变电站网络安全重大隐患排查治理工作的标准化流程设计与应用

陈文涛
国网新疆电力有限公司哈密供电公司，新疆 哈密 839000

[摘要]新型电力系统建设下变电站智能化改造提速，调度、集控、五防、在线监测、无人机巡检多业务互联互通，网络安全隐患隐蔽多变。哈密是千万千瓦级沙戈荒能源基地与疆电外送桥头堡，风光场站大规模汇集，“两直两交”特高压通道跨区输电，工控、新能源调控、特高压协同业务深度交织，网络风险可跨省传导，直接危及全国电力保供与国家能源安全。当前变电站网络隐患治理缺少统一标准，智能业务管控细则缺失、分级管控精度不足。本文结合电力安全规范与哈密送端电网运维痛点，梳理治理短板，构建隐患识别、定级、上报、整改、验收、复盘全生命周期标准化流程，配套支撑体系与差异化落地策略。

[关键词]变电站；网络安全；重大隐患；排查治理
DOI：10.64635/ja.2026.1387 中图分类号：TM63 文献标识码：A

Design and Application of a Standardized Process for the Investigation and Remediation of Major Cybersecurity Hazards in Substations

Chen Wentao
Hami Power Supply Company, State Grid Xinjiang Electric Power Co., Ltd., Hami, Xinjiang 839000, China

Abstract: With the construction of new power systems, the intelligent transformation of substations has accelerated. Multiple services, including dispatching, centralized control, five-prevention systems, online monitoring, and UAV inspection, are becoming increasingly interconnected, while cybersecurity hazards are becoming more hidden and variable. Hami is a ten-million-kilowatt-scale desert, Gobi, and barren-land energy base as well as a bridgehead for Xinjiang power transmission. Large-scale wind and photovoltaic power stations are concentrated in this region, and “two DC and two AC” ultra-high-voltage transmission channels support cross-regional power delivery. Industrial control, new-energy regulation, and ultra-high-voltage coordination services are deeply intertwined, making network risks capable of cross-provincial transmission and directly threatening national power supply security and energy security. At present, substation cybersecurity hazard management lacks unified standards, detailed control rules for intelligent services are insufficient, and the precision of hierarchical control remains inadequate. Based on power safety standards and the operation and maintenance difficulties of Hami’s sending-end power grid, this paper reviews the shortcomings in current governance practices and constructs a standardized whole-life-cycle process covering hazard identification, grading, reporting, rectification, acceptance, and review, supported by corresponding guarantee systems and differentiated implementation strategies.

Keywords: substation; cybersecurity; major hazard; investigation and remediation

引言

变电站是电网输配电核心枢纽，其网络安全稳定运行是新型电力系统可靠供电的根基。电力工控系统属于国家关键信息基础设施，网络安全工作直接关乎总体国家安全观落地与国家能源自主可控。当前国际网络空间对抗加剧，能源行业已成定向攻击、工控勒索的重点目标，叠加全国沙戈荒风光大基地集中投产、电网数字化转型提速，站内调度、集控、五防、无人机巡检、新能源远程调控多业务互联互通，传统物理隔离防护体系失效，隐患隐蔽迭代、风险跨域传导特征凸显，常规单点防护模式已难以适配新形势。

西北新能源送端电网具备特殊风险传导属性，局部网络异常可沿跨区通道扩散，直接影响中东部负荷中心供电稳定。哈密作为千万千瓦级沙戈荒能源基地、疆电外送桥

头堡，依托“两直两交”特高压与 750kV 骨干网架，跨区绿电外送规模超 1700 万 kW，海量风光场站集中并网，形成高新能源渗透率、交直流混联、全域远程调控的电网格局。新能源功率调节、特高压协同控制、无人机无线图传等业务深度交织，大量远程链路与无线终端拓宽攻击路径，单点网络漏洞极易引发新能源大规模脱网、跨区输电中断，直接冲击全国电力保供大局，标准化闭环隐患治理工作迫在眉睫。

