风电场电气工程智能监控系统的可靠性与安全性研究

谭海昕　赵宏伟　毕　庆　白云鹤　王明星
华能新能源股份有限公司蒙东分公司　内蒙古　通辽　028100

摘　要：随着风电场规模扩大与智能化转型，其电气工程的稳定运行对能源供应安全至关重要。智能监控系统作为核心管理手段，其可靠性与安全性直接影响发电效率、设备寿命及电网稳定性。本文从功能需求、可靠性强化技术、安全防护体系三个维度展开研究，针对硬件故障、网络攻击、数据异常等挑战，提出冗余配置、数据加密、智能诊断等理论方案，并结合工业场景需求探讨技术融合路径。研究指出，通过物联网、人工智能与区块链技术的协同创新，可构建具备高鲁棒性、实时性与抗攻击能力的智能监控系统，为风电场安全运维提供理论支撑。

关键词：风电场智能监控；可靠性设计；网络安全；故障预测；边缘计算

引言

在全球能源结构低碳化转型背景下，风电场作为可再生能源主力军，其电气系统复杂性持续升级。传统人工运维模式已难以应对大规模风电场的实时状态监测、故障预警与能效优化需求。智能监控系统通过集成先进传感、通信与智能分析技术，成为保障风电场稳定运行的关键。然而，系统在极端环境下的可靠性不足、工业网络边界防护薄弱等问题仍待突破。本文围绕系统架构优化、可靠性增强与安全保障技术展开研究，旨在为风电场智能监控提供理论创新与工程实践指导。

1 风电场智能监控系统的架构与功能需求

1.1 系统架构分析

典型的风电场智能监控系统采用分层架构，各层紧密协作，共同保障风电场的高效稳定运行。感知层是系统的数据基石。在这一层，部署了丰富多样的传感器，像振动传感器能敏锐捕捉风机部件的细微振动变化，温度传感器可精准监测关键部位的温度，电流互感器则实时获取电流参数。这些传感器如同敏锐的触角，全方位采集风机的运行状态、电网参数以及环境数据，为后续的分析和决策提供详实可靠的数据支撑。传输层是数据流通的高速通道。它依托5G专网或光纤骨干网构建高可靠通信链路。然而，这一过程中面临诸多难题，电磁干扰可能使数据出现偏差，长距离传输损耗会影响数据质量，实时性保障更是关键，任何延迟都可能导致决策失误。因此，需要采用先进的抗干扰技术、信号增强设备以及优化通信协议来解决这些问题。处理层是系统的智慧大脑。边缘计算节点凭借其强大的实时处理能力，快速完成故障特征提取等数据分析任务。云平台则发挥其海量数据存储和强大计算能力的优势，负责深度学习模型训练与全局优化决策，为系统的智能化运行提供核心支持。应用层是系统与用户交互的界面。它提供设备健康管理、功率预测、能效优化及应急控制等功能模块。通过这些模块，管理人员可以实时了解风机状态，提前预测功率输出，优化能源利用效率，并在突发故障时迅速采取应急措施。

1.2 功能需求与挑战

风电场智能监控系统面临着多方面的功能需求与挑战。首先是高可靠性需求，风电场往往位于沙漠、海上等严酷环境中，系统需要在极端温度、湿度条件下稳定运行。这就要求系统的硬件设备和软件系统都具备高度的可靠性和稳定性。安全威胁也是系统面临的重要挑战之一。系统需要防御针对工业控制系统的定向攻击，如Triton恶意软件，还要防止数据篡改及拒绝服务攻击。这需要采用先进的安全技术和策略，保障系统的网络安全。动态适应性同样不可忽视。系统需要实时响应风速波动、电网调频指令及突发故障，实现秒级决策与毫秒级控制[1]。这就要求系统具备快速的数据处理能力和灵活的控制策略，以应对各种复杂的情况。只有满足这些功能需求，克服相应的挑战，风电场智能监控系统才能发挥其最大的作用，为风电场的高效运行提供有力保障。

2 风电场电气工程智能监控系统的可靠性强化技术研究

2.1 硬件可靠性设计

硬件作为智能监控系统的基础支撑，其可靠性直接决定了整个系统的稳定运行能力。因此，在硬件设计中，必须充分考虑冗余配置、环境适应性等因素，以确保硬件设备的高可靠性。

2.1.1 冗余配置策略

冗余配置是提高系统可靠性的有效手段之一。在风电场电气工程智能监控系统中，关键设备如主控制器、

通信网络等应采用双机热备或三模冗余（TMR）结构。双机热备意味着在系统正常运行时，一台设备作为主设备工作，另一台设备作为备用设备处于待机状态。一旦主设备出现故障，备用设备将立即接管工作，确保系统不间断运行。而三模冗余结构则通过三个相同的模块同时工作，并通过投票机制决定输出结果，从而进一步提高系统的可靠性。理论分析表明，采用TMR结构可以使系统可靠性提升10倍以上，有效降低系统故障风险。

