文章类型：论文|刊号（ISSN）：2972-4112(P) / 2972-4120(O)

热工控制系统网络安全防护与异常检测

吕昊阳
华电库车发电有限公司
DOI:10.32629/pe.v4i1.19006

[摘　要] 热工控制系统作为电力、化工、冶金等关键基础设施的核心组成部分,其稳定运行直接关乎工业生产安全与社会公共利益。随着工业信息化与智能化的深度融合,热工控制系统逐渐打破封闭架构,向网络化、互联化转型,在这一过程中,网络安全漏洞与威胁隐患大幅增加,病毒入侵、恶意攻击、数据篡改等安全事件频发,对系统运行可靠性构成严峻挑战。本研究基于热工控制系统的结构特性与运行规律,深入剖析当前系统面临的网络安全风险与威胁类型,系统阐述网络安全防护体系的构建思路与关键技术,重点研究异常检测的核心方法与实现路径,为提升热工控制系统网络安全防护能力、强化异常检测精准度提供理论支撑。
[关键词] 热工控制系统；网络安全防护；异常检测
中图分类号：G250.72　文献标识码：A

Network Security Protection and Anomaly Detection for Thermal Control Systems

Haoyang Lv
Huadian Kuche Power Generation Co., Ltd.

[Abstract] Thermal control systems, as a core component of critical infrastructure in power, chemical, and metallurgical industries, directly impact industrial production safety and public interests through their stable operation. With the deep integration of industrial informatization and intelligentization, thermal control systems are gradually breaking away from closed architectures and transforming towards networking and interconnection. During this process, network security vulnerabilities and threats have increased significantly, with frequent security incidents such as virus intrusions, malicious attacks, and data tampering, posing a severe challenge to system reliability. This research, based on the structural characteristics and operational patterns of thermal control systems, deeply analyzes the current network security risks and threats faced by these systems. It systematically elaborates on the construction ideas and key technologies of a network security protection system, focusing on the core methods and implementation paths of anomaly detection, providing theoretical support for improving the network security protection capabilities of thermal control systems and enhancing the accuracy of anomaly detection.
[Key words] Thermal control system; Network security protection; Anomaly detection

引言

在工业4.0推动下,工业控制系统向分布式网络控制转型,热工控制系统作为调控温度、压力等参数的关键子系统,广泛应用于火电、核电等能源密集型行业,其稳定运行直接关乎工业生产安全。加强热工控制系统网络安全防护与异常检测研究,构建智能化防护体系,实现异常精准识别与响应,成为保障关键基础设施安全运行的迫切需求。本研究将围绕风险分析、旨在为防护体系构建及异常检测技术展开研究作参考。

1 构建热工控制系统网络安全防护体系

1.1网络边界防护

网络边界是热工控制系统抵御外部威胁入侵的第一道防线,其防护核心是实现工业控制网与外部网络(如企业管理网、互联网)的安全隔离与可控访问。首先,应采用物理隔离与逻辑隔离相结合的方式,强化网络边界隔离效果。工业防火墙作为网络边界防护的关键设备,应具备针对工业控制协议的深度解析与过滤功能。网闸通过“物理隔离+数据摆渡”的方式,实现工业控制网与外部网络之间的安全数据传输[1]。网闸在工作过程中,会切断两个网络之间的直接连接,通过内部的存储介质实现数据的单向传输,有效防止外部网络中的病毒、恶意代码等威胁通过数据传输环节入侵热工控制系统。在实际应用中,应根据数据

传输的需求,合理配置网闸的传输策略,确保数据传输的安全性与实时性[2]。

1.2终端设备防护

终端设备是热工控制系统的基础组成部分,包括DCS控制器、智能仪表、传感器、执行器以及操作员站、工程师站等,其安全性能直接影响整个系统的安全稳定运行。因此,强化终端设备防护是网络安全防护体系的重要环节。部门可以先加强终端设备的硬件安全防护,对关键控制设备(如DCS控制器)进行物理防护,设置专用的设备机房,配备门禁系统、视频监控系统等,防止设备被非法接触与篡改[3]。部门还可以强化终端设备的软件安全防护;而对于智能终端设备,应及时更新设备固件与操作系统补丁,修复已知安全漏洞;关闭设备上不必要的端口与服务,减少攻击面; 配置强密码与身份认证机制,防止设备被非法登录。对于操作员站、工程师站等终端主机,应安装工业级杀毒软件、主机入侵检测系统(HIDS)等安全软件,实时监测主机的运行状态,及时发现与清除病毒、恶意代码等威胁。另外对于老旧终端设备,由于其硬件性能落后,无法支持最新的安全防护技术,需要制定合理的设备更新改造计划,逐步替换老旧设备;对于暂时无法替换的设备,可以采取隔离防护措施,限制其与其他设备的通信范围,降低安全风险。

