新能源场站电力监控系统网络安全管理策略与机制研究

文◆内蒙古上都发电有限责任公司　耿晓伟

引言

随着新能源占比快速提升，电力监控系统面临日益复杂的网络安全挑战。传统防护体系难以应对 APT 攻击、内部人员违规操作以及硬件供应链风险交织的复合型威胁。本文聚焦新能源场站监控系统特性，通过剖析典型攻击路径与脆弱环节，构建“技术防护 + 管理机制”双轮驱动的安全架构。研究目标在于形成覆盖全生命周期的安全管理范式，提升对恶意代码、数据篡改、设备失控等典型场景的防御韧性，为能源行业数字化转型提供可量化的安全保障方案。

1 系统安全风险分析

1.1 外部网络攻击威胁分析

网络攻击者通过系统存在的安全漏洞或使用简单密码作为突破口，对电力监控系统实施非法入侵。此类攻击行为会导致监控画面被篡改、设备控制指令遭劫持、恶意程序被植入系统核心模块等问题，进而引发发电单元异常运行甚至整体停电事故。境外情报机构以能源数据为目标，通过长期网络侦察手段窃取发电设备技术参数、电网调度策略等核心信息，直接威胁国家能源战略安全。

1.2 内部人员操作风险剖析

运维人员因专业技能不足或操作疏忽，引发系统配置错误、关键数据丢失等操作事故。特别是在执行设备隔离、参数整定等高风险操作时，细微失误都会造成保护装置误动或监控数据失真。更需警惕的是，部分内部人员基于利益驱使，故意破坏系统防护机制、违规外传敏感数据，这种主观恶意行为具有极强的隐蔽性和破坏性。

1.3 硬件设备安全隐患梳理

服务器、测控终端等关键设备因元器件老化或极端环境影响出现性能衰退的问题，导致数据采集异常或通信中断。更值得关注的是，设备全生命周期各环节均存在安全风险，如生产环节被植入恶意芯片、物流环节遭遇固件篡改、部署环节遗留后门程序等，这些隐患在设备投运前就已埋下安全定时炸弹 [1]。

2 安全防护策略

2.1 网络边界防护方案

在电力监控系统与外部网络的交界区域部署专业级工业防火墙，根据业务类型建立精细化访问控制规则集。通过持续更新威胁特征库，确保能够有效拦截非常规端口扫描、恶意代码传播等攻击行为。配套部署入侵检测与防御系统，该系统可实时分析网络流量，识别异常数据包特征，及时触发告警并执行自动阻断操作。针对远程运维需求，采用 IPSec VPN 技术构建加密传输隧道，确保跨网段数据交互的机密性和完整性。

2.2 数据安全保障机制

建立多层次数据保护体系，对关键业务数据实施 AES–256 加密存储，配合 RSA 非对称加密算法实现密钥安全交换。制定“3—2—1”数据备份策略，即至少保留 3 个备份版本，采用 2 种不同存储介质，其中 1 份存储至异地灾备中心。构建基于角色的精细化权限管理系统，将用户划分为系统管理员、运行值班员、设备维护员等角色，通过属性证书实现最小权限分配，确保数据访问操作全程留痕可追溯。

【作者简介】耿晓伟（1993—），男，内蒙古锡林浩特人，本科，助理工程师，研究方向：通信、自动化。

2.3 工控系统防护措施

开展工控设备安全基线加固，强制实施 12 位以上复杂密码策略，关闭闲置网络端口和服务，建立固件完整性校验机制。对 Modbus TCP、DNP3 等工控协议实施深度包检测，通过数字证书认证通信实体身份，采用 HMAC–SHA256 算法保障协议数据完整性。实施网络纵深防御，将监控系统划分为生产控制大区、管理信息大区等安全域，各区域间部署工业防火墙和单向隔离装置，建立“安全接入区”作为内外网数据交换的唯一通道 [2]。