2.1.2 环境适应性优化

风电场环境复杂多变，设备常常面临极端温度、盐雾腐蚀、尘土飞扬等恶劣条件的挑战。因此，在硬件设计中，必须充分考虑环境适应性。选用宽温范围工业级芯片（-40℃~85℃）可以确保设备在极端温度下仍能正常工作。同时，采用防盐雾涂层可以有效抵御盐雾腐蚀，延长设备使用寿命[2]。此外，设备外壳应采用IP68防护等级，确保设备在尘土、水汽等恶劣环境中具备良好的密封性能。通过这些环境适应性优化措施，可以显著提升设备在恶劣环境下的生存能力，保障系统的稳定运行。

2.2 软件可靠性保障

软件作为智能监控系统的核心组成部分，其可靠性同样至关重要。为了提高软件可靠性，可以从容错算法设计和自愈机制构建两个方面入手。

2.2.1 容错算法设计

在智能监控系统中，传感器数据是系统状态估计和决策的重要依据。然而，由于传感器本身存在噪声和异常值，这些数据往往并不完全准确。为了提高状态估计精度，可以采用基于扩展卡尔曼滤波的数据融合算法。该算法能够有效过滤传感器噪声与异常值，通过融合多个传感器的数据，得到更加准确的状态估计结果。这不仅提高了系统的监控精度，还为系统的决策提供了更加可靠的数据支持。

2.2.2 自愈机制构建

自愈机制是智能监控系统的一项重要功能，它能够在系统出现故障时自动进行故障诊断和恢复，从而缩短故障响应时间，提高系统的可用性。为了实现自愈机制，可以借助数字孪生技术构建虚拟设备模型。数字孪生技术是一种通过数字化手段构建物理世界与虚拟世界之间映射关系的技术。在智能监控系统中，可以利用数字孪生技术构建风电机组、变压器等关键设备的虚拟模型。这些虚拟模型能够实时反映物理设备的运行状态，并进行故障模式仿真。一旦物理设备出现故障，虚拟模型可以迅速定位故障原因，并生成自动恢复策略。通过执行这些恢复策略，系统可以在秒级时间内恢复正常运行，大大降低了故障对系统的影响。

2.3 数据传输可靠性

在智能监控系统中，数据传输的可靠性同样至关重要。如果数据传输过程中出现误码或丢失，将导致系统无法准确获取设备状态信息，进而影响系统的监控和决策能力。为了提高数据传输可靠性，可以从信道编码技术和分布式存储方案两个方面入手。

2.3.1 信道编码技术

信道编码技术是一种通过增加冗余信息来提高数据传输可靠性的方法。在智能监控系统中，可以采用LDPC（低密度奇偶校验码）前向纠错码来降低误码率。LDPC码是一种具有优异性能的信道编码方式，它能够在较低的信噪比下实现较高的纠错能力。通过采用LDPC码，系统可以在数据传输过程中有效抵抗噪声和干扰，提高数据传输的可靠性。同时，结合QoS（服务质量）机制，可以优先保障控制指令的传输带宽，确保控制指令能够及时、准确地传达到各个设备。

2.3.2 分布式存储方案

关键运行参数是智能监控系统的重要数据资源，它们的完整性和可追溯性对于系统的运行和维护至关重要。为了确保关键运行参数的安全存储，可以采用基于区块链技术的分布式冗余存储方案。区块链技术是一种去中心化的分布式账本技术，它能够通过加密算法和共识机制确保数据的完整性和可追溯性[3]。在智能监控系统中，可以将关键运行参数存储在多个节点上，形成分布式冗余存储。这样，即使某个节点出现故障或数据丢失，也可以从其他节点中恢复数据，确保数据的完整性和可靠性。

3 风电场电气工程智能监控系统的安全性防护体系构建

在保障智能监控系统可靠性的同时，还必须充分考虑系统的安全性。因为一旦系统遭到攻击或数据泄露，将可能导致严重的后果。为了构建安全可靠的智能监控系统，可以从网络安全防护、数据安全保护以及物理安全加固三个方面入手。

