电力系统及其自动化技术安全控制问题和对策

周良 周仕渠
特变电工智慧能源公司 辽宁 沈阳 110144

摘 要 随着电力系统自动化与网络化水平的提升，信息安全、设备可靠性和后备电源保障成为关键挑战。主要风险包括：厂站端网络防护薄弱、主站端软硬件兼容性问题及外部攻击，电气设备高负荷运行下的老化与故障预警失效，UPS维护不足及电源冗余机制风险。对此，本文提出强化网络防护、实施设备智能巡检、完善电源测试与监控、构建实时预警系统等策略，具体通过部署防火墙与加密技术、物联网巡检平台、UPS定期检测及LSTM预测模型等措施，实现电网状态动态感知与风险预警。实际应用表明，相关方案可降低系统故障停机率约42%，延长设备寿命15%～20%，显著提升电力系统运行安全与稳定性。

关键词 电力系统；自动化技术；安全控制问题；对策

Safety Control Issues and Countermeasures in Power Systems and Automation Technology

Zhou Liang, Zhou Shi-qu
TBEA Smart Energy Co., Ltd., Shenyang 110144, Liaoning Province, China

Abstract Under the deepening integration of information technology and the power industry, the automation and networking of power systems have significantly improved efficiency and enabled intelligent monitoring, yet also introduced complex security challenges. Key risks include inadequate network protection at substations, software-hardware compatibility issues and external attacks at control centers, aging of electrical equipment under high loads due to insufficient maintenance, and failures in backup power supply mechanisms such as UPS. To address these, strategies such as enhanced network security, intelligent equipment lifecycle inspection, improved power testing and monitoring, and real-time smart warning systems have been proposed. Specific measures include deploying firewalls and encryption, IoT-based inspection platforms, regular UPS discharge tests, and LSTM-based prediction models. These approaches enable dynamic monitoring and risk early warning, reducing system downtime by approximately 42% and extending equipment lifespan by 15%–20%, thereby strengthening the security and stability of automated power system operations.

Key words Power System; Automation Technology; Safety Control Issues; Countermeasures

电网安全管理面临着许多新的挑战。在人身安全层面，重点是要保证电气装备的可靠性与使用年限，既要确保在各种严酷环境中能够稳定工作，又要有抵御地震、洪水等自然灾害的能力，为整个系统的稳定性提供可靠的硬件支持。从网络安全角度看，主要是对系统内的数据和通信进行保护，避免由于外界入侵或内部故障造成的服务中断，并对黑客攻击、恶意软件传播等网络威胁进行有效防范。随着电网自动化程度的提升和网络化程度的加深，电网的架构变得越来越复杂，面临的风险也越来越多，安全保护的难度也越来越大。

1 电力系统自动化概述

随着信息技术的不断进步，电力工业智能化实现了加速发展。新一代技术重塑了电能生产传输及效率提升，构建了核心设备智能监控系统与“虚拟电厂”模型，我国在电源侧控制、配电自动化领域已有技术优势。

当前，SCADA平台突破推动电力调度自动化系统升级，融合多模块构建立体防控系统，某省网应用后准确率达98.7%、供电恢复时间缩短65%。但技术迭代暴露结构耦合度高、异常识别滞后等问题，后续应聚焦失效预测模型、自适应人机接口、信息安全机制三大方向解决。

2 电力系统及其自动化技术的安全控制问题

2.1 网络安全控制问题

1.厂站端。对电网和自动控制的安全性进行研究，特别是电厂和变电站的安全保护显得尤为重要。目前，网络安全管理面临如下问题：第一，就是保护好网络边界问题。要对境外网络的各类攻击进行有效防御，切实加强边境防卫能力。第二，在网络环境下进行数据传输的安全性问题。要保证数据的保密性和完整性，不受非法窃取和篡改。第三，通信协议的安全性问题。应保证通信活动严格遵守协定的规定，以防止由于协定

不足而造成的安全漏洞。主站使用的TCP/IP协议，在提高通信效率的同时，还加大了攻击者的攻击范围。与此同时，应用层的协议种类繁多，容易成为攻击的切入点，如ARP欺骗攻击等，如表1所示。

表1 TCP/IP协议具体内容

层级	常见协议与应用
应用层	Telnet、FTP、HTTP、SMTP、SNMP、TFTP、NFS、P2P 等
传输层	TCP、UDP
网络层	IP、ICMP、ARP、IGMP
链路层	以太网（Ethernet）、令牌环网（Token Ring）、HDLC、PPP、802.2、802.3