3 防护管理机制

3.1 主动防御机制

3.1.1 漏洞全生命周期管理机制

电力监控系统运营单位应建立规范化的安全漏洞管理流程，通过部署自动化漏洞扫描工具定期执行全系统安全检测。检测范围需覆盖操作系统、数据库、应用软件以及网络设备等核心组件，重点排查未授权访问、弱口令、配置缺陷等典型漏洞。技术人员需依据 CVSS 评分体系对漏洞危害等级进行量化评估，针对高危漏洞建立 48 小时应急响应机制，中低危漏洞实施月度整改计划。整改完成后，必须通过回归测试验证修复效果，并建立漏洞修复档案库，实现从发现到闭环的全流程追踪管理。

3.1.2 威胁情报驱动防御策略

网络安全团队应构建多源威胁情报收集网络，通过订阅行业权威威胁情报平台、加入能源行业信息共享联盟等方式，实时获取 APT 攻击组织动向、工业控制系统专用恶意软件样本、零日漏洞利用代码等关键信息。依托安全大数据分析平台，建立威胁情报关联分析模型，对攻击者 TTPs（战术、技术、程序）进行画像构建。根据情报研判结果，动态调整防火墙策略规则，更新入侵检测系统特征库，在关键网络节点部署蜜罐系统诱捕攻击行为，形成预测性防御能力。

3.1.3 安全配置基线强化工程

应参照等保 2.0 以及电力行业特殊安全要求，制定覆盖主机终端、网络设备、安全设备的配置基线标准，具体包括禁用不必要的网络服务端口、实施最小化权限分配原则、强化日志审计功能配置、规范加密算法使用策略等。通过部署基线配置核查工具，每月开展全系统合规性检查，对偏离基线的配置项生成整改工单，要求责任部门在规定时限内完成修正，确保系统始终处于安全基准状态。

3.2 应急响应机制

3.2.1 预案体系化设计方法

需结合电力监控系统业务特性，构建“1+N”应急预案体系。其中“1”为总体应急预案，明确应急组织架构、响应分级标准、处置流程框架；“N”为专项处置方案，涵盖勒索软件攻击、数据篡改、设备失控等典型场景。预案需细化到具体岗位操作手册，明确各岗位在事件处置中的职责边界、决策权限、操作步骤，并通过沙盘推演验证预案可操作性。

3.2.2 实战化演练实施规范

每半年组织全员参与的应急演练活动，演练场景应包含但不限于 DDoS 攻击导致监控系统瘫痪、恶意代码感染工程师站、虚假数据注入引发调度误判等。演练过程采用“双盲”模式，不预先通知演练时间与攻击向量，重点检验值班人员应急响应速度、部门间协同效率、备用系统切换能力。演练结束后必须召开复盘会议，运用鱼骨图分析法梳理处置环节存在的问题，针对性完善预案内容。

3.2.3 事件处置闭环管理

当发生网络安全事件时，值班人员应立即启动应急预案，按照“识别—隔离—取证—恢复—复盘”五步法开展处置。需使用网络隔离装置快速切断受影响系统与生产控制大区的连接，通过全流量分析设备捕获攻击流量，利用数字取证技术固定电子证据。事件平息后，需在 72 小时内提交完整的事件分析报告，从攻击路径、漏洞利用、影响范围等多个维度进行技术复盘，并将处置经验转化为防御能力提升项。

3.3 认证管理机制

3.3.1 多因子身份鉴别机制

建立覆盖人员、设备、应用的立体化认证体系。人员认证采用动态口令令牌与生物特征识别相结合的方式，关键操作岗位部署“人脸识别 + 行为特征”分析系统。设备认证通过数字证书体系实现，为每台接入设备颁发唯一身份凭证，在接入层部署 802.1X 认证网关。应用系统访问实施基于角色的权限控制（RBAC），重要操作需经过双因素认证以及审批流程。

