新型电力系统网络安全管理体系建设与优化研究

倪晨讯

（国网江苏省电力有限公司扬中市供电分公司，江苏 镇江 212200）

摘 要 在能源转型不断深入的行业环境下，新型电力系统依靠新能源并网、数字化转型和智能化升级来实现体系的重新构建，网络结构表现出开放化、分布式、泛在化的全新特点，传统的封闭式电力网络安全管理方式已不能满足目前系统运行的要求。电力系统各类终端设备、数据传输链路以及业务平台的网络化联系愈加紧密，安全风险隐患表现出多元化的特征，并越发隐蔽。本文以新型电力系统运行特点和网络安全发展现状为出发点，对目前网络安全管理体系存在的短板和不足进行梳理，建立符合新型电力系统发展的安全管理体系框架，从制度、技术、运维等方面提出体系优化路径，以期为提高电力系统网络安全防护水平提供参考，进而保证电力系统安全稳定可持续运行。

关键词 新型电力系统；网络安全管理体系；网络安全管理制度；网络安全防护技术；网络安全运维管控

中图分类号：TM73；TP309 **文献标志码**：A **DOI**：10.3969/j.issn.2097-3365.2026.30.026

0 引言

随着“双碳”目标的持续推进和电力数字化改革的不断深入，新型电力系统逐渐从传统的以火电为主的运行模式中脱离出来，形成以新能源为主、多能互补、源网荷储协同的新运行模式。数字化、智能化技术广泛应用后，电力生产、传输、调度、用电各环节都被网络化地覆盖，提高了电力系统的运行效率，并打破了传统电力网络的封闭安全边界。目前，电力网络安全管理机制、防护技术和运维模式还存在一些同新型电力系统开放化、分布式运行特点不相适应的问题。因此，开展新型电力系统网络安全管理体系建设与优化研究，能够给电力行业网络安全管控升级提供理论支撑，对防范网络安全风险、保障能源网络安全具有重要意义。

1 新型电力系统网络安全管理体系发展现状

1.1 网络安全管理制度框架初步成型

目前，我国电力行业已建立基本的网络安全管控制度体系，根据电力系统运行特点制定一系列的网络安全管理规范和行业标准，初步形成以电力生产、调度、运维等重要环节为主要内容的安全管理制度体系。各类电力运营主体依照行业通用标准，创建内部网络安全管理机制，明晰各个岗位的安全管理责任，规范网络设备运维、数据存储传输、系统更新迭代等常规工作流程。整体制度体系可以满足传统电力网络的基础安全管控要求，为新型电力系统网络安全管理工作开展提供制度基础，但是不能很好地适应新能源并网、分布式终端接入等新型场景。

1.2 网络安全防护技术持续迭代升级

电力行业数字化转型期间，网络安全防护技术一同推进更新发展，防火墙、入侵检测、数据加密、漏洞扫描等基本防护手段在电力网络系统中得到普遍应用，可以有效地抵挡常规网络攻击以及违规访问行为。新型防护技术也渐渐加入电力安全管控体系中，依靠大数据、人工智能技术对网络风险进行监测、预警、溯源，从而大幅提高电力网络风险的主动防控能力。整体防护技术体系由被动防御转向主动防控，但是对分布式终端、无线传输链路等新的薄弱环节的专项防护技术还存在不足。

1.3 网络安全运维管控模式逐步完善

电力行业已经建立常态化安全运维体系，形成日常巡检、风险排查、漏洞修复、应急处理的闭环运维过程，专业的运维队伍对电力网络系统进行日常的安全控制工作，可以及时处理常规的网络安全隐患。与此同时，行业内也逐渐形成网络安全应急响应体系，就网络攻击、系统瘫痪、数据泄露等突发的安全事件制

作者简介：倪晨讯（1992-），男，本科，工程师，研究方向：电力安全管理。

订处置方案，并且不定期地开展应急演练，以提高突发事件的应对水平。但是，由于电力网络结构不断扩展，大量终端设备接入造成传统的手工运维模式压力越来越大，智能化、精细化的运维管控水平还需要提高。

2 新型电力系统网络安全管理体系存在的核心问题

2.1 安全管理制度适配性存在短板

现有的电力网络安全管理制度大多是以传统的集中式电力网络结构为基础来制定的，制度条款和管控标准更适合于封闭式、固定化的电力运行环境，不能很好地适应新型电力系统分布式并网、多主体参与、跨区域联动的新运行模式。新型电力系统接入主体类型多样，包括各种新能源场站、分布式用电终端、市场化交易平台等，不同的主体网络运行场景和安全需求也大相径庭，但是现有的制度缺少分层分类的精细化管控条款，制度约束和指导作用无法得到充分的发挥，部分新型电力业务场景存在着管理空白。

