配电自动化系统的运维技术分析

阿勒斯坦别克·米娜提汗　邓钰祺　邱家祺
国网新疆电力有限公司乌鲁木齐供电公司　新疆　乌鲁木齐　830000

摘　要：随着新型电力系统建设的加速推进和“双碳”目标的提出，配电网作为连接主网与用户的“最后一公里”，其安全、可靠、高效运行的重要性日益凸显。配电自动化系统（DistributionAutomationSystem,DAS）作为提升配电网智能化水平的核心支撑，已在全国范围内大规模部署。然而，系统的复杂性、设备的多样性以及运行环境的严苛性，给其全生命周期的运维工作带来了前所未有的挑战。本文旨在系统性地分析当前配电自动化系统运维所面临的关键问题，深入探讨涵盖状态感知、故障诊断、智能决策、远程运维及安全防护等维度的先进运维技术，并结合未来发展趋势，提出构建以数据驱动、人工智能赋能、云边协同为特征的新一代智能运维体系的构想，为提升配电自动化系统的健康水平、运行效率和供电可靠性提供理论参考与实践路径。

关键词：配电自动化；智能运维；状态监测；故障诊断；人工智能；网络安全

引言

在能源革命与数字革命深度融合的时代背景下，传统配电网正经历着从被动、单向、无源向主动、双向、有源的深刻变革。在此背景下，配电自动化系统应运而生，其核心目标是通过集成先进的传感、通信、控制与信息技术，实现对配电网的实时监控、快速隔离故障、自动恢复供电以及优化运行管理，从而显著提升供电可靠性和用户服务质量。经过数十年的发展，我国配电自动化已从早期的试点探索阶段迈入全面推广应用阶段。截至2025年底，国家电网公司已在超过90%的城市核心区和70%的城镇区域部署了不同层级的配电自动化系统，覆盖了数百万台配电终端（如FTU、DTU、TTU）。然而，大规模的部署也暴露出运维环节的诸多痛点：海量终端设备的离线率高、数据质量参差不齐、故障定位与处理效率低下、网络安全风险加剧、运维人力成本高昂等。这些问题不仅制约了DAS投资效益的充分发挥，甚至可能因系统自身故障而引发新的安全隐患。因此，如何从传统的“被动响应式”、“经验驱动型”运维模式，转型升级为“主动预测式”、“数据智能驱动型”的现代化运维模式，已成为业界亟待解决的关键课题。

1 配电自动化系统运维面临的挑战

配电自动化系统的运维是一项复杂的系统工程，其挑战主要源于以下几个方面：

1.1 系统架构复杂，设备种类繁多

现代DAS通常采用“主站-子站-终端”三层或“主站-终端”两层架构。其中，终端层包含馈线终端单元（FTU）、站所终端单元（DTU）、配变终端单元（TTU）等多种类型，分别安装于架空线路、环网柜、箱变等不同位置。这些设备来自不同的供应商，采用各异的通信规约（如101/104、MQTT、IEC61850等）和硬件平台，导致系统集成度低、互操作性差，给统一监控、配置管理和软件升级带来了巨大困难。

1.2 运行环境恶劣，设备可靠性要求高

配电终端长期暴露于户外，需承受高温、高湿、强电磁干扰、雷击、凝露等严酷环境考验。同时，其供电通常取自PT或电池，电源稳定性差[1]。这些因素极易导致终端设备出现元器件老化、通信中断、死机重启等问题，造成数据丢失或误报，直接影响主站对电网状态的准确感知。

1.3 数据规模庞大，信息价值密度低

一个中等规模的地市公司DAS，每天可产生TB级的遥测、遥信、事件顺序记录（SOE）等数据。然而，这些数据中蕴含的有效信息（如故障特征、设备劣化趋势）往往被大量的正常运行数据和噪声所淹没。如何从海量异构数据中高效提取高价值信息，是实现智能运维的前提。

1.4 故障机理复杂，诊断难度大

DAS自身的故障可分为硬件故障（如电源模块损坏、通信模块失效）、软件故障（如程序跑飞、配置错误）和通信故障（如通道中断、报文丢包）。这些故障之间往往存在复杂的耦合关系。例如，一次通信中断可能是由终端硬件故障引起，也可能是由光缆被挖断或主站前置服务异常所致。传统的基于告警阈值的简单规则难以准确、快速地定位根因。

