文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

新能源风电系统网络安全建设与维护策略研究

刘全
国家电投集团宁夏能源铝业中卫新能源有限公司
DOI:10.12238/etd.v6i8.17095

[摘　要] 新能源风电系统网络安全至关重要。本文先分析其网络架构,呈现分层分布式特点,并指出设备、网络、数据、应用各层级的安全风险及产生机理。接着设计网络安全建设框架,明确建设目标、原则,给出全生命周期及分层建设方案。随后制定维护策略,构建动态维护体系,提出日常、应急维护策略,并依托智能化技术提供支撑。旨在构建全面安全防护体系,保障风电系统稳定运行,满足行业合规要求。
[关键词] 新能源风电系统；网络安全；安全建设；维护策略
中图分类号：TM76　文献标识码：A

Research on Cybersecurity Construction and Maintenance Strategies for New Energy Wind Power Systems

Quan Liu
CPI Ningxia Energy Aluminum Industry Zhongwei New Energy Co., Ltd.

[Abstract] Cybersecurity in new energy wind power systems is of paramount importance. This paper begins by analyzing the network architecture of these systems, highlighting their layered and distributed characteristics, and identifies security risks and their mechanisms at various levels, including equipment, network, data, and application layers. Subsequently, a cybersecurity construction framework is designed, outlining construction objectives and principles, and proposing lifecycle and layered construction solutions. Maintenance strategies are then formulated, establishing a dynamic maintenance system that includes routine and emergency maintenance strategies, supported by intelligent technologies. The aim is to build a comprehensive security protection system to ensure the stable operation of wind power systems and meet industry compliance requirements.
[Key words] New Energy Wind Power Systems; Cybersecurity; Security Construction; Maintenance Strategies

引言

在全球能源转型的大背景下,新能源风电产业蓬勃发展。然而,随着风电系统智能化、网络化程度的提升,网络安全问题日益凸显。新能源风电系统网络架构复杂,涵盖设备、网络、数据、应用等多个层级,各层级均面临不同类型的安全风险,如设备级的老旧控制器易被攻击、网络级的通信协议存在漏洞等。这些风险不仅影响风电系统的稳定运行,还可能对电网安全造成威胁。因此,开展新能源风电系统网络安全建设与维护策略研究迫在眉睫。

1 新能源风电系统网络架构及安全风险分析

1.1风电系统网络架构解析

新能源风电系统网络架构呈现分层分布式特点,从底层到上层依次为设备层、网络层、数据层和应用层。设备层包含风电机组的主控系统、变桨系统、偏航系统及传感器等硬件设备,通过现场总线实现本地数据交互；网络层由工业以太网、无线通信模块及边缘网关组成,负责设备层数据上传与控制指令下发,采用电力专用通信协议保障传输稳定性；数据层涵盖本地边缘服务器和远程云平台,承担数据存储、预处理及备份功能；应用层包括监控中心的运维管理系统、发电预测系统和故障诊断系统,为管理人员提供可视化操作界面[1]。各层级通过标准化接口实现数据流转,形成“感知-传输-处理-应用”的闭环架构,其中边缘计算节点与云平台的协同运作,既保障实时控制需求,又满足远程运维管理要求。

1.2网络安全风险分类与机理

新能源风电系统网络安全风险可按影响层级分为设备级、网络级、数据级和应用级四类。设备级风险源于部分老旧风电机组控制器缺乏访问控制机制,攻击者可通过物理接触或串口通信注入恶意代码,导致变桨异常或停机；网络级风险主要包括通信协议漏洞和非法接入,如Modbus协议未加密传输易被窃听篡改,无线通信信道可能遭受干扰导致数据丢失；数据级风险体现在数据传输过程中完整性遭破坏,以及存储数据被未授权访问,如发电数据被篡改会影响电网调度决策；应用级风险表现为运

文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

维管理系统存在SQL注入漏洞,攻击者可通过漏洞获取管理员权限,伪造控制指令。这些风险的产生机理多与工业控制系统“重功能轻安全”的设计理念相关,加之风电场景分散导致的防护难度增加,使得风险易形成连锁反应。

2 新能源风电系统网络安全建设框架设计

2.1建设目标与设计原则

新能源风电系统网络安全建设目标为构建“纵深防御、动态适配、智能响应”的安全体系,实现对设备运行、数据传输、应用管理全流程的安全防护,保障风电系统连续稳定运行,抵御已知和未知网络攻击,满足电力行业网络安全合规要求。设计原则需遵循四个核心：一是合规性原则,严格契合《电力行业网络安全等级保护实施指南》等标准规范,确保安全建设符合行业监管要求；二是纵深防御原则,在设备、网络、数据、应用各层级部署独立防护措施,同时实现各层级防护协同联动;三是最小权限原则,对各类访问主体明确权限范围,仅授予完成操作必需的权限,避免权限滥用；四是技术与管理并重原则,既要部署先进安全技术设备,又要建立完善的安全管理制度,通过人员培训提升安全防护意识,形成技术防护与管理规范相互支撑的格局。

