

新型电力系统下电力通信网络安全风险防控研究

高晨博 杨明飞 金鑫 方超 葛文洁 陈琳

甘肃同兴智能科技发展有限公司 甘肃 兰州 730050

摘要：新型电力系统改造工作推进后，电力通信网络的开放程度持续提升，网络安全隐患也随之增多，对电网常态化稳定运行造成一定威胁。本文围绕新型电力系统运行场景，系统梳理电力通信网络存在的各类安全风险，总结当前防护体系、管理制度、技术水平和人才团队建设等方面存在的短板，结合行业发展现状制定对应的优化防控措施，以此完善电力通信网络安全防控体系，为电网安全、稳定、长效运行提供理论参考。

关键词：新型电力系统；电力通信网络；安全风险；风险防控

引言：随着新型电力系统建设持续推进，新能源并网体量不断增加，电网通信组网方式和运行架构出现明显调整。原有封闭式电力通信网络的边界逐步开放，整体安全防护环境发生改变，各类安全风险问题开始显现，对电网平稳运行造成潜在威胁。现阶段传统安全防控模式存在一定滞后性，无法适配电力系统转型升级的发展需求。本文结合当前电力通信网络的运行现状，梳理现存安全风险与防控短板，提出对应的优化改进方案，为电力通信安全运维工作提供可行参考。

1 新型电力系统下电力通信网络安全风险类型

1.1 网络架构安全风险

新型电力系统推行源网荷储协同运行的模式，打破了传统电力通信网络封闭独立的运行结构，让通信网络具备更强的开放性与广泛性，也让架构层面的安全风险有所上升。传统电力通信网络拥有清晰的运行边界，系统整体的防护独立性相对较好，可以有效阻挡外部网络的各类入侵行为^[1]。新型电力系统建设过程中，大量分布式设备和市场运营主体持续接入专用通信网络，公私网络之间的数据交互变得更加频繁，网络边界逐渐模糊，外部攻击渗透的途径也随之变多。很多新增通信终端都布置在户外偏远区域，设备运维覆盖不够全面，终端防护配置整体较为简单，存在明显的安全薄弱点。同时传统网络架构的设计标准较为老旧，难以适配新能源大规模并网后的高频数据传输需求，容易出现网络拥堵和链路中断等问题，间接影响电网的稳定运行。

1.2 设备终端安全风险

电力通信网络终端设备整体布设数量较大，设备类型较为繁杂，布设区域相对分散，终端设备也是电力通信安全隐患的主要来源。新型电力系统持续扩容终端设

备的应用规模，设备层面的安全隐患也会随之增加。多数民用级通信终端的生产成本较低，设备出厂阶段并未配置对应的安全防护模块，设备本身存在系统漏洞、权限开放过度等基础问题，运维单位也没有落实常态化的漏洞修复工作，设备安全缺陷会长期存在。电力系统接入的各类新型电力设备标准并不统一，设备通信协议存在差异，设备数据交互过程容易产生安全漏洞。户外终端设备多处于无人值守状态，设备物理防护条件有限，运维人员难以全面排查全部设备隐患，非法接入和设备异常问题无法及时处理，终端整体安全防护水平存在明显不足。

1.3 数据传输安全风险

新型电力系统业务规模不断扩大，系统运行产生的交互数据体量与数据类型都在持续增加，这也让数据传输环节的安全隐患变得更加突出，直接影响电网运行的整体稳定性。电力通信网络日常需要承载电网运行参数、调度指令、用户用电及电力交易等涉密数据的传输工作，部分基层通信线路未落实加密防护措施，数据传输过程中容易出现泄露、监听等安全问题。部分通信终端设备缺少完善的身份验证和数据核对机制，外部人员可以篡改运行数据、伪造调度指令，误导电网调度工作并引发各类运行故障。新能源设备大范围并网后，网络数据传输压力持续上升，部分老旧线路带宽配置不足，容易产生网络拥堵、数据延迟和数据丢失问题，导致传输数据失真、调度指令执行滞后，降低了电力系统运行的安全水平。

