工程与管理科学
Engineering and Management Science
第 8 卷◆第 7 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

电力二次设备常态化安全运维体系构建研究

李洪池　高飞　邓燚
南京国电南自电网自动化有限公司　江苏南京　211100

DOI：10.32629/ems.v8i7.21199

［摘　要］随着新型电力系统建设加速推进，电力二次设备规模持续呈现增长态势且智能化水平不断提升，其安全运维面临设备类型多样、网络风险复杂、运维资源分散等突出挑战。本文基于电力二次设备运维实际情况，提出以“风险预控、状态感知、闭环管控”为核心的常态化安全运维体系框架，从组织架构、技术支撑、流程规范、评价考核这四个维度开展体系设计，构建覆盖设备全生命周期的安全运维机制。

［关键词］电力二次设备；常态化运维；安全防护体系；全生命周期管理

电力二次设备是电网安全稳定运行的神经中枢，它的可靠性和安全性直接关联电力系统整体运行品质，近年来新能源大规模接入且电网智能化转型加速，二次设备种类和数量呈爆发式增长，设备间耦合关系日趋复杂使运维难度显著上升。同时传统以计划检修为主、被动响应为辅的运维模式，在面对设备隐性故障频发、网络安全威胁加剧等新挑战时，逐渐暴露出响应滞后、资源错配、标准不统一等深层次问题。

1 电力二次设备安全运维现状与问题分析

1.1 二次设备运维发展历程与现状特征

电力二次设备运维模式从计划检修持续演进到状态检修再到智能运维，早期运维工作以固定周期检修为主，依靠人工经验判断设备状态，存在效率较低且易造成过度检修或检修不足的问题[1]。随着微电子技术、通信技术与计算机技术的渗透应用，在线监测与故障诊断技术逐步被引入，运维模式开始朝着状态检修转变，设备运行数据的采集与分析能力得到显著增强。近年来以物联网、大数据、人工智能为代表的新一代信息技术加速与电力运维深度融合，智能运维理念随之应运而生，当前二次设备运维呈现出设备类型多样化、运维对象网络化、数据资源海量化等显著特征，运维工作已从单一设备维护拓展为涵盖设备本体、通信链路、应用系统及网络安全的综合保障体系，对运维团队的技术能力、协同水平和管理精细化程度提出了更高要求。

1.2 当前运维体系存在的主要问题

虽然电力企业在二次设备运维方面已经积累了丰富经验，不过现有的运维体系依旧存在着若干突出的短板问题。一方面，制度执行和标准的统一性不够，不同区域以及不同电压等级的运维规程存在明显差异，跨部门协同缺少有效的流程衔接与信息共享机制，这就造成运维资源难以实现集约化的调配。另一方面，技术支撑能力存在明显短板，设备状态感知手段主要还是依靠离线检测和人工巡检，在线监测的覆盖范围比较有限，数据采集的实时性和准确性难以满足精细化运维的实际需求。再一方面，数据孤岛现象较为严重，继电保护、自动化、通信等专业系统各自独立运行，数据标准不统一、接口不一致，跨系统数据融合与综合分析能力较为薄弱，制约了故障预警与智能决策的有效落地。

2 常态化安全运维体系总体框架设计

2.1 体系构建原则与目标

常态化安全运维体系构建要遵循系统性、预防性、闭环性和可量化这四项基本原则，系统性原则要求体系覆盖设备全生命周期，需统筹考虑规划、建设、运维、退役各阶段安全需求以避免碎片化管理。预防性原则强调从被动响应转变为主动预控，要通过状态感知与风险辨识提前发现隐患将故障消灭在萌芽状态[2]。闭环性原则要求运维流程形成完整回路，确保每个环节都具备反馈与改进机制。可量化原则要求建立科学指标体系，让运维绩效能够实现可衡量、可比较、可追溯，基于上述原则体系建设总体目标是构建一套以风险预控为核心、以数据驱动为特征、以闭环管控为保障的常态化安全运维体系，实现二次设备运维从经验驱动向数据驱动、从分散管理向集约协同、从被动处置向主动预防的根本转变。

