风电场监控系统网络安全管理与技术研究

郑春艳

国电河南新能源有限公司 河南郑州

【摘要】随着我国国民经济的高速健康发展，大部分风电场都采用无线网络电力监控系统，现代社会对风电场监控系统的网络安全可靠性的要求越来越高。近些年来，我国风电场监控系统网络安全事故频发，不利于风电场电力安全。监控系统网络安全技术迅速发展并不断完善，将其运用于监控系统网络安全管理当中，能提升电力监控系统安全性，使电力监控系统朝着智能化方向发展。本文分析了风电场监控系统网络安全技术应用，分析了风电场监控系统网络安全风险，并提出风电场监控系统网络安全管理的对策，以期促进我国风电场监控系统的安全稳定发展。

【关键词】风电场；监控系统；网络安全管理；技术应用

【收稿日期】2022 年 12 月 26 日 【出刊日期】2023 年 1 月 21 日 【DOI】10.12208/j.aics.20230005

Research on network security management and technology of wind farm monitoring system

Chunyan Zheng

Huaneng Lanzhou Fanping Thermoelectric Co., LTD. Lanzhou, Gansu

【**Abstract**】With the rapid and healthy development of China's national economy, most wind farms are using wireless network power monitoring system, modern society has increasingly high requirements for network security and reliability of wind farm monitoring system. In recent years, China's wind farm monitoring system network security accidents occur frequently, which is not conducive to wind farm power security. Monitoring system network security technology is rapidly developing and improving, and its use in monitoring system network security management can improve the security of the power monitoring system, so that the power monitoring system in the direction of intelligent development. This paper analyzes the application of wind farm monitoring system network security technology, analyzes the risk of wind farm monitoring system network security, and proposes countermeasures for wind farm monitoring system network security management, in order to promote the safe and stable development of China's wind farm monitoring system.

【**Keywords**】wind farm; monitoring system; network security management; technology application

近年来，我国大力推行可再生能源发电，风力发电市场迅速发展。与此同时，风电场监控系统的网络安全风险随之增加。一方面风电场监控系统技术应用不足，运维和管理能力较差；另一方面风电场监控系统往往重视应用开发，对安全防护缺乏重视，这就导致风电场监控系统容易遭受网络安全风险威胁。因此，需要加强风电场监控系统的技术应用和安全管理，切实提升风电场监控系统安全系数。

1 风电场监控系统网络安全技术应用

1.1 无线网络技术

把无线网络技术运用到风电场监控系统中还可以推动其向智能化方面发展,但随着中国电力行业的持续发展,变电、配电和用电等环节都是智慧电网中构建的最重要,对智能化技术设备与装置的要求也将日益增强。运用无线网络技术，可以实现风电场监控系统的自动化和智能化，对无线局域网进行扩容，并借助信息技术、检测手段等可以实时监测电力系统的运行状态，与人工监控方式相比，节省了大量人工和时间成本。同时，若是系统运行出现问题时，无线网络技术能迅速识别并自动报警，检

作者简介：郑春艳（1987-）女，汉族，工程师，单位：国电河南新能源有限公司

测出问题所在位置后将数据传输给工作人员，让工作人员能够及时处理问题故障，降低工作强度，减少人工成本。通过无线网络技术的智能化，缩减风电场监控系统故障的处理时间，提升工作效率。

1.2 服务器虚拟化技术

服务器虚拟化技术作为虚拟化技术的重要应用领域，在数字化转型升级的推动和数字基础设施安全可靠升级的需求驱动下，对风电场监控系统的网络安全具有重要作用。服务器虚拟化技术在应用迁移、拓展以及持续集成方面也更加灵活，十分高效便捷，安全与稳定性相对较强，同时虚拟化也更适合传统的应用架构。由于服务虚拟化技术对网络环境更具开放性，能够更广泛地兼容传统集中存储和网络环境，充分满足风电场监控系统的超融合建设需求。风电场监控系统的硬件寿命有限，同时具有较高的算力和存储需求，容易造成硬件资源浪费，而服务器虚拟化技术能很好地解决上述问题，实现硬件与监控系统的耦合，提升风电场监控系统的运行稳定性，降低网络安全管理成本。

