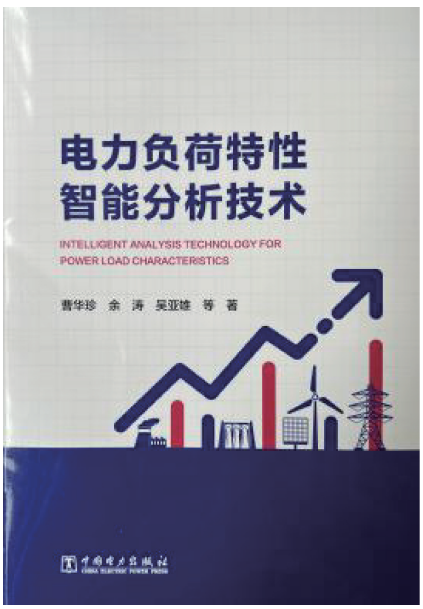
智能电网背景下电力安全防控措施

——评《电力负荷特性智能分析技术》

智能电网通过物联网、大数据分析及人工智能算法实现电力流、信息流与业务流的高效协同。然而,网络攻击频次激增、设备漏洞复杂化及新能源接入带来的不确定性,使电力信息安全风险呈现跨域传导特征。传统被动防御模式已难以适应动态攻击场景,构建基于主动理念的电力智能安全防控体系成为保障能源供应链安全的关键方式。智能电网深度融合信息通信技术与能源系统,其通过数据驱动型风险预警机制与动态响应体系,有效提升电网对复杂工况的适应性,保障新型电力系统“物理-信息-市场”的耦合稳定性。防控措施不仅强化了设备全生命周期管理,降低非计划停运风险,更通过构建协同防御网络,抵御网络攻击与极端天气等复合型威胁,为保障我国电力能源的稳定供应与智能化管理升级提供了现实可行路径。



书名:电力负荷特性智能分析技术
作者:曹华珍,余涛,吴亚雄 等
出版社:中国电力出版社
ISBN:9787519874810
出版时间:2023年12月
定价:49元

笔者在开展工业负荷聚合调节关键技术研究及应用(SGTYHT/23—JS—003)研究过程中,认真阅读了《电力负荷特性智能分析技术》一书,该书以解决传统负荷特性分析的局限性为切入点,在数据预处理层面提出创新性方法,将生成对抗网络引入负荷数据超分辨率重建,有效提升了低精度数据的可用性,为后续分析奠定了可靠的数据基础。在分析方法论上,该书突破单一维度分析模式,构建了“用户-行业-影响因素”三位一体的多维度分析体系,通过用户画像与行业画像的深度融合,实现了负荷特性的精细化刻画。书中提出的新报装用户负荷预想画像技术,将历史数据与预测模型相结合,为业扩报装决策提供了前瞻性技术支撑。全书结构严谨,理论创新与技术落地并重,既系统梳理了负荷特性研究的演进脉络,又通过模块化开发设计展现了智能分析技术的工程可操作性。

该书作者指出,在智能电网数字化转型进程中,数据安全已成为电力系统安全运行的核心风险维度。智能电网的海量异构数据在采集、传输、存储、分析环节面临复合型安全威胁,需构建覆盖数据全生命周期的纵深防御体系,实现从感知层到应用层的多维安全保障。数据采集作为智能电网运行的初始环节,其安全性直接影响后续数据处理的有效性。针对终端设备计算资源受限的特点,需采用基于国密算法的轻量级加密协议,结合边缘计算节点实现终端数据的本地化预处理。具体而言,通过国密SM4算法对感知层数据进行对称加密,动态密钥协商机制可确保密钥的时效性与唯一性,防止中间人攻击。边缘计算节点的部署能够减少原始数据向云端传输的频次,通过本地化特征提取与异常检测,降低网络传输负载的同时提升数据隐私保护能力。此外,针对5 G网络切片技术在电力通信中的应用,需建立基于零信任架构的访问控制模型,通过持续认证与微隔离技术实现细粒度权限管理,解决网络边界模糊化带来的安全风险。数据传输环节的安全保障需兼顾加密强度与传输效率,量子密钥分发技术可为关键业务数据流提供理论无条件安全的传输通道,结合TLS 1.3协议实现端到端加密,可有效抵御量子计算攻击与传统密码破解。对于非实时性要求较高的历史数据,可采用区块链技术构建分布式账本系统,通过智能合约定义数据操作规则,实现数据变更的自动审计与不可篡改特性。区块链的共识机制可确保跨域数据协同的可靠性,而分片技术与轻量级节点部署能解决智能电网大规模数据存储的扩展性问题。工业控制系统历史数据的存储与分析需平衡数据共享需求与隐私保护要求。基于联邦学习的隐私保护分析框架,可通过多方安全计算实现跨域数据协同分析,原始数据无需离开本地即可完成模型训练,有效解决了数据孤岛与隐私泄露的矛盾。在安全评估层面,需建立动态安全评估机制,运用博弈论模型量化各环节安