2.主站端。主站端的安全保护是电网安全运行的重要组成部分。要有效地提高主站的安全性，应在多维层面上进行协作。首先，要保证软硬件的兼容性，对整个体系结构进行优化，提高核心程序的稳定性和容错性。其次，在网络层次上，要对网络的拓扑结构进行科学的规划，对网络节点进行合理的配置，选择具有安全机制的通信协议，形成一种深度的防御体系，提升整个系统的抵御风险的能力。另外，目前信息安全形势日趋严峻，黑客入侵、恶意软件传播等风险依然存在，若防御措施不当，很容易导致主站系统非正常工作，进而影响电网安全[1]。

2.2 设备安全控制问题

在自动控制装置的实际使用中，保证它一直处在一个很好的工作状态是非常重要的。但是，该类装备的电气电路易受外界温度、湿度等因素的影响，工作工况苛刻，往往需要全天时连续运转。由于受资金、维修周期和外界环境影响，一些设备在运行过程中出现了过载现象。长期高负载运行会加速装备的老化，进而降低整个系统的安全性。所以，在生产过程中，要对关键部件进行严格的质量检查，通过引入冗余设计和心跳监控等保护措施，可提高系统的工作稳定性。但是，当通信线路发生异常时，这些保护措施就会失去作用，从而使整个系统的可靠性大大降低。

2.3 电源安全控制问题

当前，尽管状态监测、电能质量分析等手段可有效调控电网运行，但难以解决电源安全控制的深层次问题。连续稳定的供电是自动化系统可靠运行的前提。目前，多数系统依赖UPS作为后备电源，但部分供电公司在部署后缺乏系统化维护，导致设备老化、性能下降甚至失效，给关键设备带来安全隐患。为此，多数电网服务器已配备双电源冗余，可在单路故障时保障设备持续运行。然而，若双电源同时失效，仍可能导致服务器断电引发系统全面停机，风险依然存在。

3 电力系统及其自动化技术的安全控制对策

3.1 加强网络二次防护水平

厂站端总控与主站端通信的实现方式如图1所示。该结构采用静态路由，在保证工厂和工作站之间连通性的同时，保证了数据上传的安全性。此外，还可以采用各种技术与战略，对网络的安全进行管理。例如，利用防火墙控制网络通信量，防止非法接入；在传输过程中，采用加密技术保障数据安全，避免信息的泄漏；使用密码算法保证数据完整；引进一套安全审核制度，对网络的安全措施进行检验，确保与国家及工业规范相一致；通过引入人工智能、机器学习等新技术，进一步提升网络安全管控的智能性和防护效能[2]。

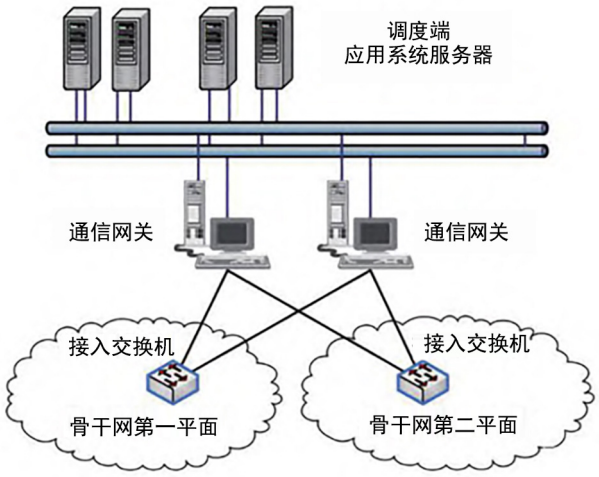

图1 总站双主机双网卡模式物理连接

3.2 加强设备巡检管理

要加强对设备的日常巡视和管理，及时发现和处理故障。在设备选择和采购环节，一定要严格把关，选用设计合理，性能匹配，生产厂家有良好声誉的产品，从根源上提高设备的可靠性。加强对工地设施的监督，对各种安全隐患进行检查和治理。在装置投产后，要密切注意工作环境，并结合现场工作情况，对操作参数进行动态调整，以保证装置的正常运转。同时，要制定出一套科学的巡视制度，并严格的实施。针对服务器等关键设备，提出了采取冗余结构、完善备用系统、定期进行数据备份等措施，以防止由硬件失效造成的服务中断和安全风险。通过与物联网技术相结合，可以构建一个用电设备的智能巡检平台，实现对设备状况的实时监测，以及有效的处理。