2.2 体系架构与核心模块

本文提出了“一平台、两机制、三层级”的常态化安全运维体系架构。“一平台”指的是统一运维管控平台，它作为

数据汇聚、业务协同与决策支持的中枢，集成了设备状态监测、运维工单管理、智能分析研判、安全态势感知等功能模块。“两机制”包含风险预警机制和应急响应机制。前者基于设备健康评估与故障预测模型实现风险分级预警，后者针对突发安全事件建立快速响应与协同处置流程。“三层级”分别是决策层、管理层和执行层，决策层负责运维战略规划与资源配置决策，管理层承担制度制定、计划编制、质量监督与绩效评价等职能，执行层负责现场巡检、检修作业、缺陷处置等具体操作[3]。三个层级之间通过统一平台实现信息贯通与业务联动，形成上下协同、横向协同的一体化运维格局。为进一步量化评估该体系架构的运行效果，可引入体系运行综合效能指数，将各核心模块的效能表现进行加权综合，其计算公式如下：

$$E = \sum_{i=1}^{n} w_i \cdot S_i$$

其中，E 为体系运行综合效能指数，S_i 为第 i 个核心模块的效能评分，w_i 为对应权重系数，满足$\sum_{i=1}^{n} w_i = 1$该指数能够直观反映体系各模块的协同运行水平，为后续运维策略的优化调整提供量化依据。

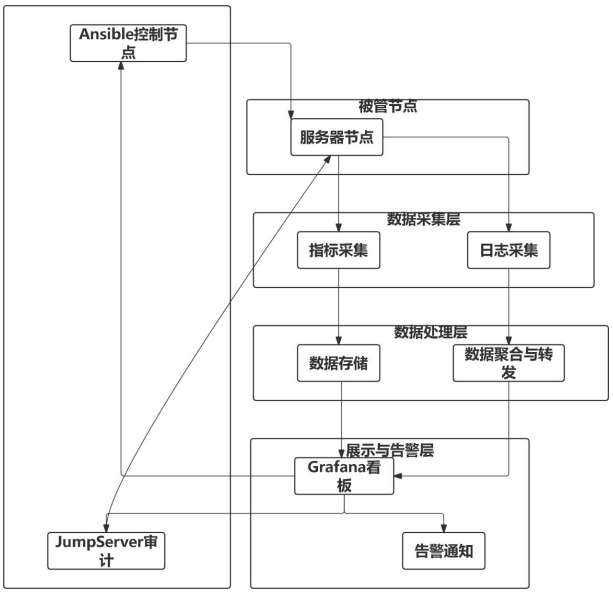

图 1　轻量化运维工具分层部署架构示意图

2.3 体系运行逻辑与协同关系

常态化安全运维体系运行逻辑能概括为闭环循环，在感知环节借助部署于设备侧多类型传感器和智能终端，实时采集设备运行参数、环境状态以及网络行为数据形成全域感知数据池，在研判环节依托大数据分析和人工智能算法，对设备健康状态、故障风险等级和网络安全态势做综合评估生成预警信息与处置建议。在决策环节管理层依据研判结果，结合资源可用性和业务优先级制定运维策略与工单计划[4]。在执行环节执行层按计划完成现场作业并通过移动终端实时回传作业过程与结果数据，在反馈环节系统对运维效果做量化评价并将评价结果纳入知识库与模型优化流程驱动后续运维策略持续改进，各环节之间通过统一平台实现数据贯通和业务联动。

3 组织管理与制度保障体系

3.1 运维组织架构优化

针对当前运维组织层级过多职责交叉响应链条长等问题，本文提出“集中管控 + 属地执行”矩阵式组织模式，在省级或区域层面设立运维管控中心，承担策略制定资源调配技术支撑与绩效评价等统筹职能，实现运维资源集约化管理和跨区域协同调度。在地市或厂站层面保留属地运维团队，负责现场巡检日常维护与应急处置等执行工作，同时配备专业技术骨干负责辖区内设备状态分析与异常研判，管控中心与属地团队通过统一运维平台实现信息实时共享与任务闭环流转，形成“中心决策、属地执行、上下联动”高效协作格局。

3.2 制度标准体系建设

制度标准是保证常态化安全运维体系有效运行的根基，本文从三个层面来构建制度标准体系，在运维规程层面制定覆盖设备巡检检修消缺技改退役等全生命周期的标准化作业指导书，明确各环节操作规范质量控制要点与安全注意事项确保运维作业有章可循有据可查[5]。在安全管理制度层面建立包括网络安全等级保护访问控制漏洞管理应急演练等在内的安全管理制度体系，将安全要求嵌入运维全流程实现业务与安全的深度融合。在考核评价标准层面设计涵盖设备健康指数运维及时率缺陷消除率安全事件数等核心指标的量化评价标准，建立定期考核与动态评估相结合的绩效管理机制以考核促改进以评价促提升。

3.3 人员能力建设与培训机制

运维人员专业素养和技能水平直接影响体系运行最终成效，本文提出分层分类的运维人员能力模型，决策层人员着重战略规划、风险研判与资源统筹能力，管理层人员着重制度执行、流程管控与数据分析能力，执行层人员着重设备操作、故障排查与现场处置能力[6]。建立常态化培训与技能认证相结合的培养机制，培训采用线上理论学习与线下实操演

