	89.3%	/
平均诊断时间缩短比例	/	67.5%	/

从表 1 数据可以看出：(1) 误报率大幅降低，有效解决了传统体系告警泛滥的问题；(2) 异常识别准确率显著提升，确保真正的安全事件能够被及时发现；(3) 安全事件响应时间大幅缩短，均满足核心目标；(4) 业务中断时长与运维工作量显著减少，降低了经济损失与运维压力；(5) 智能辅助运维功能表现优异，故障诊断建议采纳率接近 90%，平均诊断时间缩短超三分之二，有效弥补了运维人员专业能力不足的短板。优化体系误报率 4.8%、响应时间 15 min，均超额完成预设研究目标；异常识别准确率 96.2%，显著提升了防护精准度。

4.3.2 模拟攻击测试结果

模拟攻击测试中，专业团队发起四类常见的工控安全攻击，两套体系的表现如表 2 所示。

表 2 模拟攻击测试结果对比

攻击类型	传统防护体系表现	优化体系表现
PLC 暴力破解攻击	未识别，攻击成功导致设备离线，业务中断	快速识别，自动阻断攻击源，无业务影响
Modbus 协议异常调用	误判为正常通信，未告警，导致设备参数异常	快速识别，生成协议过滤策略，设备恢复正常
DDoS 攻击（流量型）	告警但误判类型，未处置，业务效率下降	快速识别，自动调整防护规则，业务正常运行
订单数据篡改攻击	未识别，导致分拣错误，造成经济损失	快速识别，阻断篡改操作，恢复正确数据

测试结果表明，基于大模型的优化体系能够快速、准确地识别各类模拟攻击，并自动执行有效的防护策略，而传统防护体系在攻击识别与处置上存在明显短板。

4.3.3 实践效果总结

优化体系部署验证表明：安全防护能力显著提升，业务连续性有效增强，运维压力大幅减轻，防护体系自适应能力明显提升，可适配新型攻击与业务变化。

5 结论

本文针对商烟物流中心传统工控安全防护四大痛点，提出基于大模型的优化方案，构建五层闭环架构，融合三类核心技术，实现四大功能模块。实践验证显示，体系误报率 4.8%、异常识别准确率 96.2%，安全事件响应时间等关键指标大幅优化，适配业务且可复制扩展，为烟草行业工控安全升级提供实用方案。

该防护体系核心架构与技术逻辑可跨行业迁移，在电力、化工等场景具备适用性，但面临工控协议差异、实时性要求不同、数据敏感性差异等挑战，需针对性优化。后续将通过跨行业试点，持续提升体系普适性与适配能力，为工业互联网安全防护提供更具推广价值的方案。

参考文献

[1] 崔建华. “两化融合”背景下烟草行业工控系统安全防护研究[J]. 科学与财富，2020，10（5）：56 - 59.

网络安全与数据治理

[2] 王晔，万佳蓉，荆琛，等. 烟草商业企业工控系统网络安全防护建设研究[J]. 网络安全与数据治理，2025，44（8）：17－23.
[3] XU H，WANG S，LI N，et al. Large language models for cyber security：a systematic literature review[J]. arXiv preprint arXiv：2405.04760，2024.
[4] ZHANG J，BU H，WEN H，et al. When LLMs meet cybersecurity：a systematic literature review[J]. Cybersecurity，2025，8（1）：1－41.
[5] 耿欣. 烟草行业工业控制系统安全保障体系构建[J]. 烟草科技，2017，50（12）：99－105.
[6] 洪轶群. 烟草工业控制系统信息安全检测技术研究[J]. 网络安全技术与应用，2020（2）：122－124.
[7] 陈福林. 大型语言模型在网络安全专家系统中的应用研究[J]. 网络安全技术与应用，2025（3）：48－52.
[8] 孟楠，周成胜，赵勋. 生成式人工智能赋能网络安全运营降噪能力研究[J]. 信息通信技术与政策，2024，50（8）：24－31.
[9] 彭太刚. 基于InTouch软件的烟草物流自动化监控系统[J]. 物流技术与应用，2013，18（2）：98－100.
[10] 李静. 计算机仿真技术下的自动化物流系统设计及应用[J]. 自动化与仪器仪表，2016（6）：220－221.
[11] 王鹏，陈德为. 现场总线技术在烟草工业成品物流自动化系统中的应用[J]. 物流科技，2011，34（5）：52－54.
[12] 方文华. 烟草商业物流工控安全体系建设探究[J]. 中国市场，2022（8）：173－175.
[13] 王德吉. 烟草行业工控安全防护建设方案[J]. 自动化博览，2018，35（S2）：40－43.
[14] 韩璐. 大数据时代背景下人工智能技术在计算机网络安全中的应用研究[J]. 科技资讯，2025，23（4）：44－46.
[15] 王冬梅. 人工智能技术在网络安全威胁检测与防御中的应用研究[J]. 信息与电脑（理论版），2024，36（13）：123－125.

（收稿日期：2025－12－26）

作者简介：

廖东阳（1993－），男，本科，工程师，主要研究方向：网络安全、数据安全。

周建钧（1971－），男，本科，工程师，主要研究方向：信息技术、综合管理。

周翔明（1986－），男，本科，工程师，主要研究方向：网络安全、数据安全、网络技术。

网络安全与数据治理

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com