2 风电场监控系统网络安全风险分析

2.1 集中控制与远程运维风险

由于风电场多位于地理位置较为偏远的山区或郊区，规模相对其他传统电力企业来说较小，电力系统维护人员相对不足。为了节约运营和维护成本，部分风电企业选择建设集控中心来对风电场的监控系统进行远程控制。同时，风电场往往支持通过互联网对监控系统进行远程维护。一方面，疾控中心和风电场监控系统的安全防护措施不到位，缺乏完善的安全防护标准。虽然部分风电企业具有加密认证和网络访问的防护措施，但是这也存在控制网络被侵入和数据泄露等风险。另一方面，集控中心对风电场监控系统进行直接控制，若是遭到黑客攻击，则容易对管辖区域内的风电场监控系统造成直接威胁，造成风电场监控系统大面积脱网。此外，部分设备厂家对风电场监控系统进行远程维护时，需要通过互联网与监控系统进行连接，这就会暴露监控系统的数据信息。同时存在维护人员账号被盗用、操作失误等风险，不利于风电场监控系统安全。

2.2 终端网络接入安全风险

风电场的占地面积较大，往往相邻的风力发电机具有较远的距离，而其之间大多是通过局域环网与监控主机进行通信。不同风电机设备接入电网，需要通过光纤交换机进行互联，而大部分风电机进行访问时都缺乏身份认证、数据保护和网络访问控制等安全防护措施。部分风电机与监控系统主机进行通信时，没有按照要求设置相应的安全方案，这就容易导致终端网络接入时，无线通信泄露、控制指令被篡改等风险。风电场分布式终端类型繁多，数据传输方式尚未标准化，接入以无线公网为主，缺乏统一的安全防护技术标准，存在带病入网等问题；不同业务的分布式终端对电网基于分区隔离的安全防护架构带来冲击，管理难度进一步增大。一些风电场风力发电机控制终端可以直接接入网络，对监控系统进行直接访问，存在数据被截获的危险。

2.3 系统本体安全风险

个别风电场监控系统所采用的服务器、交换机等网络设备未通过国家检测合格标准，并未对监控系统相关设备进行安全加固，这就导致监控系统本身存在安全隐患。一些风电场监控系统的主服务器未采用部门认证的安全加固措施，控制系统存在违规操作现象。部分监控系统的路由器、服务器等设备端口未及时关闭，提升网络安全风险。监控系统使用的设备繁多，零部件杂乱，若是出现故障，不仅诊断工作量大，而且没有及时维修的话会影响监控系统整体运行状态。

2.4 人员配置与安全管理风险

部分风电场由于建设和运行原因，并没有落实电网要求的网络安全防护政策，未设置安全的隔离设备和正反向隔离装置。有些风电场虽然设置了安全防护措施，但是设备出现问题、安全功能不完善等情况经常存在，网络访问控制策略受到限制，存在安全管理风险。在技术方面，风电场监控系统缺少网络安全监测技术手段，不能实现全方位、全时段的安全监测，缺乏一定的安全响应措施。在管理方面，部分风电场不能及时发现并整治网络安全问题，缺乏应急预案和制度落实管控能力。同时对信息机房基础环境隐患缺乏整治，网络安全管理存在漏洞，对网络与监控系统安全产生威胁。同时，风电场人员配置不合理，工作人员缺乏专业的系统培训。部分风电场依靠厂家进行监控系统的维护和管理，配有配备专门的运维人员。

3 风电场监控系统网络安全管理对策

3.1 强化监控主机的网络连接防护

风电场监控系统主机的安全管理成为风电企业网络安全工作的一个重要组成部分，不安全的监控主机网络连接存在重大的风险，并可能导致许多网络安全问题。强化监控主机网络连接防护目的就在于保护终端网络与监控主机通信时的数据和资源。一方面，需要设置风电场新能源采集终端与监控主机之间通信连接的身份认证、数据保护和访问权限等方面的安全防护措施，设置无线网络安全接入区域，实现数据的安全保护。对于暂时不具备无线传输的风电场采取有线方式进行监控，同时加强网络地址绑定、设置 IP 网络安全地址等安全加固方法。另一方面，通过轻量级 agent 探针，全面采集监控主机内部的各项信息，有效识别进程、账号、端口、软件、web 等信息，及存在的漏洞、弱口令、缺失配置等安全风险，及时进行安全预警，通过闭环的风险管理协助用户进行优化修改。增加口令强度、及时修复系统漏洞和应用漏洞，以及强化端口管理，除必要业务之外，应关闭高危端口，减少资产的暴露面，降低被攻击的可能性。

