圣博润
SBR-info

电力行业

工控安全解决方案

股票代码:430046

方案背景

进入新世纪，我国电力监控系统安全防护工作经历了一个艰辛探索、不断完善的过程，短短十几年间，实现由弱到强、由单一安全逐渐向全方位安全过渡，最终形成了一个相对完善的安全防护体系。

但同时可以看到网络攻击事件正在向有国家背景的、有组织的、长期潜伏的、定制化设计的、大规模的、针对基础设施的方向发展，信息系统安全已经进入了全球网络战时代。

新形势下，电力企业应在《电力监控系统安全防护总体方案》（国能安全【2015】36号）的基础上，根据《工业互联网安全防护工作指南》、《工业互联网安全防护检测指南》从设备安全、控制安全、网络安全、应用安全、数据安全、物理和环境安全、安全策略和管理制度等多个方面落实工业控制系统网络安全防护、检测、预警和应急处置等工作。

总体策略

安全分区 | **网络专用** | **横向隔离** | **纵向认证**

综合防护

保护	检测	响应	恢复	审计
◎ 工控防火墙 ◎ 工控隔离网闸 ◎ 工控主机防护系统（白名单）	◎ 工控监测与审计系统 ◎ 入侵检测系统 ◎ 网络准入控制系统	◎ 集中管理平台 ◎ 应急处置工具箱 ◎ 网络安全态势感知平台	◎ 数据备份与恢复 ◎ 主机监控与恢复	◎ 内控管理平台（堡垒机） ◎ 日志审计系统

防护重点

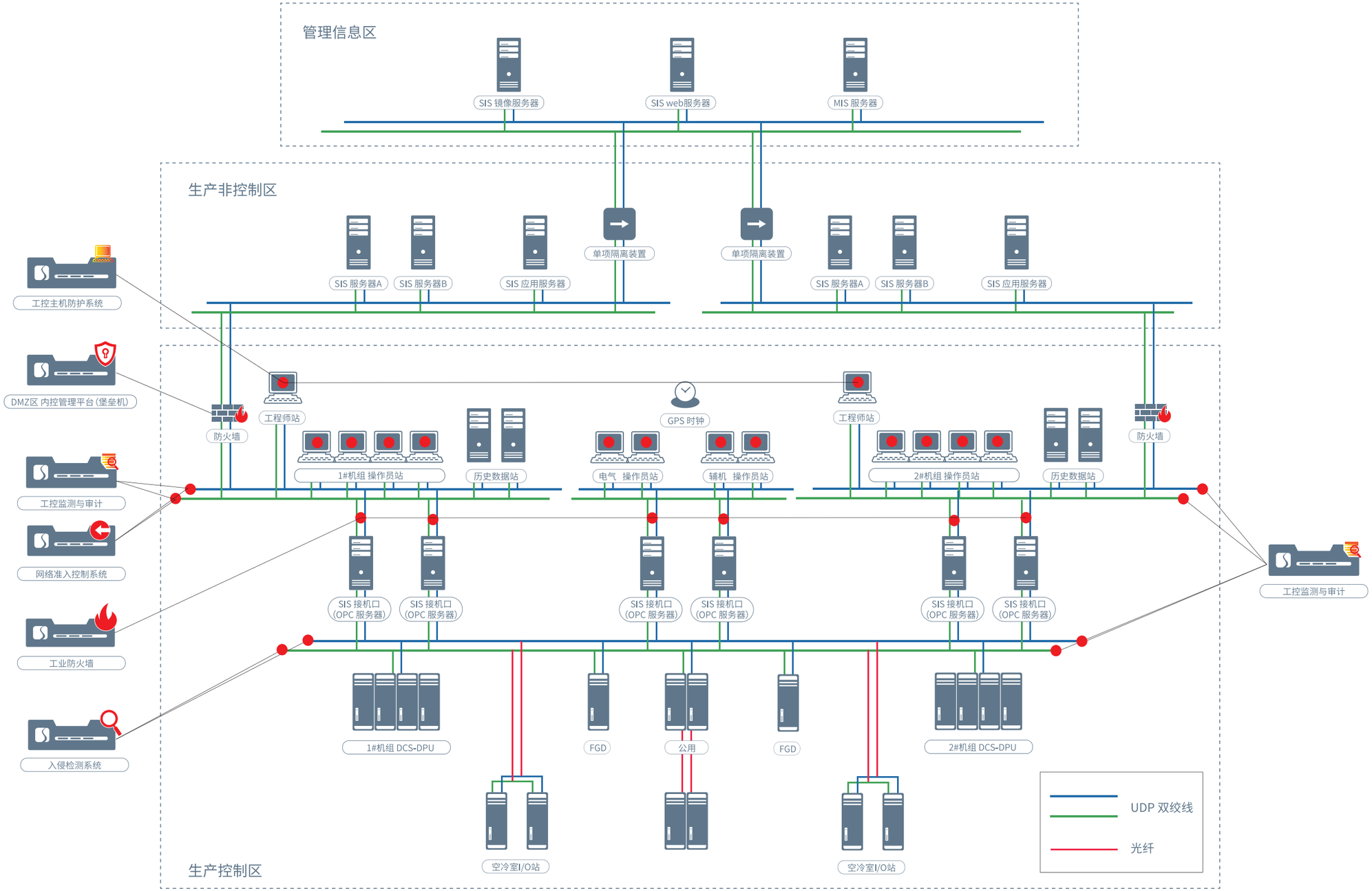
- **病毒和恶意代码防范**
  工业主机应安装应用程序白名单软件或防病毒软件；采取技术措施对工控网络临时接入设备进行准入控制及病毒查杀。