练相结合方式，定期开展新技术应用、典型故障案例分析与应急演练等专项培训以确保人员知识体系持续更新，认证建立分级技能认证体系并将认证结果与岗位任职资格、绩效考核挂钩，形成闭环提升路径。

4 技术支撑体系构建

4.1 设备状态感知与在线监测技术

全面且精准的状态感知是常态化安全运维的数据根基，本文提出构建“端、边、云”协同的设备状态感知体系，在端侧要在继电保护装置、测控装置、合并单元、智能终端等关键二次设备上部署多类型传感器，以此实时采集电气量、温度、湿度、振动、通信状态等多元参数来实现设备运行状态的全面感知[7]。在边侧利用部署于变电站或区域节点的边缘计算单元对采集数据进行预处理与初步分析，从而实现异常特征的快速提取与本地告警并降低数据传输压力与云端计算负载。在云侧依托统一运维管控平台汇聚全域感知数据，借助大数据存储与处理能力实现海量数据的集中管理与深度挖掘，端、边、云三层之间通过可靠通信网络实现数据高效流转，形成覆盖广泛、响应敏捷的设备状态感知网络为后续的状态评估与故障预测提供高质量数据支撑。

4.2 运维数据融合与智能分析

在数据融合方面，针对继电保护、自动化、通信、网络安全等专业系统存在的数据标准不统一、接口各不相同的问题，建立起统一的数据模型与数据治理规范，通过数据清洗、转换、关联以及标注等操作，将分散在各个系统的结构化与非结构化数据整合为统一的运维数据资产。在智能分析方面，基于融合之后的数据资产，构建设备健康评估模型与故障预测模型，健康评估模型借助多维度状态参数的综合加权与趋势分析，对设备健康状态进行分级量化，故障预测模型依据历史故障数据与运行数据，采用机器学习算法来挖掘故障前兆特征与演化规律，实现对潜在故障的提前预警[8]。建立知识图谱驱动的故障辅助诊断模块，将设备结构、故障模式、处置方案等知识进行结构化表达，为运维人员提供智能化的故障定位与处置建议，提升分析研判的效率与准确性。

4.3 网络安全防护与可信接入

随着二次设备网络化和智能化程度不断持续提升，网络安全已经成为安全运维体系中不可忽视的关键维度，本文设计了纵深防御和可信接入相结合的网络安全防护策略，在纵深防御层面按照“安全分区、横向隔离、纵向认证”总体原则，把二次设备网络划分成不同的安全区域，各区域之间通过防火墙、隔离装置等设备实施严格访问控制与流量过滤，在主机层部署入侵检测与恶意代码防护系统以实时监测异常行为与攻击迹象。在应用层实施身份认证、权限管理与操作审计来确保每一次运维操作可追溯、可审计，在可信接入层面针对移动运维终端、临时调试设备等非固定接入场景，建立基于设备指纹、数字证书与行为基线等多种因素的可信接入认证机制，对接入设备进行身份验证与安全评估来防止未经授权的设备接入二次设备网络。

结论

本文基于现状分析提出以“一平台、两机制、三层级”为核心的体系架构，明确体系运行以“感知，研判，决策，执行，反馈”闭环逻辑为主线且以风险预警与应急响应为双翼的协同运行机制。在组织管理层面设计矩阵式组织模式与覆盖全生命周期的制度标准体系并建立分层分类的人员能力建设机制，在技术支撑层面构建端边云协同的状态感知体系、数据融合与智能分析框架以及纵深防御与可信接入相结合的网络安全防护策略。

[参考文献]

[1]唐青勇. 基于物联网的电力设备远程监测与维护系统设计[J].电气技术与经济,2026, (5):372-375.

[2]黄巍严. 10kV 电力设备运维检修问题及对策探查[J].中国设备工程,2026, (7):205-207.

[3]刘睿智. 基于人工智能的电力设备缺陷识别与运维技术[J].通讯世界,2026,33 (2):115-117.

[4]李琼琼. 物联网在电力调度二次设备远程运维系统中的应用[J].集成电路应用,2025,42 (11):352-353.

[5]赵克敏. 复杂环境下一次设备和电力线路运维检修的难点与对策[J].光源与照明,2025, (5):116-118.

[6]钱锦,陈元中,徐汉麟,等. 基于持续状态监测的电力系统二次设备安全运维分析[J].电子设计工程,2025,33 (10):31-34+39.

[7]陈坤. 电力继电保护远程运维技术研究与应用[J].电子技术与软件工程,2019, (18):237-238.

[8]董嘉熙,刘盟. 变电运维技术在电力系统中的应用[J].科学技术创新,2019, (9):167-168.