3.2 加强监控系统网络安全边界防护

在 5G、物联网等新兴技术快速发展的背景下，我国的风电市场规模逐渐扩大，随之而来的便是对风电运营管控水平要求的提高，传统粗放式管理已不能满足当下风电市场的需求。一方面，加强风电场监控系统网络安全边界防护。区别于传统防火墙 IP 方式，采用自然语言模型来建设策略。通过针对网络安全边界进行标签建设，即使边界发生了移动或者其他变化，微隔离可以根据标签追踪，自适应将策略覆盖到网络。另外为了更方便地建设微隔离策略，通过大量研究内网流量业务模型，内置自动策略生成机制，即使从未使用过微隔离产品，也能快速上手进行策略建设。另一方面，规范风电场监控系统互联网出口管理和监控，设置防火墙等安全措施。合理优化内网入侵检测系统与入侵防御系统设备，进一步优化在防火墙内到外及外到内访问策略的 IPS 和反病毒过滤。将所有网络安全设备接入日志管理系统，并实现防火墙管理账号和权限分离，规范各类安全设备使用及配置规则。在筑牢风电场网络安全边界的基础上，还对所辖终端设备开展了安全维护工作，集中对终端设备进行漏洞核查、漏洞修复、版本升级等工作。

3.3 加强应用防护，禁止违规外联

建立风电场监控系统应用安全防护，落实安全标准，逐步完善身份认证和安全审计等板块的安全措施。开展监控系统无线网络源代码安全防护，及时对监控系统源代码进行监测，防止漏洞和恶意代码对监控系统造成不利影响。同时，严格执行电网权限管理和网络安全管理等方面的要求，加强监控系统安全性。在风电场监控系统中，工作人员使用 U 盘、移动硬盘等移动存储设备进行数据拷贝时，可能会增加监控系统风险，导致监控系统出现故障，造成风电机组与集控中心的通信中断，使风电机组脱离监控，从而引发一定的电力危险。因此，风电场监控系统需要合理使用移动存储设备，禁止违规外联。同时，依据国家网络安全法管理制度及规范，通过下发网络安全宣传资料、现场培训讲座、咨询答疑等多种形式，宣传个人重要数据保护、移动终端安全行为等网络安全知识，让工作人员了解身边的网络安全风险，认识隐藏的网络安全威胁，有效提升全员安全防范意识。

3.4 设置网络安全监测装置

对风电场监控系统加强远程监测，设置网络安全监测装置，可以识别系统内部运行状况是否受电力设备干扰的情况，若是出现故障就会发出警报，及时通知系统设备维护工作人员进行修理。同时，通过网络安全监测装置，可以监控电力系统的相关参数，保证数据及时、准确反馈给工作人员，方便工作人员进行分析和研究，设置定时排查、实时监测、自动报警等实现对监控系统的实时监测。监测监控系统还可将数据进行分类、存储，方便判断监控系统发生故障的原因，同时降低电力工作人员的工作难度，提高监控系统的安全和自动化水平。此外，设置监控系统网络安全管控平台，通过数据的实时采集、接收及传输，对风电场远程监控自动化管理，实现风电场的生产运行监测、设备故障预警和后勤管理集中化，实现风电管理智能化、精细化，真正为风电场系统降本增效。

4 结语

综上所述，我国风电场监控系统建设日益完善，随着无线网络技术和服务器虚拟技术在各行业的纵深发展以及能源分散化趋势的进一步加强，将其应

用于风电场监控系统，并加强监控系统的网络安全管理成为风电场发展的当务之急。针对当前风电场监控系统的安全风险，可以通过强化监控主机的网络连接防护、加强监控系统网络安全边界防护、加强应用防护，禁止违规外联、设置网络安全监测装置等途径加强监控系统网络安全管理，为风电场的网络安全发展提供保障。

参考文献

[1] 李林波,钱凯,莫浩,罗文延.风电场网络安全管理思路[J].云南水力发电,2022,38(S1):97-100.

[2] 汪义舟.风电场电力监控系统网络安全防护方案[J].自动化博览,2021,38(01):38-41.

[3] 栗会峰,刘哲,李宣义,栗维勋,王亚军.风电场电力监控系统网络安全防护措施优化[J].东北电力技术,2020,41(10):23-26.

[4] 钟丽波,周洋,李然,马煜,纪秀艳.电力监控系统网络末端安全防护案例分析[J].东北电力技术,2020,41(09):51-54.

[5] 丁伟.风电场电力监控系统网络安全威胁防控体系[J].电信科学,2020,36(05):138-144.