- **网络异常监测**
  应在工业控制网络部署网络安全监测设备，提供协议审计、流量审计、事件分析和异常告警。

- **OPC服务器宜独立设置防护**
  DCS、PLC、SCADA等控制系统在通过OPC服务器与MIS和SIS系统相连接时，应部署工业防火墙或工控隔离网闸进行防护。

- **设备外接端口管控**
  拆除或封闭工业主机上不必要的USB、光驱、无线等接口；如确需使用，必须通过主机外设安全管理技术手段实施严格访问控制。

方案部署



电厂工业控制系统信息安全防护架构图

边界防护

控制区与非控制区之间部署防火墙、进行逻辑隔离。逻辑隔离设施应具备状态检测、数据过滤和地址转换等基本功能，可以对传输的地址、协议、端口和数据流的方向进行控制。
生产控制区内部以火电发电机组为单位，部署工业防火墙，对主控和辅控系统进行分区防护，设置最小安全防护区，减少暴露面，降低攻击风险。

网络监测与审计

在现场监控层的汇聚交换机处部署工控监测与审计系统。进行威胁感知及事件监测，发现工控网络中的异常行为和攻击入侵行为。加强工控网络流量监测与分析能力，有效提升事件发现、应急处置和溯源能力。

工业主机防护

部署工控主机防护系统，采用白名单机制，对工控上位机上的数据采集软件、组态软件、过程监督与控制软件、单元监控软件、过程优化软件等进行白名单管理，只允许受信任的符合管理规定的软件安装和执行，阻止未经授权使用的软件进行安装和执行，以达到恶意代码防御的目的。

运维管理

《电力监控系统安全防护技术规范》要求电力监控系统应采用堡垒机进行安全运维，利用工控堡垒机来对用户身份进行认证授权，确保控制系统执行的控制命令来自合法用户，并对用户权限进行划分，避免任意用户可以执行任意功能。

集中监控

在集控中心后台部署统一安全管理平台，对监管范围内的防火墙、正反向隔离装置、纵向加密装置、入侵检测装置等安全设备的安全策略、日志进行集中收集与关联分析，结合漏洞扫描、防病毒系统对全网的整体安全情况进行综合审计。

抱圣贤之思

怀博学之志

尽润泽之力

北京圣博润高新技术股份有限公司

地址：北京市海淀区高梁桥斜街59号院2号楼3层

电话：(010) 8213-8088 / 技术支持热线：800-810-2332、400-966-2332

网址：www.sbr-info.com

圣博润 SBR-info