现有研究多聚焦单一设备防护，缺少覆盖多智能业务、适配特高压送端场景的成套管控标准，基层运维判定尺度不统一、隐患治理流程碎片化。据此，本文结合哈密送端电网运维痛点，构建全生命周期标准化隐患治理体系与差异化落地策略，为基层运维提供实操支撑，筑牢疆电外送网络安全防线。

1 变电站网络安全隐患排查治理现状与问题分析

1.1 现有排查治理主流工作模式

当前各电力运维单位已构建变电站网络安全常态化管控体系，隐患排查治理主要包含定期专项排查、日常运维抽查、事后应急排查三类实施模式，三类模式相互配合，完整覆盖变电站全部运维作业场景。

定期专项排查由单位安全管理部门统一组织，按照季度、年度周期开展全站全覆盖安全检查，能够系统性排查站内硬件设备、软件配置、管理制度存在的各类缺陷，适合开展全站整体性安全校核工作。该模式现有核查条目仅围绕通用服务器、交换机等基础网络设备设计，未结合哈密本地调度数据网、海量新能源汇集站远程调控、集控站、五防系统、在线监测、无人机巡检业务特性设置专项检查内容，适配疆电外送送端电网的专项核查条款缺失。

日常运维抽查将网络安全检查嵌入设备常规巡视、系统定期维护流程，以实时排查账号权限分配、设备运行状态、网络连通性等基础问题为核心，是日常风险管控的主要途径。现有巡检要求未将哈密区域大规模无人机无线传输链路、新能源汇集站远程调控数据库备份、集控远程访问日志等特色检查点位纳入常态化核查范围[1]。

事后应急排查为故障驱动型处置模式，仅在站内出现网络中断、设备高危告警、系统运行异常等突发问题后启动定向溯源工作，重点处置已暴露的显性故障。当出现调度路由篡改、五防越权操作、无人机图传泄密、新能源场站远程调控系统入侵等业务类故障时，现场缺少成套标准化溯源操作流程，故障处置效率受限，一旦处置延误将直接威胁跨区特高压输电通道稳定。

1.2 当前排查治理工作突出痛点

传统隐患治理模式标准化程度、闭环管控能力存在明显短板，难以适配智能变电站精细化防控要求，在哈密疆电外送枢纽、高比例新能源汇集场景下，短板带来的安全放大效应更为突出。行业通用隐患判定标准内容宽泛，未针对调度、集控、五防、在线监测、无人机、新能源场站远程调控等不同业务制定落地细则，基层运维人员判定尺度难以统一，纵向加密缺失、五防主机弱口令、无人机明文传输、新能源汇集站远程端口无防护等高风险隐患长期留存，误判、漏判问题多发。

治理各环节存在割裂问题，行业普遍重排查、轻整改、缺乏复盘，调度、自动化、辅控、新能源运维、无人机运维跨专业隐患缺少联合复核机制，整改工作易流于表面，难以实现隐患全生命周期闭环管控。运维、调度、无人机运维、新能源场站管控班组权责边界模糊，各类智能业务隐患无专属责任岗位，治理措施落地力度不足。同时单位缺少分业务资料归档与长效复盘机制，路由漏洞、新能源场站物联网非法接入、巡检数据外泄等同类隐患处置经验无法沉淀复用，难以应对持续迭代的网络攻击，制约哈密疆电外送送端变电站网络安全治理水平长效提升。

