新能源电力信息网络安全防护体系建设分析

刘　宇
内蒙古送变电有限责任公司　内蒙古　呼和浩特　010020

摘　要：随着新能源电力系统规模化发展，其信息网络架构呈现分布式、多节点、强联动特征，同时面临外部攻击、内部隐患、设备漏洞等多重安全风险，现有防护体系存在安全意识薄弱、防护技术滞后、行业标准不统一等突出问题。本文结合相关政策法规与行业实践，从技术、管理、应急运维三个核心维度，系统阐述防护体系构建路径，提出针对性实施保障与优化建议，为提升新能源电力信息网络安全防护能力、保障新型电力系统稳定运行提供坚实的理论与实践参考。

关键词：新能源电力；信息网络安全；防护体系建设

引言：在“双碳”目标引领下，风电、光伏等新能源大规模并网运行，新能源电力信息网络已成为新型电力系统稳定运转的核心支撑载体。但其拓扑结构复杂、接入节点分散、业务联动紧密，加之网络攻击手段迭代升级、隐蔽性增强，安全风险持续凸显，严重威胁电力系统安全稳定运行与能源供应安全。基于此，本文立足新能源电力信息网络安全现状，深入分析现存风险与突出问题，探索科学完善的防护体系建设方案，助力破解安全防护难题，推动新能源电力行业高质量发展。

1 新能源电力信息网络安全现状与风险分析

1.1 新能源电力信息网络架构特点

（1）新能源电力系统网络组成与拓扑结构。系统以风电、光伏等场站为核心，搭配集控中心、调度平台、远程终端等设备，形成分布式与集中式结合的拓扑架构。设备点位分散、接入节点繁多，覆盖场站侧、电网侧、用户侧，网络层级复杂，数据传输链路长。（2）生产控制区与管理信息区边界划分。两大区域实行分区防护、逻辑隔离，生产控制区负责发电运行、调度操控等核心业务，对实时性要求极高；管理信息区负责运营管理、数据统计等工作。部分场站边界防护不够严密，存在数据跨界传输、权限交叉问题。（3）新能源电站、电网调度、远程监控的网络联动特性。三方通过专用通信网络实现数据互通、远程操控，电站运行数据实时上传调度中心，调度指令远程下达执行。联动性强虽提升运维效率，但也扩大了风险传导范围，一处失守易波及全域[1]。

1.2 新能源电力信息网络面临的安全威胁

（1）外部网络攻击。病毒、木马入侵会破坏系统程序，勒索软件会加密核心数据索要赎金，黑客通过漏洞入侵、APT攻击等手段，可篡改运行数据、操控设备，严重威胁电网稳定运行。（2）内部安全隐患。员工违规操作、误改参数会引发运行故障，内部人员泄密、权限滥用会导致核心运行数据、用户信息流失，内部风险隐蔽性强，排查难度大。（3）设备与通信安全风险。场站终端、智能设备存在系统漏洞，易被非法入侵；无线传输、公用链路加密不足，易出现数据窃听、链路泄密，信号干扰也会影响传输稳定性。

1.3 安全防护现存问题

（1）安全防护意识薄弱，管理制度不完善。部分企业重生产、轻安全，防护责任落实不到位，缺少全流程安全管理制度，应急处置预案流于形式。（2）防护技术滞后，缺乏主动防御能力。多采用传统防火墙、杀毒软件，难以应对新型攻击，缺少态势感知、入侵预警等主动防御手段，事后补救居多。（3）安全标准不统一，跨区域协同防护不足。各地场站、电网企业防护标准有差异，数据互通、应急联动机制不健全，跨区域协同防御能力薄弱。

1.4 相关政策法规与标准要求

（1）国家电力行业网络安全法律法规。遵循《网络安全法》《数据安全法》等国家法规，严守电力行业安全底线，压实企业安全主体责任。（2）等级保护2.0与电力监控系统安全防护规定。严格落实网络安全等级保护要求，执行电力监控系统安全防护规范，筑牢分区隔离、权限管控防线。（3）新能源电力行业专项安全规范。贴合风电、光伏等新能源业态，执行专项安全标准，规范设备接入、数据传输、运维管控全流程安全操作。

