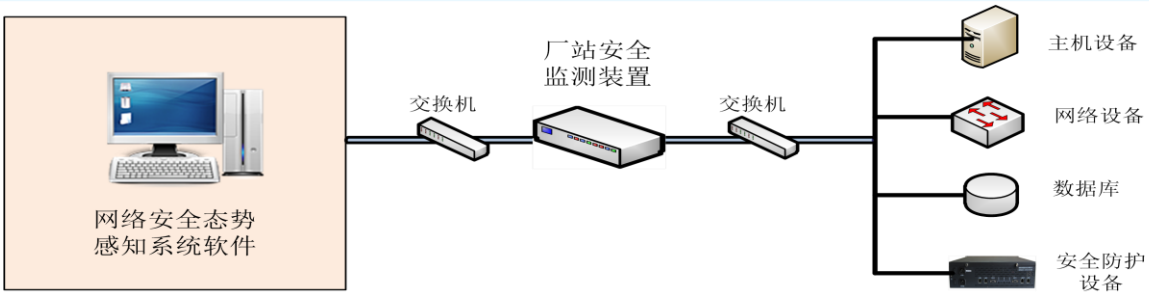
HR NSSA-3000

网络安全态势感知系统(电厂本地版)

✳感知对象数据采集
✳数据提取融合评估
✳安全趋势预测分析
✳实时监控综合审计
✳网络安全本地管理



变电站/发电厂本地网络安全态势感知系统，评估站端网络安全状态精准预测安全趋势，实现集约化厂站网络安全管理。

系统概述

系统提供包括平台软件、厂站安全监测装置的站端网络安全解决方案。紧密围绕数据采集、数据融合评估及预测、可视化展示，对站端网络安全状态做出判断及预测安全趋势，通过图形、分析报告、网络态势图等形式给出网络安全态势，达到对站端网安全状态的可测、可知、可防可控。

系统结构

系统采用分布采集、集中管理模式。在厂站间隔层的安全监测装置直接采集站控层、间隔层各监测设备运行状态及进行预处理，通过以太网与站控层平台软件通信，平台软件进行采集，分析以及可视化监视，通过图形、表格、态势图、攻击 TOP 图等形式给出网络的当前状态及预测安全趋势。

感知对象

分类	内容
主机设备	登录成功/退出/失败、操作命令、操作回显、USB 插入/拔出、串并口占用/释放、光驱挂载/卸载、网络外联、开放非法端口、网口 up/down、关键文件变更、用户权限变更
网络设备	配置变更、网口状态、网口 up/down、流量超过阈值、登录成功、退出登录、登录失败、修改密码、操作信息、MAC 地址绑定关系
安防设备	登录成功/退出/失败、修改策略、CPU / 内存利用率、电源故障、风扇故障、温度异常、网口状态异常/恢复、异常访问、攻击告警
数据库	数据库状态、磁盘信息、数据库空间使用情况、链路状况、操作记录、登录记录等
网络	全局风险评估、安全趋势分析

主机设备：包括站用服务器、工作站。

网络设备：包括路由器、交换机。

安防设备：包括纵向加密认证装置、正反向隔离装置、硬件防火墙设备。

数据库：包括 SQLSERVER、ORACLE、MYSQL。

主要功能

采集处理：对服务器、工作站，数据库，交换机、路由器，纵向加密装置、正反向隔离装置等进行综合分析。支持策略处理、归并处理及格式化处理并组织为包含但不限于外设接入、用户登录、危险操作、状态异常等新的事件，形成智能告警，为评估及预测提供数据基础

评估预测：依据采集处理数据，采用数学模型、知识推理等方法，进行全局网络安全实时状态评估。根据对单个入侵攻击事件的预测，结合每种攻击的威胁程度，计算相应的后一个时刻或则多个时刻的态势值。