2 变电站网络安全重大隐患排查治理标准化流程设计

2.1 流程设计总体原则与整体架构

为解决传统隐患治理模式随意化、碎片化、形式化的缺陷，本文结合国家网络安全法规、电力监控系统防护标准、新型电力系统安全顶层要求与哈密送端电网一线运维痛点，确立合规性、闭环性、实用性、分级管控四项核心设计原则。合规性层面，紧扣关键信息基础设施安全保护、“沙戈荒”新能源基地网络安全管控相关要求，立足哈密疆电外送战略定位，兼顾通用设备与调度、集控、五防、在线监测、无人机、新能源汇集站远程调控各类智能业务管控需求[2]；闭环性打通隐患识别至复盘全流程，消除流程断层，覆盖站内全部业务风险管控工作；实用性精简冗余操作步骤，适配新旧设备混装、多套智能系统并行、海量新能源场站接入的哈密变电站场景，操作难度贴合基层运维人员能力；分级管控按照隐患危害划分处置优先级，调度无防护跨区互联、五防缺少访问隔离、无人机无线数据泄密、新能源汇集站远程调控系统无加密通道均划为一级特别重大隐患，出现后优先停机隔离处置，阻断风险向特高压外送通道传导，提升高比例新能源送端电网风险管控精准度。

基于四项原则构建一体化架构，整体由全链条作业流程和多维度配套支撑体系组成。核心流程分为隐患识别排查、分级定级判定、上报建档备案、专项整改实施、验收闭环销号、复盘迭代优化六大递进环节。配套支撑体系涵盖标准化排查清单、规范化文档模板、清晰岗位责任、自动化技术工具四大模块，从制度、人员、工具多个维度补齐哈密新能源送端多业务管控短板，保障标准化流程在各类变电站现场稳定落地，守住疆电外送网络安全第一道关口。

2.2 全链条标准化核心流程设计

本节构建全覆盖、可闭环、可溯源的标准化作业链路，统一变电站网络安全各环节作业规范，新增新能源与各类智能业务专属核查内容，实现通用设备与特色业务一体化管控。隐患排查采用人工核查与自动化检测协同模式，依托标准化清单覆盖网络架构、工控设备、数据安全等六大通用领域，并针对五类核心业务定制专项核查规则，适配哈密新能源送端电网场景。其中，重点核验调度数据网跨特高压通道路由与纵向加密配置，排查集控站新能源远程调控链路与账号权限，校验五防系统口令安全与远程认证机制，依托辅控监测系统管控新能源物联网终端边界接入，核查无人机图传加密与飞控权限配置。隐患定级实行多专业联合研判机制，结合风险影响范围、危害程度及跨通道扩散风险，划分为两级隐患，明确区域专属高危隐患清单，弱化人工判定主观性。严格落实 24 小时逐级上报制度，推行“一隐患一档案”，按七类业务建立专项台账，留存完整核查资料，满足跨区域安全督查溯源需求。整改实行“一患一策、分业处置”，一级重大隐患必须停机隔离外送通道并专人旁站督办，暂不具备整改条件的落实物理隔离等临时防控措施。整改后通过资料审核、现场核查、工具复测三重验收，达标方可销号，同时开展专项复盘，迭代优化排查标准，形成闭环优化机制[3]。

2.3 流程落地配套标准化支撑体系

为保障标准化流程在哈密新能源汇集、疆电外送复杂场景长效落地，本文搭建全方位配套支撑保障体系。体系优化完善分层分类标准化排查清单，补充多业务专项核查条目，统一送端电网隐患判定标准，解决基层运维核查尺度不一的问题。同时规范全流程文档模板，细化各环节台账与记录填报标准，适配国家级安全督查与专项审计资料要求。明晰调度、自动化、新能源、无人机等各班组岗位职责，压实岗位责任，将疆电外送通道隐患治理成效纳入绩效考核，杜绝责任推诿、作业松懈等问题。同时配齐专业化技术检测工具，针对性配备路由审计、漏洞扫描、无线检测、物联网边界监测等设备，以自动化技术补齐人工排查短板，有效提升高比例新能源接入场景下隐患排查的精准度与效率，为标准化治理流程落地见效提供坚实制度与技术双重支撑。

3 变电站网络安全隐患治理落地实施策略优化

3.1 落地策略的整体设计与优化逻辑

前期已完成变电站网络安全标准化作业流程与支撑框架搭建，但原有方案缺乏调度、五防、无人机、新能源等智能业务的差异化落地细则，在哈密区域变电站落地过程中，存在执行力度不足、疆电外送场景适配性薄弱等问题。针对上述短板，本文从场景差异化适配、全流程闭环管控、动态风险长效迭代三个维度优化落地策略，形成适配哈密老旧常规站、改造型新能源汇集站、新建智能枢纽站的精细化治理体系，全面覆盖新能源与智能业务安全管控需求，切实筑牢疆电外送送端网络安全防线，保障跨区能源通道风险防控落地见效[4]。

