 DOI: https://doi.org/10.12345/dlynyqy.v3i7.30033

# Research on remote technical supervision of power monitoring system under multi-scenario

**Liang Zhang**

Tangshan Power Supply Company, State Grid Jibei Electric Power Co., Ltd. Hebei Tangshan 063000

**Abstract**

As China's power system rapidly evolves towards large-scale integration of new energy sources and multi-source fusion, the cybersecurity risks of power monitoring systems are increasing. Remote technical supervision, a critical tool for ensuring their safe operation, is being widely deployed and applied. Various grid-connected entities face diverse scenarios in the construction of their power monitoring systems, including complex system types, diverse access methods, and heterogeneous operating environments, which place higher demands on remote technical supervision. Therefore, researching the technical framework and implementation paths for remote technical supervision of power monitoring systems under various scenarios is crucial for enhancing the security protection level of grid-related systems and fulfilling the cybersecurity regulatory responsibilities of the power industry. This paper focuses on actual supervision needs, delves into the technical implementation framework and targeted measures, aiming to establish a remote supervision system that meets both industry standards and practical application requirements.

**Keywords**

multi-scene; power monitoring system; remote technology; supervision; method; research

# 基于多场景下电力监控系统远程技术监督的研究

张亮

国网冀北电力有限公司唐山供电公司，中国·河北 唐山 063000

**摘　要**

随着我国电力系统向大规模新能源并网和多源融合模式加速演进，电力监控系统的网络安全风险逐步加剧，远程技术监督作为保障其安全运行的重要手段，正被广泛部署与应用。各类并网主体在涉网部分电力监控系统建设中存在系统类型复杂、接入方式多样、运行环境异构等多样化场景，对远程技术监督提出更高要求。基于此，研究多场景下电力监控系统网络安全远程技术监督的技术体系和实施路径，成为提升涉网系统安全防护水平、落实电力行业网络安全监管职责的关键环节。本文围绕实际监督需求，深入分析技术实施框架及针对性措施，以构建符合行业标准与应用实际的远程监督体系。

**关键词**

多场景；电力监控系统；远程技术；监督；方法；研究

## 1 引言

电力系统作为能源互联网的典型，发电、输电、配电、用电等多个环节的协调控制均涉及电力调度生产服务相关数据，如监视采集的信号、实时量测的数据和控制变位的指令等。电力监控系统是联结数千万主厂站终端、实现实时和准实时通信的重要基础设施，近年来国家对其远程技术监管提出更为严格的技术与合规要求。有鉴于此，下文将结合相关文献查阅以及实践就基于多场景下电力监控系统远程技术监督的方法展开研究，以供参考。

【作者简介】张亮（1987–），男，中国河北滦州人，硕士，高级工程师，从事电力监控系统网络安全研究。

## 2 电力监控系统远程技术监督概述

电力监控系统远程技术监督指的是电力行业主管单位借助于技术方式在不直接进入被监督主体现场的前提下对电力监控系统网络安全状态开展持续不断地进行评估、识别和预警的一种技术监督方式。我国电力体系中并网主体复杂，涉及主网调度机构、发电企业、储能站等，它们涉网的部分电力监控系统主要为调度自动化系统、电力二次设备监控系统及相应的通信链路。由于这些系统多接入公网、专网混合通信体系，这就导致存在着大量的数据采集点分布广、边界不明确、接入频繁等问题，给系统的安全性构成威胁。当前，远程技术监督的能力主要表现为基于脱敏采样的行为监测、基于指令链的权限审计和基于时间序列的风险趋势分析。监督实施通常通过部署于监管中心的中立节点与被监督系统建立单向链路，在保证不会发生由下到上的数据逆向传

递情况下确保主体系统的独立安全运行 [1]。

## 3 基于多场景下电力监控系统远程技术监督必要性

当前我国电力系统中，风电、光伏、新型储能及综合能源服务主体日益增多，其涉网电力监控系统布局差异显著、运行规则不一，使得传统统一模式下的安全监管失效。多场景并存不仅带来接入模式与协议标准的多样化，还导致其网络边界动态变化、通信链路安全不可控、监控节点分布随机等问题频发。例如，风电场集中接入调度系统但分布广泛；光伏发电点小面广且通信依赖公网链路；新型储能系统则多与能管平台深度耦合，形成链式依赖关系。这些特征使得本地检查难以同步掌握其实时网络行为，容易导致攻击行为蔓延不可察觉。其次，当前并网主体众多但技术能力参差，部分中小型运营单位对网络安全管控意识不足，缺乏专业技术力量保障系统安全运行，形成“技术空窗区”，在没有远程技术监督覆盖的情况下，极易成为攻击链入侵路径。再者，部分地方监管机构因资源受限难以对全部并网点实施定期实地核查，远程技术监督为其提供了非侵入式、可持续的监督替代手段 [2]。结合我国电力系统多级调度结构，远程技术监督还可以实现区域层面向国家层面的一体化联动监督体系，有效压缩攻击可用窗口，提升发现、定位、处置网络安全事件的效率。因此，构建适配多场景的远程监督机制不仅是技术演进趋势，更是实现全覆盖监管闭环的现实需要。

