风力发电

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS

随着“碳达峰、碳中和”战略推进，风电作为技术成熟的清洁发电方式，装机容量快速增长，已成为继火电、水电后的第三大主力电源，被认为是最具商业潜力、最具活力的可再生清洁能源之一。风电企业网络安全建设，必须依据能源局《电力监控系统安全防护总体方案》、等保2.0标准，充分考虑风电场分布地域广、管理难度大特点，兼顾合规和实际情况，打造风电企业网络安全防护体系。

解决方案 SOLUTION

网络边界隔离防护：在站控层、风机远控与风场非控制区的边界，集控中心控制区与非控制区的边界，部署工业防火墙，实现逻辑隔离，对工业协议进行白名单防护。

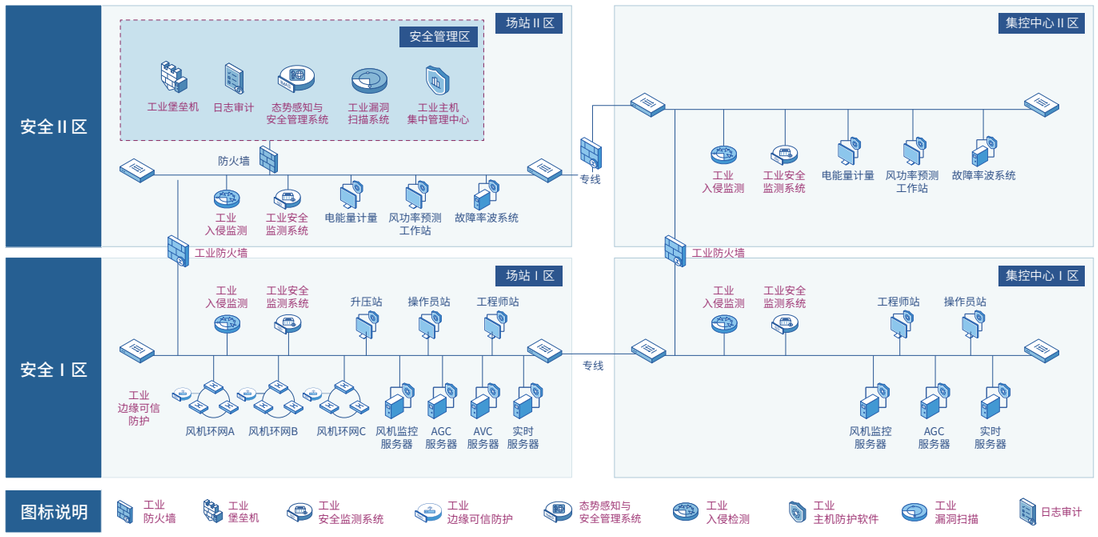
监控系统流量审计：在站控层、风机远控、集控控制区、场站和集控非控制区，旁路部署工业监测审计系统准确监测控制网络异常流量，深入解析并识别非法内联、非法外联、非法接入、网络攻击等异常行为，实时审计并在第一时间告警。

风机环网准入控制：在风机环网在内，部署工业准入设备，基于工业协议库、工控资产库，通过流量识别资产，形成资产白名单，通过网络发包，阻止未授权接入资产；前端合规评估，分析PLC、HMI是否开启了不必要的端口、是否被其他设备仿冒替换；前端行为分析，分析是否有异常控制行为、分析是否跨系统读取或传参行为。

非控制区入侵检测：在安全II区，旁路部署工业入侵检测设备，在生产控制大区网络入口，实现入侵行为检测、网络病毒检测；在场站非控制区与集控非控制区边界，部署具有入侵防御功能的工业防火墙，实现攻击防御。

工业主机安全加固：在生产控制大区内部操作站、实时服务器、监控主机等设备上部署工业主机防护软件，通过应用白名单、外设管控、病毒防御、访问控制、主机加固等技术，防止病毒、木马对主机的感染，保障各系统内工业主机安全。

控制大区集中运营：建立安全管理中心，部署工业态势感知系统，收集安全数据，基于关联分析引擎、异常行为分析模型，从资产、漏洞、工控行为、威胁等维度，展现全局网络安全态势；部署工业日志审计系统，实现网内各类系统的日志、事件、告警集中存储与审计；部署工业堡垒机，提供统一身份认证接口，对资产及账号等进行集中化运维管控。