3.3.2 设备准入控制方案

在网络边界部署下一代防火墙（NGFW），启用设备指纹识别功能，建立合法设备特征库。当新设备接入时，系统自动采集 MAC 地址、操作系统版本、安装软件

列表等特征信息，与特征库进行比对验证。对于未注册设备，强制跳转至隔离区进行安全检查，通过病毒查杀、漏洞修复后方可接入生产网络。

3.3.3 操作行为审计系统

构建基于大数据的行为分析平台，实时采集用户操作日志、系统事件日志、网络流量日志。通过用户实体行为分析（UEBA）技术，建立正常行为基线模型，对异常登录时段、特权账号滥用、数据批量导出等风险行为实时告警。关键操作实施二次授权机制，如保护定值修改、遥控指令下发等操作，需经过值班长电子签批方可执行，所有操作记录保存时间不少于 18 个月 [3]。

4 实践与应用

4.1 策略与机制实施过程

4.1.1 纵深防御部署

在互联网出口部署工业级下一代防火墙，配置基于业务特征的访问控制策略，拦截非法访问流量。同步部署全流量检测设备，运用机器学习算法建立正常通信基线，实现异常行为自动识别。针对远程运维需求，构建双因素认证的 VPN 通道，采用国密 SM4 算法保障数据传输安全。

4.1.2 数据全生命周期保护

建立“AES-256+SM2”混合加密体系，对风机功率曲线、变桨系统参数等核心数据实施加密存储。部署分布式存储架构，在本地和千里外灾备中心同步执行每日全备、每小时增量备份。开发基于角色的权限管理系统，精准映射 8 类用户角色与数据操作权限，通过操作日志审计实现行为全追溯。

4.1.3 工控系统专项加固

对 PLC 控制器实施安全基线配置，强制启用白名单机制，关闭未使用的 135、445 等高危端口。联合设备厂商完成 Modbus TCP 协议深度加固，增加双向认证和报文校验机制。将生产网划分为风机控制区、升压站监控区、管理信息区 3 个安全域，通过工业防火墙实现区域间逻辑隔离。

4.2 实施效果评估

4.2.1 主动防御机制

建立周期性漏洞管理流程，运用自动化工具每周开展全网扫描，发现的 127 个漏洞均在 72 小时内完成修复。接入电力行业威胁情报中心，实时更新入侵检测规则库。制定 238 项安全配置基线，每月通过合规检查工具验证系统状态。

4.2.2 应急响应体系

编制涵盖 17 类场景的应急预案，组建跨部门应急小组，每季度开展攻防对抗演练。2023 年三季度演练中，成功在 28 分钟内完成勒索病毒事件处置。配置热备冗余系统，确保核心业务 7×24 小时连续运行。

4.2.3 统一认证平台

部署数字证书认证系统，实现人员、设备双因子认证。开发设备准入控制系统，对接入终端执行合规性检查，阻止 12 台非授权设备联网。建立操作行为分析中心，通过 UEBA 技术识别异常操作模式，拦截高危指令 23 次。

结语

本文提出的新能源场站电力监控系统安全防护体系，通过实战化演练验证了其技术可行性与管理有效性。案例实施表明，基于威胁情报驱动的动态防御机制可使高危漏洞存活时间降低 92%，双因子认证体系阻断非授权访问成功率达 100%。未来需持续关注量子计算对加密体系的冲击及 AI 攻击技术的演进，通过构建自适应安全大脑实现从“被动防御”到“主动免疫”的跨越，为新型电力系统安全稳定运行奠定基石。

引用

[1] 雷亮,谭小瑶,刘漫,等.新能源场站电力监控系统网络安全薄弱环节分析[J].信息记录材料,2022,23(9):198-200.

[2] 吴勤勤,周安,付佳佳,等.新能源电厂电力监控系统网络安全防护[J].数字技术与应用,2022,40(5):222-224.

[3] 刘博,李梁,刘军娜,等.新能源场站电力监控系统网络安全薄弱环节分析[J].电工技术,2021(18):78-80.