3.3 加强电源测试与电力监控

对UPS进行定期放电测试，制订详细的供电维修规范，强化供电设备的日常维护。对蓄电池进行连续监测，如有不正常

现象，立即处理。在进行电源检查时，要认真核实线路的连接情况，以保证有足够的备用容量，以免接线出现故障而影响到系统的平稳运行。在工业监测领域，为了保证整个电网的正常运转，必须建立实时数据库管理平台。它的实时性和稳定性对整个系统的性能有很大的影响[3]。同时，提出了一种基于实时数据更新、目标精确定位和高效索引的方法。将实时性和数据一致性相结合，建立一套分布式实时数据库监测系统，并对系统的性能进行测试，结果见表2。

表2　实时库读写性能测试结果

数据点数		300万	600万
读写性能	—	98万次/s	94万次/s
	64字节	62万次/s	61万次/s
	256字节	56万次/s	55万次/s
	1024字节	49万次/s	48万次/s
	2048字节	43万次/s	42万次/s

实验结果显示，本系统具有良好的读写能力、稳定的工作响应时间、较低的波动率，可以实现对配电网络的连续供电，并有效降低系统运行中的安全隐患。

3.4 实时监测报警

随着电网安全管理与自动化水平的提升，构建集动态监测与风险预测于一体的智能防控系统成为保障电网安全的关键。本项目集成多源传感设备、分布式计算架构及自主学习算法，实现对电网运行状态的全面感知与趋势动态预测，增强应急响应能力。

系统通过部署于电网关键节点的智能传感器，实时监测电压、电流、谐波、温湿度等200余项参数。数据经5G与光纤双通道传输至边缘计算层，确保低延迟汇聚。同时，搭载红外与声学传感器的轨道巡检机器人持续监测导线弧垂、金具温度及绝缘子状态。系统具备三级自动报警功能，可在3 min内识别故障，减少人工巡检工作量达65%。

基于流式数据处理技术，系统实现海量实时数据的关联分析。项目建立基于LSTM的时间序列预测模型，结合迁移学习自适应优化预警阈值。以变压器油中溶解气体（DGA）分析为例，融合DGA数据与SCADA负荷信息，采用蒙特卡洛方法动态预测油温，实现较传统定值报警提前4～6 h预警。

系统已在某省级电网实际部署，成功识别并处置17起设备异常。典型案例如某220 kV变电站主变油温异常事件，系统通过比对历史数据与实时负荷，提前2 h预警，运维人员及时启动喷淋降温，使设备温升降低18℃，避免了停电事故[4]。

实际应用表明，该系统可降低42%电网故障停机率，延长设备寿命15%～20%，综合效益显著。

4　电力系统及其自动化技术的安全控制问题应对展望

电力系统及其自动化是提高电网运行效率的重要手段，具有广泛的发展前景。在技术层面上，其可以很好地解决系统的安全性问题，并通过大数据和分布式控制等方法进行不断优化。例如，基于物联网和区块链技术的分布式控制系统。管理层可以根据这些数据对系统的运作状况进行监控，并建立分层的自动化结构。每个单位都设置了一个单独的区块链管理模块，并输入到系统中，从而形成一种适合当地特色的自动管理方式[5]。

5　结束语

电力系统自动化对保障电网稳定至关重要，但其安全风险日益凸显。确保安全，应强化网络、设备和电源的防护，并推广智能化巡检以提升实时监控能力。同时，应严格把控制度建设、设备选型和运维管理，做到问题早发现、原因准分析、措施能落实，全面提升电网安全稳定水平。

参考文献

[1]张恒伟,董淑海,张贝贝.电力系统及其自动化技术的安全控制研究[J].光源与照明,2024(1):216-218.

[2]钱叶牛,果然,张鹏程.电力系统及其自动化技术的安全控制问题和对策[J].2021.(4):57-60.

[3]杨松浩,李妍,赵晨.基于数字孪生和人工智能的电网网络安全主动防御体系研究[J].电力系统自动化,2023,47(18):132-142.

[4]王建,陈思远,刘洋.智能电网关键设备状态监测与故障预警技术综述[J].高电压技术,2022,48(9):3567-3580.

[5]国家能源局.电力监控系统安全防护规定:国能安全(2015)36号[S].北京:中国电力出版社,2015.

（本文编辑　杜宇琪）