1.5 网络安全威胁日益严峻

随着DAS与互联网、移动网络的边界日益模糊，其面临的网络安全威胁呈指数级增长。攻击者可能通过伪

造终端身份、篡改遥控指令、发起拒绝服务（DoS）攻击等方式，破坏系统的完整性、可用性和保密性，严重时可能导致大面积停电事故。这要求运维体系必须将安全防护置于核心地位。

2 配电自动化系统核心运维技术分析

针对上述挑战，业界和学术界提出了多种先进的运维技术，旨在提升DAS的可观、可测、可控、可防能力。

2.1 全景状态感知与健康评估技术

状态感知是运维的基础。新一代DAS运维强调对系统全要素的全景式、精细化感知。（1）终端自诊断技术：在终端设备内部嵌入自检程序，能够周期性地对CPU负载、内存使用率、电源电压、通信链路质量、内部传感器状态等关键指标进行自检，并将自检结果主动上报主站。这使得运维人员无需现场即可初步判断终端的健康状况。（2）主站集中监测技术：主站系统建立统一的设备台账和资产模型，利用大数据平台对所有终端的在线率、通信时延、数据完整率、遥测精度等KPI进行实时统计与可视化展示[2]。通过设定动态阈值，系统可自动识别性能劣化的“亚健康”终端。（3）多源数据融合的健康评估模型：结合历史运行数据、环境数据（如气象信息）、检修记录等多源信息，利用机器学习算法（如支持向量机SVM、随机森林）构建终端健康指数（HealthIndex,HI）评估模型。该模型不仅能给出设备当前的健康状态评分，还能预测其剩余使用寿命（RUL），为精准的状态检修提供依据。

2.2 智能故障诊断与根因分析技术

当系统发生异常时，快速、准确地定位故障点并分析其根本原因是缩短故障处理时间的关键。（1）基于知识图谱的故障推理：构建DAS领域的知识图谱，将设备、通信链路、网络拓扑、告警规则、历史案例等实体及其关系进行结构化表示。当故障发生时，系统可以沿着知识图谱进行多跳推理，综合考虑所有相关告警信号，排除由单一故障引发的连锁告警，从而精准定位到最可能的故障源。（2）基于深度学习的异常检测：利用长短期记忆网络（LSTM）、图神经网络（GNN）等深度学习模型，对终端上报的时序数据流进行建模。模型在正常数据上进行训练后，能够有效识别出与正常模式显著偏离的异常行为，即使该异常尚未触发传统的告警阈值。例如，GNN可以很好地捕捉配电网拓扑结构中相邻终端数据的相关性，从而发现局部区域的异常模式。（3）数字孪生辅助诊断：建立DAS的数字孪生体，在虚拟空间中复现物理系统的实时状态。当物理系统出现故障时，可以在数字孪生体中进行故障注入和仿真推演，快速验证各种可能的故障假设，极大地提高了诊断的效率和准确性。

2.3 预测性维护与智能决策技术

预测性维护（PredictiveMaintenance,PdM）是智能运维的高级形态，旨在“治未病”。（1）故障预测模型：基于前述的健康评估和异常检测结果，利用时间序列预测模型（如Prophet、ARIMA）或生存分析模型，对特定终端在未来一段时间内发生故障的概率进行量化预测。运维资源可以据此进行优先级排序，优先处理高风险设备。（2）智能工单生成与派发：将故障诊断和预测结果与地理信息系统（GIS）相结合，自动生成包含故障位置、疑似原因、所需备品备件、最优路径等信息的电子工单，并通过移动应用推送给最近的运维人员。这实现了从“人找事”到“事找人”的转变，大幅提升了现场处置效率[3]。（3）备品备件智能库存管理：基于历史故障数据和预测性维护需求，利用优化算法动态调整各地仓库的备品备件库存，确保在需要时能够及时供应，同时避免库存积压造成的资金占用。

2.4 远程运维与自动化技术

减少现场作业、提升运维效率是远程运维的核心价值。（1）远程配置与软件升级（OTA）：通过安全加密的通信通道，主站可以对远方的终端进行参数配置、定值修改和固件/软件的远程升级。这解决了过去因版本不一致或配置错误导致的兼容性问题，保证了全网终端的同质化管理。（2）虚拟化与容器化技术：在主站侧，采用虚拟化和容器化（如Docker,Kubernetes）技术部署应用服务。这不仅提高了资源利用率和系统弹性，还使得应用的部署、回滚和扩展变得极为便捷，大大简化了主站系统的运维复杂度。（3）自动化测试与验证：建立自动化的测试平台，在软件升级或配置变更前，能够在仿真环境中对变更内容进行全面的功能和性能测试，确保其不会对生产系统造成负面影响，有效降低了人为操作风险。

