电力监控网络安全智能分析管控系统

郭珍奇，卢诗特
国网乌鲁木齐供电公司，新疆 乌鲁木齐 830000
DOI:10.61369/ETQM.2025060031

摘　　要： 提高系统运行稳定性和安全性。文章围绕电力监控网络安全智能分析管控系统进行论述，根据电力系统安全防护要求，首先阐述了电力监控网络安全内涵，其次分析了电力监控系统数据智能化分析体系不健全、平台功能相割裂、计算机病毒、自动化应急处置手段单一等问题，最后总结了一系列智能分析管控策略，建立完善的电力监控网络安全智能分析管控系统，全面提高电力监控系统安全防护水平。

关 键 词： 电力监控系统；网络安全；管控系统；智能分析

Intelligent Analysis and Control System for Power Monitoring Network Security

Guo Zhenqi, Lu Shite
State Grid Urumqi Power Supply Company, Urumqi, Xinjiang 830000

Abstract: Improve system operation stability and security. This article focuses on the intelligent analysis and control system for power monitoring network security. Based on the security protection requirements of the power system, it first elaborates on the connotation of power monitoring network security, and then analyzes the problems of the incomplete intelligent analysis system of power monitoring system data, the separation of platform functions, computer viruses, and the simplicity of automated emergency response methods. Finally, it summarizes a series of intelligent analysis and control strategies, establishes a perfect intelligent analysis and control system for power monitoring network security, and comprehensively improves the security protection level of the power monitoring system.

Keywords: power monitoring system; network security; control system; intelligent analysis

电力监控是保障电力系统稳定运行的关键环节，随着电力监控系统数据量增加，不断接入的各类智能终端，使得传统电力监控网络安全面临着严峻挑战，一旦系统出现漏洞，将导致大量重要信息泄露，诱发严重的网络安全事故。例如，2019年委内瑞拉电力系统受到网络攻击，造成了大面积的停电事故，严重威胁到国家安全。所以，保障电力监控网络安全至关重要，应坚持安全分区、网络专用等原则，建立智能分析管控系统，便于及时发现和解决安全威胁，为电力监控系统安全、稳定运行提供坚实保障。

一、电力监控网络安全的内涵

当前我国电力事业飞快发展，面对社会用电量激增带来的挑战，保障电力监控网络安全，对于保障电力生产和分配起到了重要作用。从信息安全角度来看，电力监控网络涉及到大量敏感信息，包含了用户用电数据、电网拓扑结构以及设备运行参数等信息，这些信息一旦泄露容易被不法分子利用，威胁电力系统运行安全和国家能源安全。例如，不法分子恶意盗取电网关键节点参数，推测电网的薄弱环节，从而为后续恶意攻击提供支持。所以，引入访问控制和数据加密等技术，有助于全面保障电力监控数据传输和存储安全，降低外部恶意攻击几率。

电力监控网络数据准确性和完整性，有助于为电力系统稳定、安全运行决策提供支持。如果电力数据被篡改，依据此类数据决策部署，可能会下达错误指令，导致设备误动，诱发大面积停电事故[1]。如，随意篡改电力设备保护定值，设备故障时无法正常动作，使得事故范围进一步扩大。所以，采用数据校验以及数字签名等先进技术，有助于保障电力数据传输和存储过程的完整性，为社会建设和发展提供坚实保障。

二、电力监控网络安全现状和问题

（一）现状

数字化、智能化时代背景下，保障电力监控网络安全，对于电力行业持续、稳定发展有着至关重要的作用。随着电力系统信

作者简介：郭珍奇（1993—），男，汉族，河南周口人，研究生，中级工程师现任职于国网乌鲁木齐供电公司，研究方向：电气及控制工程。

息化、智能化、自动化水平提升，不断有先进技术应用其中，形成了相较于完善的安全防护体系。如，网络边界布置 IDS/IPS、防火墙等设备，能够有效拦截外部攻击行为。数据安全方面，部分企业采用加密技术保护敏感数据，使得数据传输、存储和分析过程中的保密性得到保障[2]。一些大规模的电力企业创造性引入态势感知技术，实时监控电力监控网络安全状况，能够第一时间发现和解决安全隐患。