3.1 网络安全防护

网络安全是智能监控系统安全性的重要组成部分。为了保障网络安全，可以采用边界隔离技术和入侵检测机制。

3.1.1 边界隔离技术

边界隔离技术是一种通过划分网络区域、限制网络流量来保障网络安全的方法。在智能监控系统中，可以部署工业防火墙和单向隔离网闸，将控制区与非控制区

进行隔离。工业防火墙能够监控和过滤网络流量，阻止未经授权的访问和攻击。单向隔离网闸则能够实现数据的单向传输，确保控制区的数据不会泄露到非控制区。同时，通过实施网络流量白名单管理，可以进一步限制网络流量的传输，提高网络的安全性。

3.1.2 入侵检测机制

入侵检测机制是一种通过监测网络流量、识别异常行为来保障网络安全的方法。在智能监控系统中，可以采用基于深度学习的工业协议异常检测模型。该模型能够对Modbus/TCP、IEC 104等工业协议进行深度解析，识别隐蔽的攻击行为。通过实时监测网络流量，并与正常行为模型进行比对，可以及时发现异常行为并采取相应的防御措施，确保网络的安全性。

3.2 数据安全保护

数据安全是智能监控系统安全性的核心。为了保障数据安全，可以采用加密技术融合和隐私保护方案。

3.2.1 加密技术融合

加密技术是一种通过算法将明文数据转换为密文数据，从而保障数据机密性的方法。在智能监控系统中，可以采用AES-256算法对传输数据进行加密。AES-256算法是一种具有高安全性的加密算法，它能够有效地抵抗各种攻击手段。同时，结合数字签名技术，可以实现数据源头的认证和防篡改[4]。数字签名是一种通过私钥加密、公钥验证的方式，确保数据的完整性和真实性。通过加密技术融合，可以确保传输数据的安全性和可靠性。

3.2.2 隐私保护方案

隐私保护是智能监控系统数据安全性的重要方面。为了保障隐私数据的安全，可以采用联邦学习框架实现风机状态数据的分布式建模。联邦学习是一种去中心化的机器学习方法，它能够在不泄露原始数据的前提下，实现数据的共享和建模。在智能监控系统中，可以将风机状态数据分布在多个节点上，并通过联邦学习框架进行建模和分析。这样，既可以利用大数据的优势提高模型的准确性，又可以确保原始数据不出场，满足GDPR等隐私合规要求。

3.3 物理安全加固

物理安全是智能监控系统安全性的基础。为了保障物理安全，可以采用设备认证机制和电磁防护设计。

3.3.1 设备认证机制

设备认证机制是一种通过验证设备身份来保障物理安全的方法。在智能监控系统中，可以采用基于物理不可克隆函数（PUF）的硬件根密钥生成技术。PUF是一种利用物理特性生成唯一标识的技术，它能够确保每个设备都有一个独特的身份标识。通过PUF技术生成的硬件根密钥可以用于设备身份的认证和加密通信，防止未经授权的设备接入系统，提高系统的物理安全性。

3.3.2 电磁防护设计

电磁防护设计是一种通过减少电磁干扰和抵御电磁攻击来保障物理安全的方法。在智能监控系统中，关键设备应采用金属屏蔽罩和电磁干扰滤波器。金属屏蔽罩能够有效地阻挡外部电磁场的干扰，保护设备内部的电子元件不受损害。电磁干扰滤波器则能够滤除电源线和信号线上的电磁噪声，减少设备对外部电磁场的敏感性和发射性。通过电磁防护设计，可以提高设备的抗电磁干扰能力和抵御电磁攻击的能力，确保系统的物理安全性。

结语

本文提出的风电场智能监控系统架构，通过硬件冗余、边缘计算与安全防护技术的协同优化，形成了高鲁棒性、低时延与强抗攻击能力的理论体系。研究指出，冗余配置可显著提升系统可靠性，数字孪生技术为故障自愈提供新范式，而区块链与联邦学习的融合则解决了数据安全与隐私保护难题。未来随着新能源渗透率的提升，智能监控系统将成为保障能源安全的关键基础设施。未来研究需进一步探索多源异构数据融合、群体智能决策等前沿方向，构建更为安全、高效、智能的风电运维体系，助力能源系统深度脱碳。

参考文献

[1]郭建英.风电场电力监控系统安全防护的探讨[J].电气技术与经济,2023,(07):300-302.

[2]郝天敏.风电场中的电气参数检测与监控技术研究[J].电工技术,2024,(S1):320-323.

[3]张智伟,黄琛,杨武炳,等.海上风电场中的远程集成监控系统设计[J].电子技术,2024,53(04):56-57.

[4]孙本鹤,汝会通,季树海.风电场电力监控系统网络安全管理与技术研究[J].电力安全技术,2023,25(05):7-10.