2.2 安全防护技术体系存在薄弱环节

现有的电力网络安全防护技术大多集中于核心调度系统、主干网络等重要部分，对于海量的分布式终端以及边缘网络的防护技术配置欠缺，总体上存在的防护体系漏洞比较明显。此外，新型分布式终端种类繁多，且其数据传输机制尚未形成统一标准，大多依赖无线公共网络接入，这一现状加剧了安全防护技术标准的缺失问题，使得“带病入网”现象频发。上述因素共同作用，使得电力系统的网络安全风险显著增加，电力系统网络空间边界防护难度进一步增大。同时，各类防护技术之间缺少有效的联动，数据共享和协同防控能力较弱，不能应对复杂的、组合式的新型网络攻击手段。

2.3 安全运维管控体系精细化不足

新型电力系统网络设备数量、终端类型、数据流量呈爆发式增长，网络拓扑结构更加复杂，但是目前电力网络安全运维还存在着粗放式的管理问题，智能化运维工具的应用范围比较小，对于海量终端设备的实时监测和动态管控的能力较差[1]。运维工作大多集中在事后处理上，事前的风险预测、事中的动态控制能力较弱，不能及时发现隐藏的、长久的网络安全风险。另外，运维岗位权责不清，缺少跨部门、跨主体的协同运维机制，风险处置效率低。

3 新型电力系统网络安全管理体系建设优化路径

3.1 优化迭代分层适配的安全管理制度体系

根据新型电力系统开放化、分布式、多元化的特点，以现有的制度框架为基础进行迭代优化，建立分层分类、精准匹配的网络安全管理制度体系，弥补新型业务场景下管理的空白[2]。首先，从行业整体发展的角度出发，细化新型电力系统各类接入主体的安全管理标准，对新能源并网、分布式终端接入、电力市场化交易、源网荷储协同运行等新型场景制定专项安全管理规范，明确各个场景下网络安全管控的要求、操作标准和责任边界，消除制度管控的盲区。其次，完善层级化的管理制度结构，创建起行业统筹、企业执行、岗位细化的三级管理制度体系，依照电力系统数字化运行的特点，更新网络设备管理、数据安全管控、系统权限管控、外包服务管理等配套制度，使管理制度全方位适应新型电力系统运行模式。最后，建立制度动态更新机制，根据网络安全技术更新、网络攻击手段升级、电力业务模式创新等的变化，定期对现有的管理制度进行梳理和修订，保证制度的时效性和适应性，给网络安全管理工作提供全面、精准的制度支持，从制度上规避新型电力系统各种网络安全风险。制度落地实施层面，还要建立制度执行监督和考核约束机制，解决传统电力安全管理重制定、轻落实的问题。新型电力系统参与者众多，各个参与者的安全管理能力、执行标准不同，构建统一的监督考核体系，可对各主体的安全行为加以规范，防止出现制度形同虚设的情况。同时，可以结合电力行业数字化管控的优势建立制度执行动态监督体系，对各环节的制度执行情况实行常态化的督查，对制度执行薄弱环节进行专项整改指导，使安全管理制度由纸面规范变为实际管控能力，不断夯实新型电力系统网络安全管理的制度基础。

3.2 构建全域协同的智能化安全防护技术体系

根据新型电力系统网络安全防护的薄弱之处，依靠数字化、智能化技术革新防护架构，创建覆盖全网、全域、全环节的协同防护技术体系，补齐传统防护体系存在的漏洞和缺陷[3]。一是扩大安全防护的覆盖面，在夯实核心调度网络、主干网络防护的基础上，加大分布式终端、边缘网络、无线传输链路的安全防护力度，统一分布式终端入网安全标准，创建终端入网检测、认证、监测一体化防护体系，从源头上把控终端入网安全隐患，破解终端带病入网的行业难题。二是推进防护技术的智能化升级，融合大数据、人工智能、区块链等前沿科技，创建智能风险监测预警平台，可以对网络流量、设备运行状况、数据传输轨迹展开及时采集并加以智能剖析，从而准确找出异常访问、网络攻击、数据泄露等风险隐患，加强风险的提前预知以及精确应对。三是搭建多技术协同防护架构，将防火墙、