（二）问题

1.数据智能化分析体系不健全

现阶段电力监控网络安全面临诸多严峻挑战，尤其是多源异构数据的处理问题。PMU、SCADA等系统的数据标准不统一，导致不同系统之间数据无法正常的传输、共享，一定程度上增加了跨系统数据关联分析误差12% ~ 15%左右。传统电力监控网络系统的响应速度滞后，数据批量处理延迟达到了300ms以上，而《电力监控系统安全防护规定》要求系统实时响应达到200s，仍然存在很大的距离。加之配套及其学习模型对于 APT 攻击误报率较高，达到了35%以上，严重威胁电力监控网络安全[3]。

2.平台功能相割裂

电力监控网络安全平台多样，平台功能相割裂，协同运作效率不高。对于系统的安全功能模块，分散在不同平台中，如，楼栋管理平台负责扫描系统漏洞，入侵检测平台则负责监测网络流量以及攻击行为等，此类平台之间数据交互标准不统一，阻碍数据传输和共享，最终陷入到信息孤岛的困境。此种情况下，安全管理人员需要频繁切换不同的平台，消耗过多的精力浪费在不必要行为中，影响系统整体运行效率[4]。例如，某地区电网调度中心配备了7套独立安全系统，各系统平台之间的信息整合离不开人工手段支持，导致协同处置效率大大折扣。IEC 61850和 Modbus 协议转换过程中，可能丢失部分通信元数据；防火墙更新缓慢，同入侵检测系统之间存在协同延迟，大概8min ~ 15min左右，从而出现安全防护真空期。

3.计算机病毒

威胁电力监控网络安全的因素多样，其中计算机病毒问题最为典型。电力监控系统运行需要应用程序、操作系统、网络协议等提供支持，但由于系统和程序众多，不可避免地存在漏洞，一旦被病毒利用入侵，则会威胁到电力监控网络的运行安全[5]。实际上，电力监控网络的设备类型多样，有些设备更新速度缓慢，由于型号老旧，无法技术升级，为计算机病毒高度入侵埋下可趁之机。例如，蠕虫病毒经由电子邮件以及网络共享等途径传播，电力监控网络一旦感染将会导致大量设备瘫痪，造成众多数据丢失。情况严重下，病毒会下达误动指令，威胁电力监控网络系统运行安全，甚至造成大面积停电事故。另外，2023年某换流站事件的爆发，反映出超过40%的病毒是经由 USB 调试接口传播，防护边界延伸到物理隔离区。从中可以看出，计算机传播方式、攻击手段日趋复杂，并且更加隐蔽，传统网络安全检测手段无法有效应对，为电力监控网络安全带来了严峻挑战。

4.自动化应急处置手段单一

电力监控网络一旦出现突发事故，由于自动化应急处置手段较为单一，使得系统出现数据泄漏和网络攻击等突发情况时，无法自动化应急处置。由于处置方式过于单一，系统无法根据事件严重程度和影响范围等因素智能化分析处置。例如，系统遭受网络攻击时，一刀切的断开网络连接，使得某些核心业务无法正常展开，不利于电力监控系统安全、稳定运行[6]。实际上，电力监控网络系统响应速度缓慢，一旦出现突发事故，主站系统灾备切换消耗时间较长，大概45min ~ 60min，而《电力网络安全应急演练指南》规定30min以内，不符合标准，应急响应能力不足，可能会造成重大的经济损失。

