火力发电厂网络安全防护策略研究

候安宁

内蒙古国华准格尔发电有限责任公司 内蒙古 017100

摘 要：随着火力发电厂信息区域（第三区）日益暴露于远程运维与互联网访问环境，其边界安全风险显著上升，传统静态防护手段难以有效应对隐蔽性、多阶段的攻击行为。本文基于纵深防御理论与零信任架构，结合 MITRE ATT&CK 攻击链模型，提出一套融合身份认证、通道加密、行为感知与策略联动的信息区域边界纵深防护体系。通过构建仿真环境开展远程命令执行与横向渗透等攻击模拟实验，验证了该模型在识别准确率、响应时效与系统兼容性方面的优越性能。实测结果表明，模型可有效拦截典型攻击路径，系统检测率达92.7%、横向拦截成功率 89.3%，同时保障关键业务系统高可用运行。研究进一步提出可评估的部署策略与指标体系，为火电厂信息区安全体系建设提供了可复制、可落地的实践路径。

关键词： 火力发电厂；信息安全；边界防护；纵深防御；零信任架构

在火力发电厂信息区域（即第三区）中，随着运维系统、管理系统与互联网环境的深度融合，网络攻击威胁日益严峻，尤其是在远程维护、文件交换和运维终端接入等典型场景下，暴露出了较大的边界安全风险[1]。信息区域往往开放 VPN、Web 门户、邮件接口等对外服务，攻击者通过社会工程手段、网络扫描与凭据滥用等方式入侵第三区后，极可能向更高权限区域渗透，威胁电厂整体信息系统的稳定性与数据完整性[2]。

鉴于火电厂信息区域的攻击场景呈现出多通道入口、跨平台交互及隐蔽化行为等特点，单一防护手段难以覆盖其复杂性与动态性[3]。因此，需引入兼具多层感知与策略联动能力的理论体系。随着电力行业不断推进数字化转型，工业控制系统与办公信息网络之间的交互日益频繁，网络边界的模糊化趋势愈发明显。火力发电厂作为关键能源基础设施，其信息区域（即“第三区”）不仅承载了管理系统、运维平台等核心服务，也与互联网有较高程度的连接性。在远程维护、文件交换和终端接入等典型场景下，边界暴露面不断扩大，成为攻击者突破防线、渗透高权限系统的重要入口[4]。攻击行为往往通过社会工程、网络扫描、凭据滥用等方式进入第三区，再实施横向渗透或数据外泄操作，严重威胁电厂信息系统的稳定性与数据完整性。因此，研究攻击链条及其关键行为特征，构建具备识别性与响应力的防护模型，已成为火电厂信息安全的关键任务。

一、国内外相关研究现状

随着电力行业不断推进数字化转型，工业控制系统与办公信息网络之间的交互日益频繁，网络边界的模糊化趋势日益明显。作为与互联网连接的重要接口区，第三区的信息系统在安全性上面临前所未有的挑战。

在国内，研究工作正由早期的隔离防护向综合纵深防御体系演进。典型成果包括可信终端接入架构、双向隔离机制、Web 与 VPN 等服务接口的精细化控制策略等。相关研究强调通过统一身份认证、安全审计和行为分析手段提升系统的整体安全性与响应能力[7][8]。近年来也逐渐引入零信任理念，在多因子认证、动态授权和行为感知等层面构建更具适应性的安全防线。在国际领域，美国 NIST 的 SP800-207《零信任架构》和 IEC 62443 标准为信息系统与控制系统之间的边界隔离与安全通信提供了结构化指导[5][6][10]。同时，一些研究聚焦于多阶段攻击链建模、基于行为的入侵检测机制以及策略动态调整框架等，形成了完整的从“识别—防御—响应—恢复”全过程管理体系。

