

电力技术发展与电力生产安全探讨

尉亚军

陕西能源电力运营有限公司 陕西 西安 710016

摘要：电力技术发展历经传统、工业化至智能化阶段，安全需求随之演变，从聚焦设备操作到应对系统性风险，再到防范网络、数据等新兴安全挑战。技术进步在提升自动化、强化监测预警以降低事故率的同时，也因技术复杂度攀升增加了管理成本。为此，需构建技术发展与安全保障的协同机制，推动安全标准更新与复合型人才培育，确保电力生产安全适配技术变革。

关键词：电力技术发展；电力生产安全；协同优化路径

引言：电力是现代发展的基石，其技术发展不断重塑着能源格局。从传统火力、水力发电到如今核电、新能源大规模应用，从孤立发电到跨区域互联电网形成，再到智能化电力系统崛起，技术进步极大提升了电力供应能力与质量。但与此同时，电力生产安全也面临新挑战，新技术的引入带来新的风险点。在此背景下，探讨电力技术与电力生产安全关系，具有重要的现实意义。

1 电力技术发展历程与安全需求演变

1.1 传统电力技术阶段

(1) 火力发电以蒸汽机、内燃机为核心动力装置，依赖煤炭等化石燃料燃烧驱动发电，技术原理简单、单机容量小；水力发电依托自然水系落差，通过水车、早期水轮机将水能转化为电能，受地理环境限制明显，发电稳定性较差，两者均以孤立发电模式为主，未形成规模化联网。(2) 早期安全管理重点聚焦设备本身及人工操作：设备故障方面，需防范锅炉爆炸、机械传动部件磨损断裂等风险，定期检查维护发电核心装置；操作规范上，明确人工启停、燃料添加、设备检修的标准化流程，避免因误操作引发安全事故，安全管理以经验型、事后补救为主。

1.2 工业化电力技术阶段

(1) 随着工业化进程加快，电力需求激增推动电网规模化发展，跨区域输电网络逐步形成，实现多电厂联合供电；核电技术兴起并商业化应用，依托核裂变反应产生能量发电，具有高效、低碳的特征，但技术复杂度远超传统发电方式。(2) 安全挑战呈现系统性、专业化特征：系统稳定性方面，电网规模扩大导致节点增多，潮流分布复杂，需防范电网振荡、电压崩溃等系统性故障；核安全监管成为重中之重，建立严格的核反应堆运行监控、放射性物质防护、核废料处理体系，防范核泄漏等重大安全风险，安全管理转向制度型、全过程管控。

1.3 智能化电力技术阶段

(1) 可再生能源（风电、光伏）大规模并网，发电具有间歇性、波动性特征；特高压输电技术突破，实现远距离、大容量电力输送；人工智能、大数据技术深度应用于电网调度、设备运维，推动电力系统向智能化转型。(2) 新兴安全风险日益凸显：网络安全方面，电力系统工控设备、调度系统面临黑客攻击威胁，可能导致电网瘫痪；数据安全聚焦发电、输电、用电全链条数据泄露、篡改风险；设备兼容性问题突出，不同厂商、不同技术标准的智能设备联网运行，易引发系统协同故障，安全管理需兼顾技术防护与制度保障。

2 电力技术发展对生产安全的影响机制

2.1 技术进步带来的安全提升

(1) 自动化控制技术替代人工操作关键环节，大幅减少人为误操作。如火电厂锅炉水位控制、电网调度指令执行等，通过PLC（可编程逻辑控制器）、DCS（集散控制系统）实现自动化运行，避免人工误判参数、误操作设备导致的爆炸、电网波动等事故，某电厂应用后人为操作事故率下降70%。(2) 实时监测与预警系统实现风险早发现，降低事故概率。输电线路搭载红外测温、覆冰监测传感器，变电站部署气体泄漏预警装置，数据实时传输至管控平台，可提前预警设备过热、绝缘损坏等隐患，如某电网应用后线路故障处置时间缩短60%，重大事故发生率降低55%^[1]。

2.2 技术迭代引发的安全新挑战

(1) 新能源接入的波动性冲击电网稳定。风电、光伏受风速、光照影响出力波动大，大规模并网易导致电网频率、电压偏离正常范围，2023年某区域因大风骤降引发风电出力突减，造成局部电网电压异常。(2) 数字化系统面临网络攻击风险。智能电表、调度系统联网后，易遭黑客入侵，2022年某国电网遭ransomware（勒索软