## 4 基于多场景下电力监控系统远程技术监督的方法

### 4.1 火电涉网系统的远程技术监督

火电涉网系统远程技术监督方法，可以基于现有电力调控主站数据接入通道，建立多层级、多节点的指令一致性比对机制，其中主控层核心须将调度自动化系统和 DCS 闭环控制响应控制在毫秒级的对时窗口之内，对调节指令从母站到子站的传输路径、指令执行的响应时间和下达指令后的响应反馈这三大环节进行同步校核，以便尽早发现线路中存在的链路阻塞、指令重发、控制滞后的隐患；调度主站侧上，借助于高精度时间标签对比模块地部署，准确掌握负荷调节、启停指令与机组侧反馈之间的响应差异，从而判断控制链路中继设备是否存在故障、耦合点有无出现偏差等问题；在 DCS 系统内部，利用事件驱动识别算法，跟踪负荷调整、闭环调节及工况切换等关键动作节点状态变化，结合远程策略判别模型，对控制信号执行路径进行逐级映射验证。针对热控系统逻辑切换频繁的运行特点，远程监督平台需集成状态转移判定模型，并结合现场标准控制序列，建立指令链路跳转轨迹识别机制，从中解析逻辑旁路、跳级执行及未授权路径调用等异常操作行为。在执行层面，应按周期性采样策略，对关键测点控制输出、电气量采集记录、保护装置动作状态等进行采样一致性比对，采用分布式特征分析方法验证控制执行一致性、信号稳定性与保护触发的联动准确性，最终形成多场景覆盖、分层监督、闭环反馈的远程技术监督体系。

### 4.2 水电涉网系统的远程技术监督

针对水电涉网部分电力监控系统的远程技术监督，应基于其运行场景特点与系统结构，构建差异化、分层次的监督方法体系。在网络拓扑结构审查方面，应采用远程逻辑拓扑映射技术，精准识别调度数据网与厂站层设备间边界防护配置的合理性，重点核查厂站隔离装置配置是否满足“单向传输、物理隔离、协议过滤”三重控制要求；在访问控制策略检查方面，应通过配置文件远程抓取与策略匹配算法，对主机系统及网络设备访问控制列表（ACL）进行精细化比对，验证权限划分是否存在越权或冗余配置。在系统账号安全性审查方面，应实施基于时间窗口的集中登录日志采集与多维行为关联分析，对于是否存在问题账号共用或者账号长时间未修改口令的情况进行判断；对于水电企业常用的如 Modbus 等工业控制协议通信报文采用远程调用深度协议识别模块进行实时报文流审计，以检查数据报文是否完整，有无非法指令注入的风险；针对恶意代码防护功能，可采取发送指令，使终端防护策略回显，并与厂站服务器的白名单、防病毒策略和补丁更新日志进行对比，确保它们一致性；应急响应机制的审查主要是调取演练时录下的全部记录、联动日志和应急预案文档，并利用厂站运行日志进行事件响应过程的闭环执行验证 [3]。对于链路安全方面的检测，则使用加密隧道抓包回传以及根据某几个关键数据包的特点，对整个 VPN 通道加密程度、密钥更换周期、身份认证形式等项目指标做出评估，以保证电力监控系统远程通信过程的机密性及完整性。

### 4.3 风电涉网系统的远程技术监督

为实现风电涉网电力监控系统远程技术监督，需建立针对高跳数通信链路和多协议混用场景下的监督机制。考虑到风电场多处于通信资源匮乏地区，调度链路往往表现为多跳转发的特点，因此在风电监控主站侧，应结合 VPN，在监督中心侧与风电监控主站之间搭建加密虚拟隧道，实现控制链路与业务数据流之间的分离。基于链路层部署报文行为判别引擎，以链路层统计量信息为基准，对报文重传率、时延抖动程度以及跨周期数据同步偏移量进行检测分析，辅助识别判断链路不稳定以及边界不匹配的问题。在应用层使用识别探针集成多协议识别器，采用基于深度报文序列指令模式对比的方法，发现越权调度行为、非授权传输事件。针对 Modbus 协议与 IEC104 协议共存的风电场，需要建立基于协议语义的指令溯源模型，对调度指令关键字与目标对象行为的一致性进行回溯分析，发现伪造指令、参数操控的风险。此外，物理链路上部署冗余识别模块对链路切换日志、调度操作时序数据进行提炼，通过其相互之间关联性的对比分析，确认是否出现了链路漂移引导或者链路故意错位的现