总体而言，国内外研究都指出信息区域安全的核

心在于：构建可持续感知、可动态响应的边界安全机制，以限制攻击者的潜伏空间和横向移动能力。

二、研究思路与技术路线

针对上述问题，本文以“攻击识别—模型构建—策略部署”为主线，首先基于 MITRE ATT&CK 框架对火电厂信息区常见攻击路径进行系统建模，形成贯穿攻击前期侦察、中期渗透与后期持久化的攻击链视图。结合真实案例与安全日志分析，总结出包括网络钓鱼诱导、远程命令执行、横向权限提升、数据外传及后门植入等在内的典型攻击流程，提取了如异常 IP 连接、登录失败频率激增、非工作时间异常行为等行为指标，构建风险数据库并作为后续动态检测机制的核心特征输入，提升系统对“合法外壳、恶意行为”的攻击识别能力。

在防护体系设计上，本文融合零信任架构与纵深防御理念，提出一套针对火电厂信息区域的边界防护模型，围绕“身份可信、通道加密、行为感知、日志审计”四大核心原则展开部署。一方面通过多因子认证与集中式权限控制平台强化用户身份识别机制，确保接入源合法；另一方面，在通信路径中全面采用加密通道及动态访问控制策略，阻断非法连接通道；同时结合终端检测响应（EDR）与用户行为分析（UEBA）手段，建立基于行为特征的持续监测能力，并依托 SIEM 平台构建联动审计机制，实现攻击的事中识别与事后溯源。此外，通过微分段与细粒度策略控制，实现信息区内最小权限访问，限制横向移动范围，从体系结构上压缩攻击面。该模型具备策略分层清晰、兼容性高、部署灵活等优势，可为火力发电厂信息区域的网络安全防护提供可复制、可评估的技术路径。

为验证所提防护模型的实际效果，本文构建了包含 VPN 网关、Web 管理平台、文件传输通道等典型组件的仿真信息区域网络环境，并通过模拟多种攻击行为（如远程命令执行、会话劫持、横向渗透等）对防护体系进行实证测试。实验结果表明，在部署零信任导向的访问控制与行为监测策略后，系统对未经授权访问行为的检测率达 92.7%，横向移动攻击的拦截成功率提升至 89.3%。同时，借助日志集中分析平台实现了攻击链的可视化追踪，事件响应平均延迟由原先的 5 分钟缩短至 1.8 分钟。在对比测试中，未部署本模型的基线系统在遭遇组合攻击时的平均可用性维持在 83.6%，而集成防护模型后系统稳定性提升至 95% 以上，误报率控制在 3% 以内。

综上，本文提出的边界纵深安全模型不仅在理论结构上具备可迁移性与可扩展性，在实际部署环境中也展现出较强的攻击拦截与事件响应能力。未来研究可进一步结合 AI 驱动的行为识别模型与自动化策略调整机制，提升模型的动态适应性与智能联动水平，为火电厂信息区域网络安全建设提供更加稳健的技术保障。

三、信息区域边界纵深防护模型

基于前述攻击链建模与策略分析结果，本文构建了一套面向火力发电厂信息区域的边界纵深防护模型。该模型采用“分层隔离、身份验证、行为识别、策略联动”的整体结构，目标在于打通识别、分析、防护、响应全过程，使得攻击行为无论从入口还是内部传播路径均被动态拦截。

模型的第一层为接入控制与身份验证层，主要用于阻断未经授权或凭据滥用的接入尝试。系统在此阶段引入多因子认证机制（如动态令牌 + 设备绑定），并通过集中式身份管理平台对接入者进行实时权限核查与策略匹配。所有访问请求均需通过统一的访问控制网关，该网关内嵌基于角色的访问控制（RBAC）与基于属性的访问控制（ABAC）引擎，从身份源、访问情境和行为模式多维度动态授权，确保访问过程具备最小权限、最短持续时间和最窄访问路径。