成功案例 SUCCESSFUL CASE

- 国电奈曼风电有限公司
- 华能新能源股份有限公司
- 江西丰城风电厂
- 湖南金觉峰风电

电力调度

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS

电力调度中心，是电力系统信息处理、监视和控制的中心机构；其根据电力系统当前运行状况和预计的变化进行判断、决策和指挥，是电力系统的关键部门。调度中心的网络安全建设在能源局“安全分区、网络专用，横向隔离、纵向认证”总体原则基础上，结合等级保护相关要求，已经建成了相对完善的安全体系，逐渐实现了“实时管控、纵深防御”的目标；为了进一步实现对业务行为的监测，提升电网动态行为的全局监测与分析能力，应持续推进安全与业务的深度融合，建设电力监控系统安全态势感知体系。

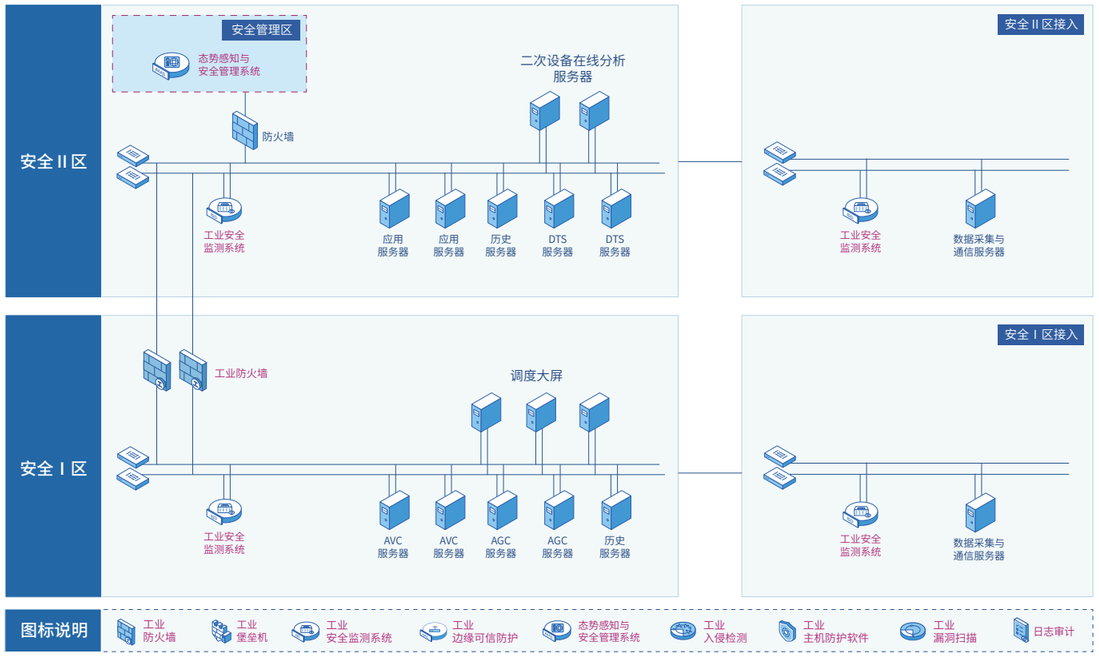
解决方案 SOLUTION

集中管理：基于生产控制大区流量，建立以资产管理为中心的设备集中管理和监控，实现资产业务分组、资产多维度属性、资产分类、资产活跃度等多维度管理；根据电力调度场景，结合业务结构，绘制具有业务术语的拓扑图，动态展示资产连接关系、资产状态等。

威胁分析：态势感知以资产为核心，以流量和安全日志为基础，构建资产风险量化，资产风险指数、风险等级、失陷状态、非法接入状态、漏洞数量、威胁告警、异常行为告警等多维度风险管理体系；对电力监控设备进行的脆弱性监测，包括设备所对应的漏洞信息、开放的端口和不安全的协议等，通过联动威胁情报，对本地数据进行关联分析，及时告警并通知安全管理员。

调度行为分析：调度行为分析是针对调度场景采用的大数据行为建模分析方法，基于智能分析引擎、调度协议深度解析能力，实现异常资产分析、异常网络行为分析、异常调度操作行为分析等，重点监测“三遥”信号，最终从安全角度监测业务合法性，将调度控制模型与安全相结合，构建调度控制安全分析模型。

调度态势感知：在资产管理、风险分析、威胁分析、调度业务行为分析能力基础上，建立态势感知，分析预测安全趋势。通过对资产态势、风险态势、漏洞态势、威胁态势、调度行为态势等分析与预测，并深度融合调度业务场景，全面提供内生的工业安全态势。



成功案例 SUCCESSFUL CASE

- 国网新疆调度控制中心