象，一旦发现异常就应分别对该点生成所有的异常事件的全生命周期唯一标识，归集入区块结构中的远程证据链管理平台。最后，根据调度级次制定不同级别的监督检查规则，同时再依照风电场接入等级以及主站防护等级，规定报文的行为偏移阈值和协议访问指令的频度上限，组成分级控制及定向监督检查的关联管控方式。

### 4.4 光伏涉网系统的远程技术监督

光伏发电涉网电力监控系统开展远程技术监督工作应结合点多面广、接入方式多样、边缘设备存在众多不同的通信协议等特点，建立起高适配性的分层监督架构。结合远程技术手段，在现场端首先需要安装部署轻量级边缘链路数据采集模块，并通过协议镜像和指令触发方式进行监测，及时获取到 RTU、DTU 等边缘终端通信链路的报文上传周期、指令响应时延、心跳频率等关键参数信息；从通信行为特征入手建立动态的行为基准模型，设定相应的频次阈值和响应时延边界，实现指令滥发、通信中断及异常断点重连的精准识别。在公网链路接入场景中，引入动态 IP 跟踪机制，对通信链路中公网地址变动实施周期性探测与轨迹记录，结合地理位置反解析构建通信地理画像，并通过多周期行为演化图谱实现异常路径可视化展示 [4]。考虑光伏项目中通用 RTU 使用率高的设备构成特征，需配置指令频度矩阵模型，对定值修改、远程合分闸、遥控软启等高敏感操作形成命令热力图，识别疑似注入型控制操作。在固件层面，采用远程固件指纹比对策略，建立与可信基线库一致性校验流程，周期性核验接入终端固件签名，识别固件替换、篡改等异常行为。所有监督数据通过状态量转移路径模型进行关键指标偏移路径分析，实时输出策略变更提示，以支撑调控端快速响应链路异常及设备安全态势。

### 4.5 新型储能主体涉网系统的远程技术监督

对于开展新型储能主体涉网电力监控系统的远程技术监督来说，可围绕控制链路完整性和行为合规性实施，以建立多维协同监督模型。针对控制链路追踪上，采用基于 EMS 到储能控制器间指令转发链，设定“指令发起源标识符 - 控制单元响应报文”的映射关系及网络时间戳、业务号的方式实现路径一致性校验；针对高频调节环节，基于网络级 HTKP 控制指令与反馈报文采用滑动时间窗机制实时比较高频调节环节的功率调节指令与对应的实时反馈响应的一致性；针对通信报文可信性审查上，应通过建立跨节点数字签名一致性验证机制，对控制指令及响应报文在各级主控与子控节点间的签名转移过程进行全链条溯源比对，防范篡改、中间人攻击及签名缺失风险 [5]。针对储能系统多接口、多协议运行特点，需引入协议调用行为建模机制，按 Modbus、IEC61850、DNP3 等典型通信协议分别构建调用频率—参数组合—响应码三元行为谱系模型，实施远程调用路径行为分析，及时甄别接口探测、参数越权等异常特征。为防控主控平台的进程级风险，还应部署远程可疑进程监听机制，基于系统层审计日志实时检测未备案进程运行事件，并结合指纹特征归档模块锁定其行为特征，防止非法可执行文件形成横向控制链路。所有监督事件与日志结果应通过非对称加密机制完成远程加密归档，并按主体、链路、时间维度构建可溯事件索引，实现监督过程的闭环管理与取证支持。

## 5 结语

综上所述，面对电力系统多类型并网主体不断扩展的现实格局，构建适应不同场景、不同系统结构的远程技术监督体系已成为保障电力监控系统网络安全的核心任务。本文结合我国电力系统运行现状，系统性分析了多类并网主体在实际涉网系统中的关键技术特征与安全风险，提出了针对性远程监督方法路径。后续，需在技术标准统一性、数据共享机制规范化及智能化监督能力建设方面持续推进，实现监管技术与业务实际的深度融合，切实提升电力系统整体网络安全韧性。

## 参考文献

[1] 冯陈佳,朱江,朱寅,等.电力监控网安设备策略统一管理体系及其实践[J].信息安全研究, 2024, 10(5):481-488.

[2] 汤乐平.基于5G通信技术的电力智能监控与管理平台构建[J].江苏通信, 2024, 40(4):8-12.

[3] 朱江,冯陈佳,杨采薇,等.电力监控系统网络安全策略统一描述方法[C]//第39次全国计算机安全学术交流会论文集.2024.

[4] 王超.基于物联网技术的电力设备远程监控与管理系统探讨[J].中国设备工程, 2024(24):207-209.