件)攻击,导致部分区域停电。(3)老旧设备与新技术兼容性差。部分电厂仍在使用的传统继电保护装置,与新接入的新能源控制系统通信协议不匹配,易出现数据传输中断,影响安全管控。

2.3 技术-安全协同的辩证关系

(1)正向作用体现为技术升级推动安全标准迭代。特高压输电技术发展后,催生《特高压交流输电线路安全规程》修订,补充绝缘配合、防雷设计新要求;人工智能在运维中应用,推动《电力人工智能安全评估标准》出台,规范算法模型安全验证流程,形成“技术突破-安全需求-标准完善”的良性循环。(2)负向作用表现为技术复杂度增加安全管理成本。数字化系统需配备专业网络安全团队,采购防火墙、入侵检测设备,每年投入的安全防护成本较传统系统增加30%;新能源并网需额外建设储能、调峰设施,且需培训员工掌握新型设备运维技能,进一步推高安全管理的人力、物力成本。

3 电力生产安全管理体系的适应性研究

3.1 传统安全管理体系的局限性

传统安全管理体系以“被动式应对”为核心,多在事故发生后开展调查与整改,缺乏事前预防能力。例如,针对输电线路故障,传统模式依赖人工定期巡检,仅能在故障出现后排查原因,无法提前预判线路覆冰、杆塔倾斜等隐患,导致故障处理滞后。同时,体系对经验依赖性极强,安全决策多依赖老员工的操作经验与历史案例,缺乏科学数据支撑。在新能源接入场景中,传统经验无法适配风电、光伏的出力波动规律,难以制定有效的安全管控策略,当电网运行工况超出经验范畴时,易引发安全风险,无法满足智能化电力系统的动态安全需求。

3.2 智能化安全管理体系构建

(1)基于大数据的风险预测模型成为体系核心。通过整合发电、输电、配电全环节的运行数据(如设备温度、电流电压、环境风速等),运用机器学习算法构建风险预测模型。以火电机组为例,模型可分析历史故障数据与实时运行参数的关联,提前72小时预测锅炉管道泄漏风险,准确率达85%以上;在电网层面,模型能结合新能源出力数据与负荷变化,预判电压波动范围,为调度人员提供提前调整策略,将潜在事故发生率降低60%。(2)区块链技术为安全追溯提供不可篡改保障。将电力设备采购、运维、检修等关键信息上链,形成全生命周期追溯链条。例如,变压器运维过程中,每次巡检数据、维修记录均实时写入区块链,一旦出现故障,可快速追溯设备历史状态,明确责任主体;在电力交易安全领域,区块链能记录交易数据,防范数据篡改导致的交易风险,确保电

力市场安全运行,提升安全管理的透明度与可信度^[2]。

3.3 政策与标准对技术安全的引导作用

(1)国际安全标准持续更新适配技术发展。IEC 62305(雷电防护标准)针对智能电网设备特性,新增对光伏逆变器、风电控制柜的雷电防护要求,明确设备接地电阻、浪涌保护器选型标准,避免雷电灾害对数字化设备的损坏;IEC61850标准则统一了电力系统通信协议,为智能化设备互联互通提供安全规范,减少因协议不兼容引发的系统故障。(2)国内政策聚焦新技术安全管控。《关于促进新时代新能源高质量发展的实施方案》明确要求新能源项目需配套储能设施,平抑出力波动,保障电网安全;《电力行业网络安全管理办法》针对数字化系统,规定电力企业需建立网络安全等级保护制度,定期开展漏洞扫描与渗透测试,防范网络攻击。这些政策与标准为电力技术安全应用划定边界,推动安全管理体系与技术发展同频共振。

4 电力技术与电力生产安全协同的优化路径

4.1 技术创新与安全标准的同步设计

(1)在电力技术研发初始阶段引入“安全前置”理念,打破“先技术、后安全”的传统模式。例如,在新型储能技术研发中,同步开展电池热失控防护、充放电安全控制的标准制定,明确储能系统的防火间距、温度预警阈值等核心指标,避免技术落地后因安全标准缺失引发事故;针对虚拟电厂技术,研发环节需同步构建安全通信协议标准,防范数据传输过程中的篡改风险,确保技术创新与安全标准形成“研发-标准-应用”的闭环,使安全要求贯穿技术全生命周期^[3]。(2)建立技术创新与安全标准的动态联动机制。当特高压输电、柔性直流等新技术实现突破时,组织电力企业、科研机构、标准制定单位开展联合论证,及时更新安全标准内容。如特高压换流阀技术升级后,同步修订《特高压换流站设备安全导则》,补充新型换流阀的绝缘测试方法、故障应急处理流程,确保技术进步与安全标准更新保持同步,避免出现技术超前、标准滞后的安全漏洞。