2 新能源电力信息网络安全防护体系构建

2.1 防护体系构建原则与目标

（1）构建基本原则。体系搭建严守四大核心准则，纵深防御指搭建多层级防护屏障，打破单一防护短板，层层抵御安全风险；分区分域遵循电力系统安全规范，

严格划分生产控制区与管理信息区，实现区域隔离、权限分立；最小权限秉持按需授权准则，严控各类账号、设备的操作权限，杜绝越权操作、权限滥用；动态防护打破静态防护局限，紧跟新型网络威胁，实时调整防护策略，实现灵活适配。（2）整体防护目标。核心是保障新能源电力系统软硬件稳定运行，杜绝因网络攻击、设备漏洞引发的停运故障；严守数据安全底线，防止运行数据、调度信息、用户资料泄露、篡改与丢失；保障发电、调度、监控等核心业务不间断运转，守住电网安全稳定运行的生命线，兼顾安全防护与业务效率的平衡。（3）体系设计思路。采用全方位覆盖模式，兼顾物理、网络、终端、数据、管理全环节，不留防护死角；搭建多层次防护架构，从边界阻隔、终端管控到后台运维，形成立体防线；推行闭环管控模式，实现风险监测、预警处置、复盘优化的全流程闭环，让防护工作有始有终、持续升级。

2.2 技术防护体系建设

（1）物理环境安全防护。严控机房出入管理，实行专人值守、刷卡准入、身份核验制度，严禁无关人员进入核心机房区域；配齐备用电源、冗余设备，搭建双回路供电体系，防止断电、设备故障导致系统停运；加装温湿度监控、火情报警、防盗监测装置，实时把控机房环境状态，及时排查物理安全隐患。（2）网络边界安全防护。部署防火墙、安全网闸等设备，严格阻断非法网络访问，规范跨区数据传输流程；搭建入侵检测、入侵防御系统，实时监控网络流量，精准捕捉恶意攻击、非法入侵行为，做到即时拦截、快速处置；细化访问控制策略，启用白名单机制，仅允许合法设备接入，过滤异常访问请求，筑牢网络边界防线。（3）终端与主机安全防护。推行应用白名单管控制度，禁止非法软件、不明程序安装运行，严控终端操作权限；定期开展全面漏洞扫描，及时修复系统漏洞、更新软件补丁，封堵攻击入口；常态化开展病毒查杀、木马清理工作，升级杀毒软件库，严防恶意程序入侵破坏[2]。（4）数据安全防护。对核心运行数据、敏感信息采用加密技术存储和传输，防范数据窃听、泄密风险；对数据分级分类管理，按岗位职级分配访问权限，杜绝越权查看、拷贝数据；建立定时备份、异地备份双重机制，配备专用数据恢复工具，遭遇数据损坏、丢失时能快速复原，保障数据可溯、可恢复。

2.3 管理防护体系建设

（1）安全管理制度体系建立。完善日常运维管理制度，细化设备巡检、系统操作、运维流程，规范日常作业行为；制定专项应急管理制度，明确各类网络安全事件处置流程、责任分工；健全人员管理规范，约束内部员工操作行为，形成全流程、标准化的制度体系，让安全工作有章可循。（2）安全责任落实与权限管控机制。层层压实安全主体责任，明确企业负责人、运维人员、基层员工的安全职责，将责任细化到人、落实到岗；精细化管控操作权限，定期排查账号使用情况，及时注销闲置、违规、过期账号，清理过剩权限，全程留存操作日志，便于追责溯源。（3）人员安全培训与考核体系。定期开展网络安全专项培训，讲解行业规范、防护技能、应急处置方法，剖析典型安全案例，提升全员安全防护意识和实操能力；建立配套考核机制，将安全知识掌握度、规范操作执行力纳入绩效考核，实行奖惩结合，倒逼员工严守安全规范。

2.4 应急与运维体系建设

（1）安全风险监测与预警机制。搭建全天候、全覆盖的安全监测平台，实时监控网络流量、设备运行、系统操作状态，精准识别异常行为和风险隐患；设定科学预警阈值，出现网络攻击、数据泄露、设备故障等苗头性问题时，立即发出声光、短信预警，实现风险早发现、早预警、早处置。（2）应急响应预案与演练流程。针对黑客攻击、勒索病毒、数据泄露、设备瘫痪等突发安全事件，制定细化、可落地的应急处置预案，明确处置步骤、责任分工、抢修流程；定期开展实战化应急演练，模拟各类安全事故场景，检验预案可行性，优化处置流程，提升应急团队快速响应和实战处置能力[3]。（3）常态化运维与安全评估机制。实行日常巡检、定期维护相结合的运维模式，及时保养设备、优化系统、排查隐患，防范设备老化、系统故障引发安全问题；定期开展全方位安全评估，查漏补缺，针对薄弱环节升级防护措施，持续优化防护体系，实现安全防护长效稳固。