1.4 网络攻击安全风险

新型电力系统持续推进网络化改造工作以后，电力通信网络的对外开放范围有所扩大，网络遭受恶意攻击的

整体概率也出现明显提升。电力通信网络在日常运行过程中会遭遇多种类型的网络攻击,不同攻击方式都会对电网通信运行状态产生负面影响。常规网络攻击的发生频次整体偏高,这类攻击能够直接扰乱通信网络的正常工作状态,造成网络局部瘫痪、设备离线、数据传输中断等常见故障^[2]。部分攻击者会对电力核心网络实施长期定向渗透,这类攻击的隐蔽性较强,能够窃取系统内部数据、损毁运行程序,严重时可引发大面积电网运行异常。防护能力较弱的终端设备还会被不法人员集中控制,设备被统一调动后会占用网络带宽资源,干扰全网数据传输秩序,最终影响新型电力系统的整体运行安全。

2 电力通信网络安全风险防控现存问题

2.1 安全防护体系建设不完善

现阶段电力通信网络的安全防护体系大多沿用传统电力系统的搭建框架,这套体系已经难以适配新型电力系统的运行防护要求。行业当前采用的防护模式以被动应对问题为主,并没有建立覆盖全过程的风险管控机制,难以应对持续动态变化的网络安全隐患。防护资源的分配存在不均衡的问题,核心网络区域的防护工作相对完备,边缘节点与终端接入区域的防护工作存在明显薄弱环节。防护技术的更新迭代速度相对缓慢,传统防护方式的适配性在持续降低,这就让整体安全防护工作的实际成效受到限制,无法全方位保障电力通信网络的运行安全。

2.2 安全管理制度执行不严格

电力通信行业已经搭建起对应的安全管理规章制度体系,但制度在实际落地过程中存在执行不到位的问题,无法适配当下新型电力通信的管理工作要求。现行制度内容大多针对传统电力通信业务制定,并未结合新型电力业务更新内容,新兴业务的安全管理工作缺少对应的制度依据。基层运维岗位普遍存在重视业务推进、忽视安全管控的工作问题,常规安全管理工作难以有效落地。岗位安全权责的划分不够明确,日常监督管控力度较为薄弱,行业缺少完善的问责机制,安全问题发生以后,相关责任追究工作难以正常开展,整体管理约束效力存在明显不足。

2.3 技术防控能力存在短板

目前国内电力通信安全防控技术的发展速度较为滞后,相关技术体系难以适配新型电力系统的常态化安全防护标准。现阶段行业采用的风险监测手段相对单一,工作人员仅可以排查表面的网络故障和常见攻击问题,难以识别隐藏的系统漏洞和潜在风险,全网实时风险管

控能力存在明显不足^[3]。智能防控设备在行业内的普及程度不高,大部分安全突发问题依旧依靠人工方式处理,整体处置效率偏低,也会提升风险扩散的可能性。各类新型安全防护技术没有得到全面落地运用,电力通信系统的智能分析、风险判断以及主动防御能力,都还有一定的提升空间。

2.4 人才队伍建设相对滞后

电力通信安全防控属于交叉性工作,这项工作对从业人员的综合专业能力有着较高要求,当下行业人才队伍建设工作仍旧存在不少问题。在岗人员的专业知识体系普遍比较单一,大多只能完成基础的通信运维工作,对于网络安全防护、风险识别研判等相关工作并不具备对应能力。行业内部的培训体系更新速度偏慢,培训内容难以贴合新型电力系统的发展变化,从业人员的专业能力无法得到有效提升。行业人才激励体系尚且不够完善,高端复合型人才引进和留存存在难度,人才队伍稳定性不足,会在一定程度上制约电力通信安全防控工作的整体开展成效。

3 新型电力系统下电力通信网络安全风险防控策略

3.1 完善全域安全防护体系

电力通信网络需要搭建全覆盖的安全防护体系,工作人员可以结合网络自身的三层结构,落实分层分级的整体防护思路。相关防护工作可以划分三个层级开展,工作人员需要对核心传输网络做好安全加固工作,通过布设各类防护设备抵御网络渗透行为,保障电网调度与生产业务稳定运行^[4]。接入网需要做好设备接入审核与权限管控工作,工作人员要对所有接入设备和通信链路开展合规检测,从边界位置阻断非法接入行为。行业需要统一各类终端设备的安全防护标准,补齐基层终端的防护缺陷,消除全网防护盲区。除此之外,防护体系需要搭配动态更新机制,工作人员可以结合电力业务和网络攻击方式的变化,定期调整防护策略、更新设备配置。行业也需要建立常态化评估模式,及时排查防护体系存在的薄弱问题并完成整改,让被动防护模式逐步转变为主动动态防护,适配新型电力系统的长期运行需求。