全收益与成本,通过强化学习算法实现防护策略的自主优化。该机制可基于历史攻击数据与系统运行状态,动态调整加密算法强度、访问控制策略等参数,形成闭环反馈的安全防护体系。

笔者认为,智能电网物理系统与信息系统的深度耦合也催生了安全防护系统的新型脆弱性,传统分立式安全防护模式已难以应对跨域攻击。基于数字孪生的实时安全防护框架通过物理-信息空间的映射与交互,可实现脆弱性的动态感知与主动防御。物理层设备的安全状态监测是防护框架的基础。开发具有自感知能力的智能电网设备,集成光纤光栅传感技术与电磁指纹识别模块,可实时采集设备温度、振动、电磁特征等多维数据。光纤光栅传感技术通过光信号变化反映设备机械应力与温度分布,电磁指纹识别通过设备辐射的电磁信号特征实现身份认证与异常检测。针对变电站设备,采用三维激光点云建模技术构建高精度数字孪生体,结合有限元分析模拟设备在不同工况下的应力分布,预测潜在故障模式。迁移学习算法可利用历史故障数据训练预测模型,实现异常状态的早期预警。信息物理系统的交互特性使得攻击可能跨越物理与信息空间。建立基于攻击树模型的混合威胁预测系统,通过深度强化学习模拟攻击者决策路径,可提前识别关键节点与攻击路径,部署针对性防御策略。针对电力物理信息系统特有的时空关联特性,开发基于时空图卷积网络的异常检测算法,融合设备空间分布与时间序列数据,可有效识别虚假数据注入攻击与协同式网络物理攻击。通过图卷积捕捉设备间的空间关联,结合时间卷积分析状态变化趋势,提升对复杂攻击模式的检测精度。控制层的安全防护需兼顾系统可靠性与响应速度。设计具有容错能力的自适应保护装置,可采用多智能体协商机制实现保护定值的在线动态调整。多智能体系统通过分布式决策减少中心化控制延迟,各保护单元基于局部状态信息与邻域通信,协商确定最优保护策略,提升系统对连锁故障的抵御能力。为支撑安全决策,需配套建设电力安全知识图谱,通过自然语言处理技术整合历史故障案例、设备参数、安全规程等多源异构数据,构建包含实体、关系与规则的语义网络。知识图谱可支持因果推理与关联分析,为安全运维人员提供决策依据。

伴随着人工智能(Artificial Intelligence,AI)技术快速进步,智能电网安全防控模式亦随之发生深刻变革——从传统的被动响应转向主动预测,从单点防御升级为系统协同。智能电网建构及运营过程中,AI 与安全防控深度融合的关键在于构建智能决策与自主演化机制,引导安全防控系统朝着智能自主决策模式演进,具体需要引入深度学习技术,且通过多模态数据融合分析提升检测效能。在具体实践操作中,将擅长捕捉空间特征的卷积神经网络与擅长分析时间演化特征的长短期记忆网络结合,全面深度解析网络流量的时空特性,增强对未知攻击的识别能力。针对深度学习模型存在的“黑箱”问题,亦可构建基于因果推理的威胁检测框架,同时,运用贝叶斯网络或结构因果模型分析事件间的因果关系,区分正常操作与恶意行为。上述方式既能降低误报率,又为安全响应提供更可靠的决策依据。安全防控也需要讲究自主性,多智能体系统通过分布式决策实现局部控制与全局协调,即每个智能体基于局部观测信息与邻域通信,采用协商或竞争机制达成共识。强化学习算法则赋予智能体自主学习能力,使其通过与环境交互持续优化决策策略,如在分布式能源接入场景中,智能体可学习最优的功率分配与保护定值调整策略,兼顾系统安全与经济性。虽然 AI 能显著提升安全防控效率,但是人类专家的经验与判断仍不可替代,基于此,有必要构建人机协同机制,实现安全分析师与 AI 系统的优势互补体系。AI 系统负责实时监测、数据解读、初步分析与策略建议,安全分析师则进行最终决策与模型优化。为提升人机协同效率,可开发交互式可视化平台,将 AI 系统的检测结果、因果推理过程以直观的图示方式呈现,辅助分析师快速定位、决策并解决问题。

综上,智能电网安全防控体系的建构,需通过数据全生命周期管理、数字孪生映射与 AI 技术的深度融合,实现从单点防御到系统协同的范式转变。在数据安全层面,国密算法与区块链技术的协同应用,为跨域数据交互提供可信技术保障;在态势感知维度,时空图卷积网络与攻击树模型的结合,可有效提升复杂攻击场景的检测精度;在自主决策方面,多智能体强化学习机制突破了传统规则驱动的局限,实现了防护策略的动态优化。面对能源数字化转型带来的新型脆弱性,必须持续推进安全防护理论与工程实践的协同创新,通过知识图谱构建、因果推理框架及人机协同机制,形成具备自适应进化能力的智能安全防护体系,为新型电力系统建设提供坚实的技术支撑。

(陆骏/宁波三明电力发展有限公司/高级工程师; 焦阳/宁波三明电力发展有限公司/高级工程师)