第二层为通道加密与通信控制层，系统采用 TLS 1.3 标准对数据传输进行端到端加密，确保在传输路径中攻击者无法嗅探或篡改通信内容。对于 VPN 远程接入通道，平台通过启用分布式防火墙与 VPN 行为审计模块，对接入行为进行路径溯源与策略自适应配置。该机制能够识别出如“隧道协议异常切换”“高频连接尝试”“数据包封装特征偏离”等行为，第一时间发出警报并触发策略限制。

模型的核心层为行为感知与动态识别层。该

层通过引入UEBA（User and Entity Behavior Analytics）模块，对用户与设备行为构建多维画像，借助机器学习算法（如聚类分析、异常点检测）对非预期行为进行实时识别。例如，模型能快速识别出“非工作时间登录行为”“低权限账户访问高敏数据”“终端短周期内频繁跨区域跳转”等特征模式，一旦与既有攻击链特征匹配，即触发后续联动响应机制。配合风险数据库的持续更新，行为识别模块能在实际部署中显著提高早期威胁发现能力。

第四层为纵深隔离与策略落地层。本层通过部署微隔离（micro-segmentation）技术，将信息区域内系统划分为多个逻辑子网，核心资源仅向明确授权的终端或用户开放访问。模型在每个隔离区边界部署策略转发点（Policy Enforcement Point, PEP），对网络流量进行流级别访问控制。该机制确保即使攻击者攻破某一节点，其后续的横向移动受限于策略隔离，无法继续扩散攻击路径。

最后一层为策略编排与联动响应层，系统借助SIEM平台统一收集日志、行为、策略与警报数据，进行威胁等级评估与响应流程触发。平台通过预设响应模板与脚本，实现自动隔离、策略调整、告警通报与溯源分析等功能闭环。实际部署中，当系统识别出某账号存在高风险行为时，可在5秒内完成访问中断、策略收敛与事件上报。

模型实施验证表明：在模拟攻击环境中，该防护体系对远程命令执行攻击识别率达92.7%，横向渗透拦截成功率提升至89.3%，有效降低了基于合法身份下实施异常行为的攻击成功概率。同时，系统平均误报率控制在3%以内，关键业务系统在受到攻击时仍能保持95%以上的服务可用性，体现出该模型在实战环境下的高可靠性、响应及时性与安全防护深度。

综上所述，该模型通过多层次联动、动态响应机制与可持续学习策略的协同作用，为火力发电厂信息区域构建起一套高度可操作、可评估、可迭代的纵深安全防护体系，在提升整体网络韧性与应急处置能力方面具有良好推广应用价值。

四、策略评估体系构建与部署建议

为进一步推动信息区域边界纵深防护模型的落地实施与可持续优化，本文基于前期实验评估结果与行业实际需求，构建了一套面向火力发电厂的安全策略评估体系，并提出分层分级部署建议。

在实际应用适配方面，本文根据电厂规模与信息系统复杂程度提出了差异化部署建议。对于小型或单体运行的发电厂，建议以轻量化边界防护为主，重点部署VPN接入管控、行为审计模块与多因子认证组件，优先实现外部访问控制与账户权限清理。在此基础上，结合微隔离策略对关键节点进行网络分段，有效提升初始防护水平。对于具备多个厂站、存在集团集中运维模式的企业类型，则应以集中控制平台为核心，统一管理认证接入、策略下发与日志采集，构建跨区域、可编排、可视化的安全运营中心（SOC）。该模式通过引入策略编排引擎与自动化分析工具，实现对下属站点统一管理与动态风险响应。

在推广路径方面，本文建议采取“核心先行、逐步扩展”的分阶段部署策略。首阶段应聚焦于VPN网关、邮件系统、Web服务等关键访问入口，部署集中认证平台、UEBA行为分析系统与EDR终端响应机制，快速建立初步防护体系。第二阶段拓展至跨系统访问控制与策略动态更新功能，引入微隔离网关与策略联动平台，实现多维度策略响应与攻击链级联分析能力。最后阶段则结合AI辅助策略生成与自适应检测模型，实现防护系统的智能化与闭环优化。在策略维护方面，应建立基于威胁情报的持续更新机制，结合安全事件演练与策略版本控制，形成“部署—评估—优化”三位一体的策略生命周期管理闭环。