3.2 健全常态化安全管理制度

新型电力系统的业务模式处于持续更新的状态,电力通信安全管理制度也需要随之做出对应调整,这样才能够适配现阶段电网运行的管理要求。原有管理制度大多是依据传统电力业务制定而成,对于各类新兴通信业务的约束力度存在不足,制度体系本身存在一定空缺。行业需要结合新型电力业务的运行特点,补充对应的安全管理规范,

明确设备接入、通信操作、数据管控等基础工作的统一标准。运维单位需要细化各岗位的工作细则,搭建动态的制度更新机制,让制度内容可以贴合技术迭代与业务拓展的整体进度。相关企业需要明确工作人员的岗位安全职责,将管理责任落实到具体人员,构建层级清晰的责任管理体系。同时企业需要建立常态化监督检查机制,持续监督各项制度的落地执行情况,及时整改运维工作中的不规范操作,持续夯实电力通信网络的安全管理基础,保障电网通信系统可以长期稳定运行。

3.3 升级智能化安防技术

智能化技术的迭代升级,是提升电力通信网络安全防控能力、适配新型电力系统运行需求的关键举措。电力行业需要搭建全域覆盖的智能风险监测平台,整合电网运行数据与各类设备接入信息,依托基础算法完成网络风险的识别、研判与提前预警,能够有效弥补传统人工监测模式精度不足、存在监测盲区的问题^[5]。相关运维单位需要同步搭建配套的智能应急处置体系,针对各类网络安全隐患制定标准化处置流程,依靠系统功能实现风险自动拦截与漏洞自主修复。企业还要定期组织应急演练,提升工作人员的突发问题处置能力。在此基础上,工作人员需要落实数据全流程安全管控工作,针对数据传输、存储、应用等各个环节落实防护措施,通过权限分级、数据加密、操作溯源等基础手段规范数据管理工作,规避数据泄露、篡改等安全问题,全方位强化电力通信网络的整体安全防护水平。

3.4 打造专业化人才队伍

电力通信网络安全防控工作的落地落实,需要依托完善的人才建设体系作为支撑,行业可以从人才引进、人才培养、考核激励三个方面完善人才队伍建设工作。行业需要结合电力通信安全的岗位需求,引进掌握电力运行、网络通信、安全防护及数据管理能力的复合型人才,同时优化人才引进相关政策,完善对应的福利与晋升机制,吸纳基层实操人才,优化整体人才结构。相关

单位需要搭建常态化的人才培育模式,及时更新培训知识内容,围绕新型电力系统相关技术、安全风险和防控规范开展培训工作,结合多元学习方式提升人员实操能力,让员工专业水平可以跟随行业发展持续提升。企业还要建立配套的考核激励制度,将安全工作成效、技术能力与创新成果纳入考核范围,依托奖惩结合的管理模式约束员工工作行为,调动从业人员的工作积极性,进一步稳固人才队伍整体建设质量,为电力通信安全防控工作提供持续的人力保障。

结束语

新型电力系统的建设发展让电力通信网络运行环境发生明显变化,各类新型安全风险逐步凸显,现存防控工作短板也不断暴露。通信网络安全稳定是电网整体安全运行的基础保障,做好风险防控工作对电力系统长效发展有着重要作用。通过完善防护体系、健全管理制度、升级防控技术、优化人才队伍等措施,能够有效化解各类通信网络安全隐患,补齐防控工作短板,助力新型电力系统实现安全、稳定、高效的常态化运行。

参考文献

- [1] 黎国斌,肖祥军.基于5G-A的新型电力系统内生安全通信架构[J].通信技术,2026,59(4):431-437.
- [2] 汪曦,吴锋,管笠,邵焯楠,徐洋.新型电力系统安全面临的挑战及应对建议[J].中国设备工程,2026(2):234-236.
- [3] 普布索朗,巴旦次仁.大数据下电力系统监控信息网络安全探究[J].中国科技论文在线精品论文,2025,18(4):45-47.
- [4] 万健.基于模糊滤波的电力通信网络安全风险评估[J].通信电源技术,2025,42(19):89-91+143.
- [5] 郭彦希,唐习悦,胡议文,薛若涵.电力通信融合系统的安全防护机制研究与实现[J].中国信息界,2025(8):176-178.