3 新能源电力信息网络安全防护体系实施保障与优化建议

3.1 体系实施保障措施

（1）组织保障。成立专项安全管理小组，由企业负责人牵头，统筹运维、技术、管理等多部门人员，明确岗位职责与分工，打破部门壁垒，形成统一指挥、协同配合的工作格局。专职负责防护体系搭建、落地推进、日常管控等工作，解决实施过程中的各类难题，保障各项防护工作有序开展。（2）资金与技术保障。加大网络安全专项投入，划拨专用资金，用于设备升级、技术引进、人员培训、应急演练等工作，补齐防护短板。积极引进人工智能、大数据、态势感知等先进防护技术，淘

汰老旧落后的防护设备，贴合新能源电力网络特性，适配复杂多变的网络安全环境，提升防护硬实力。（3）监督考核保障。建立常态化督查机制，定期对防护体系落地情况、设备运行状态、制度执行力度开展专项检查，及时排查整改疏漏问题。完善绩效评估体系，将安全工作落实成效、防护任务完成质量纳入部门与个人考核，实行奖惩挂钩，倒逼各项防护措施落地见效，杜绝形式主义。

3.2 体系落地实施难点与对策

（1）新旧系统兼容问题与改造方案。部分新能源电站存在老旧设备、遗留系统，与新型防护技术兼容性差，易出现运行卡顿、数据不通等问题。针对这一难题，采取分步改造策略，优先对核心控制区设备升级换代，加装适配接口与转换模块，实现新旧系统平滑衔接；保留原有稳定功能，逐步替换落后设备，降低改造对业务运行的影响。（2）跨部门协同不畅与联动机制优化。安全防护涉及运维、调度、管理等多个部门，易出现职责不清、配合脱节问题。优化跨部门联动机制，建立定期会商、信息互通制度，明确各环节责任边界，打通数据共享通道。设立专项联络专员，统筹协调各项工作，形成上下联动、左右协同的工作合力，提升体系运转效率[4]。（3）技术落地成本控制与效益提升。先进防护技术采购、运维成本较高，加重企业资金压力。推行按需投入、分批建设模式，优先部署刚需防护设备，聚焦核心风险点补齐短板。整合现有资源，提升设备利用率，同时加强技术运维培训，减少后期故障维修成本，兼顾防护效果与经济效益，实现低成本、高效率防护。

3.3 防护体系优化升级路径

（1）引入智能化防护技术。摒弃传统被动防护模式，融入AI威胁识别、大数据安全分析技术，实时监测网络流量，精准识别新型攻击、隐蔽漏洞，实现风险自动预警、快速处置。搭建智能防护平台，提升威胁研判、防御响应效率，适配复杂网络威胁环境。（2）建立全生命周期安全管控模式。覆盖设备采购、接入运行、维护升级、报废淘汰全流程，落实全环节安全管控。从源头把控设备质量，严控接入安全，常态化开展运维检测，及时淘汰老旧隐患设备，实现安全防护全程可控、全程可溯，消除全周期安全隐患[5]。（3）推进行业协同防护与信息共享。打破企业、区域防护壁垒，建立行业安全信息共享机制，及时通报典型网络攻击案例、新型安全漏洞。搭建跨区域协同防御平台，统一行业安全标准，开展联合应急演练，形成行业联防联控格局，提升整体抗风险能力。

结束语

新能源电力信息网络安全防护体系建设是一项系统性、长期性工程，直接关乎新型电力系统安全稳定运行与国家能源战略落地实施。本文构建的“技术+管理+应急”三位一体防护体系，结合配套实施保障措施与动态优化路径，可有效破解当前行业面临的安全防护痛点难点。未来需紧跟信息技术发展趋势，持续推进防护体系智能化升级与行业协同联动，不断完善全生命周期安全管控机制，筑牢新能源电力信息网络安全防线，为新能源电力行业安全、健康、可持续发展保驾护航。

参考文献

[1]陈晓芳,刘紫熠,李祯祥,等.智能电网中的物联网技术应用与发展[J].长江信息通信,2022,35(10):104-106.

[2]徐登科.基于大数据技术应用的智能电网监控系统研究[J].电气时代,2022,8(10):28-30.

[3]李伯恺.电力企业网络安全综合防护体系构建探析[J].长江信息通信,2021,34(12):182-184.

[4]李曦,易荣.电力企业网络安全主动防御技术探究[J].网络安全技术与应用,2021,25(12):112-113.

[5]廖仲钦,刘东华.电力企业信息网络安全防范措施探讨[J].网络安全技术与应用,2021,22(12):113-114.