2.5 全方位网络安全防护技术

安全是DAS运维的生命线，必须贯穿于设计、建设、运行的全过程。（1）纵深防御体系：构建从终端、通信网络到主站的多层次安全防护体系。在终端侧，采用安全芯片进行身份认证和数据加解密；在网络侧，部署工业防火墙、入侵检测系统（IDS）进行边界防护和流量审计；在主站侧，实施严格的访问控制、操作审计和安全日志分析。（2）零信任安全架构：遵循“永不信任，始终验证”的原则，对任何试图访问DAS资源的主体（无论是内部还是外部）都进行严格的身份认证和权限校验[4]。每一次访问请求都需要重新评估其风险等级，动态授予最

小必要权限。（3）安全态势感知：利用大数据和AI技术，对全网的安全日志、网络流量、终端行为进行实时采集和关联分析，构建全局的安全态势视图。系统能够自动识别高级持续性威胁（APT）等隐蔽攻击，并及时发出预警，实现从被动防御到主动免疫的转变。

3 新一代智能运维体系的构建

面对未来配电网更高程度的数字化、互动化和柔性化需求，DAS的运维体系也必须持续进化。笔者认为，未来的智能运维体系应具备以下核心特征：

3.1 数据驱动为核心

打破数据孤岛，建立统一的数据湖或数据中台，汇聚来自DAS、PMS（生产管理系统）、GIS、营销系统等多源异构数据。通过强大的数据治理能力，确保数据的准确性、一致性和时效性，为上层所有智能应用提供高质量的数据燃料。

3.2 人工智能深度赋能

AI不应仅作为辅助工具，而应成为运维体系的“大脑”。通过持续学习和迭代，AI模型将能够自主完成从状态感知、异常发现、根因分析到决策建议的完整闭环，实现运维知识的沉淀、固化和复用，逐步降低对专家经验的依赖。

3.3 云边协同架构

采用“云-边-端”协同的架构。边缘计算节点（如部署在变电站的边缘代理）负责处理本地实时性要求高的任务（如快速故障隔离、数据预处理），而云端则聚焦于全局性的、计算密集型的任务（如大数据分析、模型训练、资源调度）。这种架构既保证了响应速度，又发挥了云计算的强大算力优势。

3.4 业务流程高度自动化

将运维的最佳实践固化为可执行的自动化工作流（Workflow）。从故障告警触发，到工单生成、人员派发、现场处理、结果反馈、知识归档，整个过程尽可能实现无人干预的自动化流转，形成高效的PDCA（计划-执行-检查-改进）闭环。

4 结语

配电自动化系统作为现代配电网的“神经中枢”，其自身的健康稳定运行是保障电网安全可靠供电的前提。本文系统分析了当前DAS运维所面临的复杂性、可靠性、数据、诊断和安全等五大核心挑战，并深入探讨了以全景感知、智能诊断、预测维护、远程操作和安全防护为代表的先进运维技术。研究表明，未来的DAS运维将不再是简单的设备维护，而是一个融合了物联网、大数据、人工智能、边缘计算和网络安全等前沿技术的综合性智能服务体系。构建以数据驱动、AI赋能、云边协同为特征的新一代智能运维体系，不仅是应对当前运维困境的有效途径，更是释放配电自动化系统全部潜能、支撑新型电力系统高质量发展的必然选择。这需要电网企业、设备厂商、科研机构等多方协同，共同推动运维理念、技术标准和管理模式的创新，最终实现配电自动化系统“更坚强、更智能、更高效”的运维目标。

参考文献

[1]王伟.配电自动化系统的运维技术分析[J].光源与照明,2024,(10):96-98.

[2]单旭.配电自动化系统的运维技术分析[J].集成电路应用,2024,41(09):258-259.

[3]胡彬.配电自动化系统中的智能运维技术分析[J].集成电路应用,2024,41(12):206-207.

[4]吴俊.配电自动化系统的智能运维技术分析[J].集成电路应用,2024,41(12):338-339.