3.2 基于变电站类型的场景适配治理

结合哈密各变电站设备工况、智能化改造进度与新能源业务部署差异，实行分类差异化治理，破解统一方案落地失效问题。老旧常规站硬件基础薄弱，以人工排查为主、自动化扫描为辅，重点整治五防主机弱口令、交换机闲置端口、动环备份缺失、远程端口防护不足等隐患，无固定无人机业务站点仅完善外来设备管控流程，不改动原有工控硬件。改造型新能源汇集站新旧设备混杂、新能源接入体量较大，采用分区逐台核验模式，重点核查加密装置、新能源访问权限、五防数据库及物联网终端接入合规性，新增无人机点位独立划段，实现与生产、特高压调度区域物理隔离。新建 750kV 智能站与换流站全面搭载安全检测工具，聚焦调度加密通道、特高压远程遥控、无人机图传、新能源集群调控等高风险点位，从源头阻断跨通道风险传播。

3.3 隐患治理全流程闭环管控手段

针对现场流程松散、验收宽松、跨专业复核缺位等问题，构建适配疆电外送场景的全流程闭环管控机制。排查定级实行双人核查+多专业联合会商模式，各专业分工核查特高压调度、五防集控、新能源接入、动环设备、无人机终端等隐患，规避漏查、误判问题。隐患坚持当日录入归档，分类留存核查资料，一级外送通道隐患同步上报专项专班。整改实行分级管控，一级重大隐患立即停机隔离、专人旁站督办，短期无法整改的落实物理隔离与 24 小时

值守，防范风险外溢。整改后通过资料核验、现场复查、工具复测三重校验，达标方可销号，压实全流程管控责任。

3.4 面向动态风险的长效防控机制

适配网络攻击迭代、新能源装机扩容、外送通道拓展带来的动态风险，建立长效防控迭代机制。运维团队定期梳理安全新规、工控漏洞与新能源系统安全预警，每季度更新多类业务隐患排查清单与判定标准[5]。常态化开展岗位实操培训与考核，补齐运维人员业务能力短板。同时复盘历史隐患台账，总结高频隐患发生规律，优化日常巡检防控重点，推动变电站网络安全治理从被动整改转向事前主动预防，持续提升高比例新能源、跨区特高压外送融合场景下的网络安全治理效能。

4 结论

本文结合哈密新能源基地与疆电外送枢纽电网特性，针对多业务融合场景下的网络安全治理短板，依托行业规范与现场经验，构建适配送端电网的全流程标准化治理体系。通过分类制定场站差异化管控方案，优化闭环管控流程与动态防控机制，可一定程度统一基层运维标准，规范特高压调度、新能源调控、无人机巡检等业务安全管理，改善传统治理碎片化问题。研究成果适配本地电网运行特征，可为西北同类新能源外送站点的网络安全治理提供参考思路。

［参考文献］

[1]谢哲,冯韵丞.智能变电站电力监控系统安全隐患治理策略研究[J].农村电气化,2025(5):26-29.

[2]徐日洲.本质安全建设实践方法研究(8)——隐患排查治理[J].电力安全技术,2020,22(8):1-4.

[3]文辉辉,苏楠.智能变电站电力监控系统网络安全防护研究[J].网络安全技术与应用,2024(6):132-133.

[4]祝婷.智能电网信息安全标准化工作探究[J].企业改革与管理,2017(17):219.

[5]文辉辉,苏楠.智能变电站电力监控系统网络安全防护研究[J].网络安全技术与应用,2024(6):132-133.

作者简介：陈文涛（1987.10—），男，汉族，陕西省西安市蓝田县，大学本科学历，职称级别：工程师，研究方向：资产全寿命周期管理、电网防灾减灾、生产网络与信息安全。