1.3通信安全防护

通信安全是保障热工控制系统数据传输完整性与机密性的关键,针对工业控制协议的安全缺陷,部门需要从协议优化、数据加密、身份认证等方面入手,强化通信安全防护。首先,应逐步升级与替换老旧的工业控制协议,推广使用具有安全功能的新型协议。例如,将传统的Modbus协议升级为ModbusTCPSecure协议,利用SSL/TLS加密技术对数据传输进行加密处理; 采用OPCUA协议替代OPCClassic协议,通过内置的身份认证、权限控制与数据加密功能,提升数据交换的安全性。协议网关可实现不同协议之间的转换,并在转换过程中对数据进行过滤、验证与加密,防止恶意指令通过协议漏洞入侵系统;协议过滤则通过解析协议数据包的内容,识别并拦截不符合规范的指令与数据,保障通信安全。可建立完善的身份认证与权限控制机制,对参与通信的设备与用户进行严格的身份验证; 还可采用数字证书、USB密钥、生物识别等多种身份认证方式,确保设备与用户的合法性;基于角色的访问控制(RBAC)模型,为不同用户与设备分配不同的操作权限,严格限制对核心控制指令与敏感数据的访问权限,防止未授权操作。

1.4数据安全防护

热工控制系统中的数据包括实时控制数据、设备运行数据、生产工艺数据等,这些数据是系统运行与生产调度的核心依据,其安全性直接关乎工业生产的稳定与安全。数据安全防护应围绕数据采集、传输、存储、使用等全生命周期,采取加密存储、数据备份、访问控制、数据脱敏等多种技术手段,保障数据的完整性、机密性与可用性[4]。部门在数据采集环节,应确保数据采集设备的合法性与数据采集过程的安全性,防止数据被篡改或伪造。采用加密传输技术,对采集的数据进行实时加密处理,确保数据在传输过程中不被窃取或篡改。在数据存储环节,应采用加密存储技术,对敏感数据进行加密处理后再存储到数据库中;同时,建立完善的数据备份与恢复机制,定期对数据进行备份,备份介质应进行异地存储,确保在系统发生故障或安全事件时,能够快速恢复数据,减少损失。在数据使用环节,需要加强对数据访问的权限控制,严格限制不同用户对数据的访问范围与操作权限;对敏感数据进行脱敏处理,在不影响数据使用价值的前提下,隐藏数据中的敏感信息,防止敏感数据泄露。

1.5安全管理体系建设

技术防护是网络安全防护体系的基础,而完善的安全管理体系则是保障技术防护措施有效实施的关键。热工控制系统的运营企业应建立健全网络安全管理制度,明确各部门与人员的网络安全职责,形成“全员参与、层层负责”的安全管理格局。部门需要首先制定完善的网络安全管理制度,包括设备管理制度、权限管理制度、安全补丁管理制度、应急响应制度等,规范各项操作流程,确保网络安全工作有章可循。另外,部门还需要加强网络安全培训与教育,增强工作人员的网络安全意识与专业能力。定期组织网络安全培训,内容涵盖网络安全风险识别、安全防护技术、应急处置流程等方面; 开展网络安全应急演练,提升工作人员应对网络安全事件的处置能力。同时还需要建立严格的人员准入与考核机制,对参与热工控制系统操作与管理的人员进行严格的背景审查与专业考核,确保人员的可靠性与专业性。对于建立健全网络安全应急响应机制,制定详细的应急响应预案,明确应急响应流程、各部门职责与处置措施。部门可定期对预案进行修订与完善,确保预案的针对性与可操作性。当发生网络安全事件时,能够快速启动应急响应预案,及时采取有效的处置措施,控制事件影响范围,降低损失[5]。此外,还需要加强与政府部门、安全服务机构的合作,建立网络安全信息共享机制,及时获取最新的网络安全威胁信息与防护技术,提升系统网络安全防护能力。

2 热工控制系统异常检测技术研究策略

2.1基于统计分析的异常检测技术

基于统计分析的异常检测技术是最早应用于工业控制系统异常检测的技术之一,其核心原理是通过对热工控制系统正常运行状态下的关键参数(如网络流量、控制指令、设备运行参数等)进行统计分析,建立正常运行模式的统计模型,然后将实时监测到的参数与统计模型进行对比,当参数偏离模型的阈值范围时,判定为异常行为。本研究使用均值方差法通过计算正常运行状态下参数的均值与方差,设定合理的阈值范围,当实时参数的取值超出阈值范围时,判定为异常。而聚类分析法则通过对大量正常运行数据进行聚类,形成多个正常数据簇,将实时监测数据与正常数据簇进行匹配,若数据无法匹配到任何正常数据簇,则判定为异常。该方法适用于参数分布较为复杂的热工控制系统,能够有效识别出与正常运行模式差异较大的异常行为。贝叶斯推理法则基于贝叶斯概率模型,通过计算实时数据属于正常