三、电力监控网络安全智能分析管控的策略

（一）加强网络及电力二次安防设备加固

为了保障电力监控网络安全，应做好网络及电力二次安防设备加固处理，具体包括以下几点：①定期更新和升级软件，安装系统补丁，提高网络安全加固水平，降低运行成本。如，设置网络风险黑名单，设置最小权限开放 IP 地质与端口，安装升级补丁设备等[7]。②完善电力监控系统硬件设施，加大资金投入，结合电力系统运行情况完善配套安防设备和软件，有效抵御各类新型网络病毒攻击。电力系统网络中设置入侵防御系统，并配备专门的网络安全态势感知设备，定期更新升级病毒管理中心。③二次评估电力系统运行安全区，电力监控系统升级后，综合评价系统的监测和控制能力，结合系统网络安全运行预测系统是否需要迁移升级[8]。

（二）建立安全防护体系

为了保障电站运行安全，坚持因地制宜原则建立安全防护体系。依据实际情况落实安全防护责任制，编制网络安全应急预案，督促相关人员依据安全防护方案规范落实安全管理工作，一旦出现突发事件第一时间启动应急预案，将危害控制在合理范围内；加强电压等级纵向加密管理，基于远程管理技术建立纵向加密技术，保证电力监控系统始终在远程加密控制状态下稳定运行；建立35kV安全监测管理体系，遵循采集原则和统一管控原则，提升电站安全防护体系规范化水平。

（三）视频监控系统联动运作

在现有的电力监控网络安全智能分析管控体系中，加强视频监控系统联动运作，能够有效提高系统安全防护能力。建立统一的数据交互平台，提供标准化数据接口，能够兼容不同厂家和型号视频监控设备，实现电力监控数据统一传输和共享[9]。例如，遵循 MQTT 物联网数据传输协议，汇集电力设备运行与数据、视频流数据、安全预警数据源等，运用大数据技术进行分析处理，从而提取有价值信息，为后续系统联动决策提供可靠的数据支持。另外，采用人工智能算法，智能分析电力监控网络数据、视频监控图像，从而实现安全事件关联运作，提高安全事件应急处置效果。

四、电力监控网络安全智能分析管控系统设计

（一）总体框架设计

电力监控网络安全智能分析管控系统设计环节，应设计总体

框架，如图1。该系统框架自上而下分别是应用安全层、网址访问层以及运用安全层几个部分，能够极大地提高电力监控系统网络运行安全。网络路由器负责计算、传输和分析电力监控系统数据，并且通过有线或五险方式进行数据传输。应用安全层采用无源光纤网络传输数据，依托 TypeB 技术实现数据信息安全传输，最大程度上避免数据泄漏。电力监控系统采用交叉连接方式与其他业务和装置连接，联合运用 TypeB 技术和分光器，组成波长复用模式。基于此种安全保护方式，能够最大程度上实现网络数据存储、传输安全。而网址访问层有机整合虚拟局域网聚合技术，将电力监控信息和外部风险数据相隔离，并且在系统内部设立 FW 虚拟机，安全存储电力监控数据，提高数据信息处理能力。运营安全层采用改进 AC 算法，从电力监控系统中提取数据特征量，以 AC 算法加密数据格式传输和存储，最大程度上抵御外部攻击行为，全面提高数据信息安全性和完整性。