2.2全生命周期安全建设框架

新能源风电系统全生命周期安全建设框架覆盖规划设计、部署实施、运行维护、升级退役四个阶段。规划设计阶段需开展安全需求分析,结合风电项目规模和场景特点,将安全设计融入架构规划,明确各层级安全指标,选用具备安全认证的硬件设备和软件系统;部署实施阶段执行安全基线配置,对设备进行漏洞扫描和渗透测试,完成防火墙、入侵检测系统等安全设备部署,同步搭建安全监控平台;运行维护阶段建立日常巡检机制,定期更新安全补丁和病毒库,开展安全审计和风险评估,及时发现并处置安全隐患;升级退役阶段制定设备退出安全流程,对存储数据进行彻底清除,防止敏感信息泄露,同时对升级后的系统开展安全验证,确保新老系统切换过程安全可控[2]。该框架通过各阶段无缝衔接,实现安全建设贯穿系统全生命周期,避免出现安全防护断层。

2.3分层安全建设方案

2.3.1设备层安全建设

设备层安全建设以“硬件加固、访问管控、状态监测”为核心。对风电机组主控单元、变桨控制器等关键设备进行硬件加固,采用防拆外壳和电磁屏蔽设计,防止物理篡改和电磁干扰；部署设备访问控制系统,实施USB端口禁用、串口访问密码认证等措施,仅允许授权设备接入；安装主机入侵检测系统,实时监测设备进程运行状态,对异常进程和恶意代码立即拦截并报警。针对传感器等终端设备,采用数据加密传输方式,避免感知数据被篡改;建立设备固件全生命周期管理机制,定期推送安全补丁,对固件升级过程进行加密验证,防止恶意固件注入。同时,在设备部署前开展安全检测,剔除存在漏洞的设备,确保设备层具备基础安全防护能力,从源头降低安全风险。

2.3.2网络层安全建设

网络层安全建设聚焦“边界防护、通信加密、流量管控”三大重点。在风电场内部网络与外部公网、内部各子网之间部署下一代防火墙,划分安全区域,实施访问控制策略,仅开放必需通信端口；采用虚拟专用网络技术搭建风电场与远程监控中心的加密通信通道,对传输数据进行端到端加密,防止数据在传输过程中被窃听篡改。部署网络入侵检测与防御系统,实时监测网络流量,对异常流量、攻击行为进行识别和阻断；实施网络流量管控,限制非必要网络访问,优先保障控制指令和关键数据的传输带宽。建立网络拓扑动态监测机制,及时发现未授权接入设备；定期开展网络安全扫描和渗透测试,修复网络设备漏洞,升级网络协议版本,替换存在安全隐患的老旧通信设备,确保网络层具备抵御恶意攻击和异常访问的能力。

2.3.3数据层安全建设

数据层安全建设围绕“数据加密、访问控制、备份恢复”构建防护体系。对存储的发电数据、设备运行数据、运维数据等进行分类分级,核心数据采用AES加密算法存储,普通数据实施完整性校验;建立数据访问权限管理体系,基于角色分配访问权限,实现操作行为全程日志记录,确保数据访问可追溯。部署数据防泄漏系统,对敏感数据的导出、复制等操作进行管控,防止数据非法外泄;采用本地备份与异地备份相结合的方式,定期执行数据备份,备份数据进行加密存储,并开展备份恢复演练,确保数据在遭受破坏时可快速恢复。同时,建立数据生命周期管理机制,对过期数据按规范进行清理或归档,避免无效数据占用资源并带来安全隐患[3]。

2.3.4应用层安全建设

应用层安全建设以“漏洞防护、权限管控、行为审计”为核心措施。对运维管理系统、发电预测系统等应用系统开展常态化漏洞扫描,重点排查SQL注入、跨站脚本等常见漏洞,及时通过代码修复或版本升级消除隐患；采用应用防火墙对应用程序进行防护,拦截针对应用层的恶意攻击。建立严格的应用访问权限体系,实施多因素认证机制,防止账号密码被破解后非法登录;对应用系统的操作行为进行实时审计,重点监控控制指令下发、参数修改等关键操作,一旦发现异常行为立即触发报警并阻断操作。开展应用系统安全测试,在新系统上线前和版本更新后进行全面安全评估;加强应用程序代码安全管理,在开发阶段引入安全开发生命周期理念,从源头提升应用程序安全质量,确保应用层具备完善的安全防护能力。