模式的概率,当概率低于设定阈值时,判定为异常。该方法具有较强的不确定性推理能力,能够有效处理热工控制系统中数据的噪声与不确定性。一方面,该技术对统计模型的依赖性较强,当热工控制系统的运行工况发生变化时,正常运行模式也会随之改变,若统计模型无法及时更新,将导致大量的误告警或漏告警;另一方面,该技术难以有效识别出与正常运行模式差异较小的隐蔽异常行为,如缓慢的参数漂移、微小的恶意指令篡改等。

2.2基于机器学习的异常检测技术

随着机器学习技术的发展,其在工业控制系统异常检测中的应用越来越广泛。基于机器学习的异常检测技术通过对热工控制系统的历史运行数据进行训练,建立能够自动识别正常与异常运行模式的机器学习模型,然后利用该模型对实时监测数据进行分类与判断,实现异常行为的检测。与基于统计分析的技术相比,机器学习技术具有更强的自适应能力与模式识别能力,能够有效应对热工控制系统运行工况的变化与复杂的异常行为。常用的机器学习算法包括支持向量机(SVM)、决策树、随机森林、K近邻(KNN)等。支持向量机通过寻找最优分类超平面,将正常数据与异常数据区分开来,具有较强的泛化能力,适用于高维数据的异常检测。在热工控制系统中,可将网络流量的多个特征参数(如数据包长度、传输频率、协议类型等)作为输入,通过支持向量机模型进行训练,实现对异常网络流量的检测。

决策树算法通过构建树状结构的分类模型,根据数据的特征参数逐步进行决策,最终判定数据的类别(正常或异常)。该算法具有模型解释性强、计算速度快等优点,适用于对实时性要求较高的异常检测场景。随机森林则是基于多个决策树的集成学习算法,通过组合多个决策树的预测结果,提高异常检测的准确性与稳定性,能够有效降低单一决策树的过拟合问题。K近邻算法通过计算实时监测数据与历史数据集中各数据点的距离,选取距离最近的K个数据点,根据这K个数据点的类别判定实时数据的类别。该算法具有原理简单、无需训练过程等优点,适用于数据分布较为均匀的热工控制系统异常检测。然而在处理大量实时数据时存在一定的局限性。

2.3基于深度学习的异常检测技术

基于深度学习的异常检测技术是近年来的研究热点,其通过构建深层神经网络模型,能够自动提取热工控制系统运行数据中的深层特征,实现对复杂异常行为的精准识别。与传统的机器学习技术相比,深度学习技术具有更强的特征学习能力与模式识别能力,能够有效处理热工控制系统中大量的非线性、高维度数据,适用于对异常检测精度要求较高的场景。

常用的深度学习模型包括自编码器(AE)、循环神经网络(RNN)、长短期记忆网络(LSTM)、卷积神经网络(CNN)等;当实时监测数据为正常数据时,重构误差较小;当数据为异常数据时,重构误差将显著增大[4]。自编码器适用于缺乏异常数据标签的热工控制系统异常检测场景,具有较强的实用性。热工控制系统的运行参数(如温度、压力、流量等)具有明显的时序特征,通过循环神经网络或长短期记忆网络模型,能够学习到正常运行时序数据的变化规律,当实时时序数据偏离正常规律时,判定为异常[5]。卷积神经网络则擅长提取数据中的空间特征,在热工控制系统的图像数据(如设备监控图像、红外测温图像等)异常检测中具有广泛的应用;部门可以通过卷积神经网络模型,能够自动提取图像中的纹理、形状等特征,识别出设备异常状态(如设备损坏、泄漏等);但基于深度学习的异常检测技术也存在一定的不足,如模型训练需要大量的历史数据、计算复杂度高、模型解释性差等,在实际应用中需要结合热工控制系统的具体需求进行优化。

3 结语

热工控制系统作为关键基础设施核心,其网络安全关乎工业生产与公共利益。本研究通过分析系统安全风险,提出涵盖多维度的全方位防护体系思路,探讨了多种异常检测技术的应用。防护体系构建需要技术与管理结合,未来将随工业互联网等技术向智能化、一体化发展。同时,需跨领域协同完善标准、强化技术研发,提升核心技术自主可控性,以保障系统安全运行,护航工业经济高质量发展。

[参考文献]

[1]吴铮,张悦,董泽,等.基于多模型融合的热工过程异常值处理方法[J].计算机仿真,2024,41(2):108-114.

[2]张文卿.火电厂热工自动化系统检修常见问题要点分析[J].机械与电子控制工程,2024,6(20).

[3]张丽.电厂热工自动化系统检修常见问题分析及处理[J].科技创新与应用,2019(36):145-146.

[4]张明法,杨慎敏,魏向国,等.火电机组控制系统网络安全防护若干问题[J].自动化应用,2020(11):60-61,64.

[5]徐龙涛.电厂热工控制系统应用中的抗干扰技术[J].科学技术创新,2024(9):217-220.

作者简介：

吕昊阳(1994--),男,汉族,陕西汉中市人,大专,助理工程师,研究方向：热工控制。