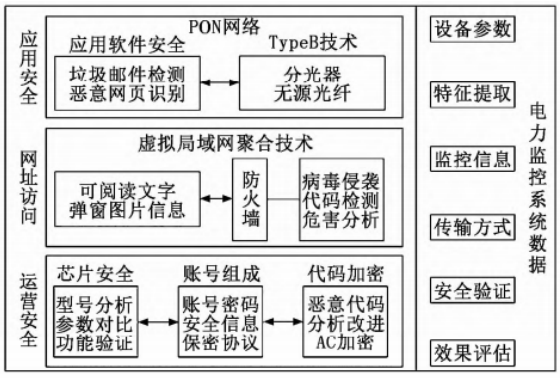

图1 电力监控网络安全智能分析管控系统框架

（二）硬件设计

系统硬件设计环节，根据要求配备网络路由处理器、分光器、无线通信模块以及存储器等部分。其中分光器构件配备了1×N端口，均匀分配光信号功率，控制工作波长在1269mm ~ 1650mm范围内，具有高隔离度以及低损耗等优势特点。网络路由处理器，采用RTL8196核心处理芯片，主频2.4GHz，数据传输速率最高为300Mb/s，保证电力监控数据实时传输、处理。存储器采用型号为 W25Q64 的存储器，该型号具有成本少、小型化的优势特点，在执行存储代码方面实现数据连续高速传输，传输速率大概64Mb/s，具有高灵敏、快速响应的特点。无线通信适配器，遵循 FCC-CE 标准采用型号为 RTL8192CE 的通信适配器，传输速率达到了150Mb/s。具体的连接电路如图2。

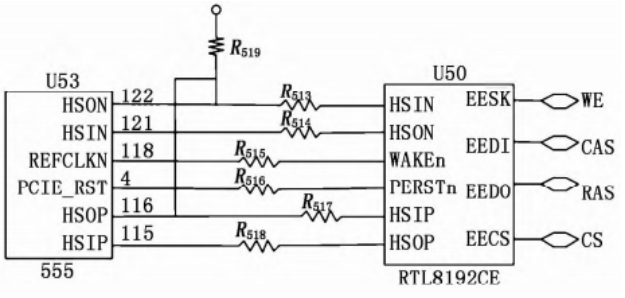

图2 无线适配器连接电路

（三）软件设计

电力监控网络安全智能分析管控系统设计中，软件设计是核心内容，微课实现电力监控数据信息安全传输，就可以采用 PON 网络 TypeB 防护技术实现[10]。而在数据库设计中，适合建立 MySQL 数据库，高效收集、存储和存储各类数据，具体涵盖安全日志数据表、安全等级数据表、实时运行数据表以及历史数据等。为了保证系统实时响应，系统间隔0.5s更新一次数据。

五、结论

综上所述，电力监控系统运行中产生的数据规模较大，建立电力监控网络安全智能分析管控系统，有助于实时监控电力系统运行状况，及时发现和解决系统异常数据，从而快速定位和应急处置安全威胁，保障电力监控系统网络安全，助推电力事业持续稳定发展。

参考文献

[1] 翁昊 . 基于网状关联分析的电力监控网络信息安全智能预警方法 [J]. 网络安全和信息化 ,2024,(09):46-48.

[2] 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,(06):132-133.

[3] 曹小明 , 张华兵 , 叶思斯 , 等 . 结合 ECC 算法的电力监控网络智能接入协议 [J]. 沈阳工业大学学报 ,2024,46(01):60-65.

[4] 虞明标 . 基于智能照明系统的电力网络安全监测与控制 [J]. 灯与照明 ,2023,47(04):63-66.

[5] 曹小明 , 张华兵 , 叶思斯 , 等 . 基于 ECC 算法的电力监控网络智能接入协议 [J]. 沈阳工业大学学报 ,1-7.

[6] 梅发茂 , 黎皓彬 , 黄浩 , 等 . 新能源涉网电力监控网络非法接入阻断技术 [J]. 电子设计工程 ,2023,31(09):177-180+185.

[7] 姜渭鹏 , 张鹏望 , 何兴谷 . 基于泛终端边缘计算的智能图像电力监控系统网络安全防护方式的采用和研究 [J]. 电力大数据 ,2023,26(04):82-89.

[8] 胡周达 , 隆运鸿 , 许丰 , 等 . 基于网状关联分析的电力监控网络信息安全智能预警方法 [J]. 现代电子技术 ,2023,46(03):69-74.

[9] 陈明亮 , 李鑫 , 谢国强 . 基于嵌入式技术的电力监控网络数据安全传输方法 [J]. 单片机与嵌入式系统应用 ,2022,22(06):33-37.

[10] 张亮 , 屈刚 , 李慧星 , 等 . 智能电网电力监控系统网络安全态势感知平台关键技术研究及应用 [J]. 上海交通大学学报 ,2021,55(S2):103-109.