3 新能源风电系统网络安全维护策略制定

3.1动态维护体系构建

新能源风电系统网络安全动态维护体系以“实时监测、风险预警、持续优化”为核心架构。搭建安全态势感知平台,整合设备层、网络层、数据层、应用层的安全监测数据,通过大数据分析技术实现安全状态实时可视化展示；建立风险预警模型,基于历史攻击数据和漏洞信息,对潜在安全风险进行分级预警,明确预警响应流程和责任主体。构建“风电场现场维护+远程集中维护”的两级维护模式,现场维护团队负责设备巡检和即时故

障处置,远程维护中心承担风险分析和技术支持;建立维护人员技能提升机制,定期开展网络安全技术培训和应急演练,提升维护团队专业能力。建立维护体系优化机制,定期收集维护过程中的问题和经验,结合技术发展和攻击手段变化,更新维护策略和技术方案,确保维护体系始终适配安全防护需求,实现从被动防御向主动防护的转变。

3.2日常安全维护策略

日常安全维护策略聚焦“常态化巡检、定期升级、规范操作”三大要点。制定每日巡检计划,安排维护人员对风电机组控制器、安全设备、网络设备运行状态进行检查,查看设备指示灯、日志信息,及时发现异常情况；每周开展网络流量分析,排查异常连接和可疑访问行为,确保网络运行稳定。每月对安全设备固件、应用系统版本、病毒库进行更新升级,对设备漏洞进行扫描修复,优先处理高危漏洞；每季度开展全面安全审计,核查访问权限分配合理性,清理无效账号和过期权限,确保权限管理规范。制定标准化操作流程,明确设备操作、数据备份、系统升级等环节的操作规范,避免人为操作失误引发安全风险;建立维护日志管理制度,详细记录巡检结果、维护操作、问题处置过程,为后续维护工作提供数据支撑,通过常态化管理筑牢安全防护基础。

3.3应急安全维护策略

应急安全维护策略以“快速响应、精准处置、恢复运行”为核心目标,建立“预警-处置-恢复-复盘”的闭环机制。制定分级应急预案,根据攻击造成的影响范围和损失程度,将应急事件分为一般、较大、重大三个等级,明确不同等级事件的响应流程、责任分工和处置时限。建立应急响应团队,由网络安全专家、设备运维人员、系统开发人员组成,24小时待命,接到应急预警后立即赶赴现场或远程介入处置。针对常见应急场景制定处置方案,如遭遇恶意代码攻击时,立即隔离受感染设备,清除恶意代码,恢复系统备份;发生数据泄露时,迅速定位泄露源头,阻断泄露通道,评估泄露影响并采取补救措施。应急事件处置完成后,组织复盘分析,查找事件原因和防护漏洞,优化应急预案和安全措施,提升应急处置能力。

3.4智能化维护技术支撑

智能化维护技术支撑体系深度依托人工智能、大数据、物联网等前沿技术,全力推动维护工作朝着精准化与高效化方向迈进。在设备故障预测方面,采用先进的机器学习算法,精心构建设备故障预测模型。该模型通过对设备运行数据的深度剖析,能够敏锐捕捉设备运行的细微变化,提前精准识别设备异常趋势,从而实现故障的早发现、早处置,有效降低设备故障对风电系统运行的影响。利用计算机视觉技术对风电机组关键部件展开远程巡检,彻底替代传统人工现场巡检模式[4]。搭建智能化安全分析平台,运用大数据挖掘技术对海量安全日志和流量数据进行全面分析,可精准识别隐藏其中的攻击行为和安全隐患,与传统人工分析相比,检测精度得到大幅提升。同时,部署具备自适应学习能力的智能防火墙和入侵防御系统,能根据网络环境变化自动调整防护策略,有效抵御新型未知攻击。另外,引入数字孪生技术构建风电系统虚拟模型,可模拟各类攻击场景和维护操作,为维护人员提供逼真的模拟训练环境,还能通过虚实联动实现维护方案的优化验证,全面提升维护技术水平。

4 结束语

新能源风电系统网络安全建设与维护是保障风电产业稳定发展的关键环节。本文通过剖析其网络架构与安全风险,设计了涵盖全生命周期与分层的安全建设框架,并制定了动态、日常、应急维护策略,借助智能化技术提升维护效能。随着网络攻击手段不断演变,未来需持续强化安全技术研究,完善安全管理体系,培养专业维护人才,以构建更坚固的安全防线,推动新能源风电系统安全、高效运行。

[参考文献]

[1]辛雁宇.新能源风电系统网络安全建设与维护策略研究[J].网络安全和信息化,2024(12):140-142.

[2]陈璐,汪晓彤,汪坤,等.新能源电站电化学储能系统辅助风电调频方法[J].电子设计工程,2024,32(22):151-154.

[3]吴新友.面向风电系统的混合储能容量优化配置研究[J].储能科学与技术,2024,13(10):3593-3595.

[4]曾广博,曾笑,邓全镔.新能源集中监视系统中的网络安全防护策略[J].电子元器件与信息技术,2025,9(3):207-209.