五、结论与展望

本文围绕火力发电厂信息区域（第三区）面临的边界安全挑战，提出并验证了一种融合攻击链建模、行为特征提取与纵深防护策略于一体的信息区网络安全防护模型。研究结果表明，基于MITRE ATT&CK攻击链视图所建立的识别机制能够高效提取远程命令执行、横向渗透、会话劫持等典型威胁路径，并结合异常登录、非工作时间操作等关键行为特征，构建了具备实战价值的风险数据库，为模型部署提供了可靠的

数据支撑。

通过引入纵深防御与零信任架构理念，本文构建了分层隔离、身份验证、行为感知、策略联动的整体模型架构，实现了从接入控制、通道加密、行为建模到策略响应的闭环机制。仿真结果表明，该模型在攻击拦截率、响应时延、误报控制与系统可用性等多个关键指标上均优于传统防火墙式边界策略，有效遏制了以合法外壳伪装的攻击路径和内部横向移动行为，显著增强了第三区在高威胁环境下的安全韧性与管控能力。

同时，本文还结合电厂实际运行环境，设计了差异化部署策略与可评估的策略落地指标体系，为不同规模和组织架构的电厂信息区安全建设提供了分阶段、可复制的推广路径。特别是在集中认证、微隔离策略、行为识别与策略联动方面所构建的技术框架，具备良好的兼容性、可维护性与扩展性，已具备工程化实施条件。

展望未来，随着电力行业数字化水平不断提升，第三区信息系统将承载更多的远程协作、数据交互与智能控制任务，网络安全防护所面临的挑战也将持续演进。在此背景下，建议后续研究重点关注以下几个方面：一是进一步融合 AI 驱动的自适应检测机制，提高系统对复杂行为模式和未知威胁的识别能力；二是探索基于威胁情报与攻击图谱的策略动态调整机制，实现模型的持续优化与闭环管理；三是开展多厂区协同防御机制设计与跨区域态势感知研究，提升整体电力系统的信息安全协同保障能力。

参考文献

[1] 张涛，赵东艳，薛峰，张波，章锐．电力系统智能终端信息安全防护技术研究框架 [J]．电力系统自动化，2019，43(19)：1－8.

[2] 陈铁铮．电力监控系统网络安全防护现状及建议 [J]．通信电源技术，2020，37(4)：109－110.

[3] NIST. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82 Revision 2 [EB/OL]. National Institute of Standards and Technology, 2015.

[4] IEC. Industrial communication networks - Network and system security - Part 1-1: General requirements (IEC 62443-1-1) [S]. Geneva: International Electrotechnical Commission, 2018.

[5] Ten C.W., Liu C.C., Manimaran G. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling [J]. IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, 2010, 40(4): 853－865.

[6] Knapp E.D., Langill J.T. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems [M]. Waltham: Elsevier, 2011.

[7] 高翔，梁宗裕．浅谈电力监控系统网络安全防护技术研究 [J]．网络安全技术与应用，2021(9)：123－124.

[8] 刘睿，洪晟，李伟，王欣．面向工业控制系统的入侵检测技术综述 [J]．信息技术与网络安全，2021，40(3)：1－7.

[9] 孙彦斌，汪弘毅，田志宏，方滨兴．工业控制系统安全防护技术发展研究 [J]．中国工程科学，2023，25(6)：126－13.

[10] NIST. Zero Trust Architecture: NIST Special Publication 800-207 [EB/OL]. National Institute of Standards and Technology, 2020.

作者简介：候安宁(1999-)男，汉族，甘肃省，学士，助理工程师，研究方向：网络安全在火电厂的应用。