4.2 复合型人才培养机制

(1)构建“电力技术+安全管理+网络安全”的交叉学科教育体系。在高校电气工程专业中,增设《电力系统网络安全》《智能电网安全管理》等课程,将网络攻击防护、智能设备安全运维等内容融入教学;开展校企合作,组织学生参与电力企业的数字化变电站安全调试、新能源并网风险评估等实践项目,提升学生对多领域知识的综合应用能力,培养既懂电力技术原理,又掌握安全管理方法和网络防护技能的复合型人才。(2)建立针

对在职人员的跨领域培训机制。定期组织电力运维人员参加网络安全攻防演练,模拟黑客对电网调度系统的攻击场景,提升应急处置能力;开展智能化设备安全操作培训,重点讲解老旧设备与智能系统的协同运行要点、数据安全防护措施,帮助工作人员适应技术迭代带来的安全管理需求变化,缓解“技术更新快、人才能力不匹配”的矛盾。

4.3 动态风险评估与弹性电网建设

(1) 依托数字孪生技术构建全生命周期风险管理体系。通过搭建电力系统数字孪生模型,实时映射物理电网的运行状态,模拟新能源出力波动、设备老化、极端天气等不同场景下的风险演化过程。例如,在台风多发地区,利用数字孪生模型预测台风对输电线路的影响,提前评估杆塔倾斜、线路覆冰的风险等级,并制定针对性加固方案;在新能源并网环节,通过模型仿真分析不同装机容量下的电网稳定性,动态调整接入方案,实现风险的事前预判、事中控制、事后追溯^[4]。(2) 加强弹性电网建设以提升风险应对能力。在电网规划中融入弹性设计理念,如在关键节点配置储能装置,应对新能源出力骤降导致的供电缺口;建立分布式电源与主网的协同控制机制,当主网遭遇故障时,分布式电源可快速切换为孤岛运行模式,保障重要负荷供电;定期开展电网弹性测试,模拟极端事故场景下的系统恢复能力,优化应急抢修流程,提升电网在风险冲击下的韧性。

4.4 国际合作与经验共享

(1) 推动跨国电网安全标准互认机制建设。积极参与国际电工委员会(IEC)、国际大电网委员会(CIGRE)等组织的标准制定工作,将我国在特高压输电安全、新能源并网管理等领域的实践经验转化为国际标准;与“一带一路”沿线国家开展电力安全标准对接,推动我国《智能变电站安全技术规范》《电力网络安全等级保护要求》等

标准与相关国家互认,降低跨国电力项目的安全标准差异成本,保障跨境电网互联的安全稳定^[5]。(2) 建立跨国电力安全应急联动与经验共享平台。针对电网cyber-attack(网络攻击)、大范围停电等跨国安全事件,与相关国家签订应急联动协议,明确信息共享、资源调配、联合处置的流程;定期举办国际电力安全论坛,分享各国在应对新能源波动性、数字化系统防护等方面的成功案例,如借鉴欧洲在虚拟电厂安全管控中的经验,优化我国虚拟电厂的风险防控策略,通过国际合作提升全球电力系统的整体安全水平。

结束语

电力技术的持续演进为能源领域注入了强劲动力,推动了电力生产向高效、清洁、智能方向迈进。然而,技术革新带来的安全挑战亦不容忽视,从设备运维到网络安全,从系统稳定性到应急管理,均需构建与新技术适配的安全防护体系。未来,唯有坚持技术创新与安全保障并重,强化标准引领、人才支撑与协同治理,方能在提升电力供应能力的同时,筑牢安全底线,为经济社会高质量发展提供坚实可靠的能源保障。

参考文献

- [1]董良庆.电力技术发展及电力生产的安全探讨[J].中国设备工程,2021,(21):219-221.
- [2]小红侯.电力技术发展中电力生产安全问题的思考[J].水电水利,2020,4(6):54-55.
- [3]常立望.电力技术发展及电力生产的安全探讨[J].电气技术与经济,2023,(8):210-212.
- [4]常立望.电力技术发展及电力生产的安全探讨[J].电气技术与经济,2023,(8):210-212.
- [5]高陈龙,王华晖.电力企业安全生产管理问题及发展路径研究[J].中小企业管理与科技,2023,(24):134-136.