入侵检测、数据加密、智能溯源、漏洞挖掘等各方面的防护技术融合起来，打通技术数据共享通道，使各种防护模块之间可以联动响应、协同防控，打破单一技术防护的局限性，对新型电力系统网络边界和内部链路的新型网络安全威胁进行全方位的防护。为使技术防护体系更具有适应性、稳定性，还需要推进防护技术同电力业务的深度融合，抛弃通用化网络防护技术的套用模式，按照电力调度、新能源发电、电力交易等各业务的运行规律和安全特性制订差异化的技术防护方案。持续推进防护技术迭代适配工作，根据新型网络攻击变异特性以及电力系统新增设备、新增业务安全需求，及时更新防护算法和技术模块，加强边缘节点、分布式场站轻量化防护能力，解决核心防护技术下沉不力、边缘防护薄弱的问题，构建核心强防护、边缘全覆盖、全域可联动的立体化技术防护体系。

3.3 打造精细高效的常态化安全运维管控体系

围绕新型电力系统复杂的网络结构和海量的终端设备，优化运维管控模式，创建精细化、智能化、协同化、常态化的运维管控体系，从而全方位提升网络安全运维管理效能，这也是新型电力系统网络安全管理体系优化的落脚点[4]。推进运维管控精细化升级，细化网络安全运维岗位职责，明确设备巡检、风险排查、漏洞修复、应急处置、数据管控等各个方面的工作标准和考核要求，根据不同的网络设备、终端、业务系统制定不同的运维方案，实行分类管控、精准运维，杜绝粗放式运维造成的风险遗漏问题。推进智能化运维能力提升，用自动化运维工具和智能管控平台取代传统的人工运维方式，对大量的终端设备进行实时监控、自动巡检、自修复漏洞、自动报警风险等，从而提高运维效率、减少人工操作的失误，将运维数据集中到平台上统一管理，给风险判定和改进提供数据支撑。完善协同运维工作机制，创建跨部门、跨主体的运维协同体系，打通电力调度、设备运维、信息技术、安全管理等方面的工作联动通道，形成常态化的沟通对接、风险联合排查、问题协同处置工作机制，解决多头管理、权责不明、处置缓慢等问题[5]。健全应急运维保障体系，根据新型电力系统网络安全风险特点，优化网络安全应急预案，细化不同种类安全事件的处置流程、处置标准和责任分工，定期开展常态化、专业化应急演练，提高运维团队应对突发网络安全事件的处置能力。建立风险复盘机制，对已发生的网络安全隐患和事件进行深入分析，找出问题产生的原因，优化运维管控流程和防护策略，形成风险排查、处置、复盘、优化的闭环运维管理模式，不断夯实新型电力系统网络安全运行基础。除此之外，还要加强运维队伍专业化建设，适应新型运维体系运行需要，根据智能化运维技术、新型防护设备和多元业务场景建立常态化人才培训体系，重点提高运维人员智能平台操作、新型风险识别、突发事件处置等专业能力。创建运维人才的考核和培养机制，培育一支专业的、复合型的运维队伍来弥补传统运维团队智能化、数字化能力欠缺的不足[6]。建立行业运维经验交流平台，汇集各种网络安全运维案例和处理办法，达成行业资源互通、经验共享的目的，不断改善运维管控流程，提高新型电力系统网络安全运维的专业性、精细度、智能化水平。

4 结束语

新型电力系统数字化、智能化、开放化的发展为电力行业高质量转型提供新动力的同时，也给网络安全管理带来了新的挑战与压力，传统网络安全管理体系的弊端愈加明显。本文从新型电力系统网络安全管理现状入手，总结出制度适配性不足、防护技术弱化、运维管理粗放等主要问题，进而提出制度、技术、运维三个层面的体系优化方案，构建符合新型电力系统发展要求的安全管理体系。未来电力行业要不断关注网络安全风险的新特点，持续改进安全管理体系，依靠制度健全、技术更新、运维提效等多方面措施，从各方面加强电力网络安全防线，为新型电力系统安全稳定、高效有序运行提供有力支撑。

参考文献：

[1] 张蓬鹤,宋如楠,李兴文,等.新型电力系统供用电安全技术研究与发展[J].新型电力系统,2025,03(04):384-396.
[2] 邓良辰,王娟,费佳颖,等.数智技术赋能新型电力系统建设[J].宏观经济管理,2025(04):49-58.
[3] 曹伟,吴繁宇,刘媛.面向新型电力系统的网络安全保障体系构建[J].广西电力,2024,47(05):63-68.
[4] 黄梦琦.基于大数据的新型电力系统网络信息安全防护策略研究[J].信息与电脑(理论版),2023,35(01):222-225.
[5] 张蓬鹤,宋如楠,李兴文,等.新型电力系统供用电安全技术研究与发展[J].新型电力系统,2025,03(04):384-396.
[6] 曹伟,吴繁宇,刘媛.面向新型电力系统的网络安全保障体系构建[J].广西电力,2024,47(05):63-68.