安全审计：对外设接入、主机登录、网络通信的行为审计；统计报警 TOP10；统计分析基于时间维度的端口使用、登录行为、用户权限密码变更。统计方式可按照设备、用户分类进行。

设备台账管理：支持对监视设备的资产台帐管理及建模功能，主要包括自动发现设备信息，编辑、导出设备台账及查询维护。

可视化管理：网络的当前状态、设备状态、安全趋势等通过多视图、多角度、多尺度的图形图像方式展示给用户并且与用户进行交互。主要包这括图表、曲线、多维数据、实时报警推送、 TOP10 柱状图，以及各类查询分析等。

主站健康评价：按照电力系统自动化设备管理要求，结合专家知识库，提供站端设备的健康评价管理、监视及状态检修预警功能，及时发现二次系统运行过程中的安全隐患、主机运行负载过高、网络流量异常等问题，为用户及时进行检修处理提供决策依据。

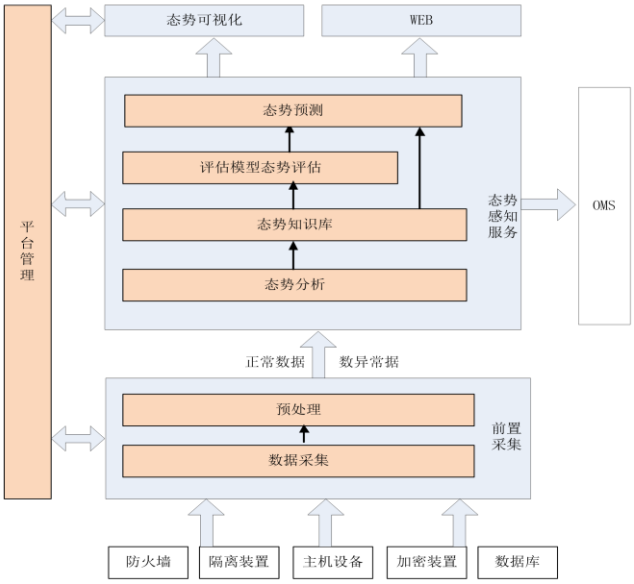
用户管理：具有责任区、角色的划分及权限管理用户登录后根据权限访问相应功能模块，支持限制同一种角色的人员的同时在线个数。具有密钥管理机制，所有用户信息在储存和传输过程进行软件加密；以日志的方式记录登录用户的所有操作信息。

告警管理：以列表方式显示详细的实时告警信息，以不同颜色表示告警级别重要性，不同权限人员只看到自己职责范围内的告警信息。支持告警条件过滤。智能告警监测到的所有事件应形成告警记录，并按照预先设置的告警策略通知运维人员处理。提供告警的查询及统计。

数据转发：具有向上级管理系统汇总转发本地管辖范围的所有态势感知数据的功能。

WEB 发布：系统支持 Web 发布，可通过互联网进行远程监测。Web 发布与平台软件的展现方式、数据完全保持一致。

软件结构



平台软件采用分层分布式结构、面向对象设计，程序间通信采用总线模式。系统按照一定的层次功能分为采集、服务处理、平台管理、可视化等程序模块。每个程序模块独立完成相应的功能，程序间通过系统总线进行数据交互。使得整个平台软件具有高可靠性、高内聚低耦合、可扩展性、强稳定性的特点。

平台软件主要程序包括前置机程序、实时服务处理程序、工作站程序、系统模型编辑器、图形编辑器、数据库维护软件、Web 服务等。

技术特点

标准化模型：系统模型遵循 IEC 61970 标准。建立符合电力系统规范的 CIM 模型，实现和其它系统的信息共享及交互，避免“信息孤岛”。

时钟同步：支持接收变电站 B 码/SNTP 时钟同步信号并具备守时功能。

身份认证：站端安全监测装置与平台软件采用国密算法在应用数据传输之前进行双向身份认证。

标准化图形：可视化图形基于电力 SVG 标准。

多种通信标准：站端安全监测装置与平台软件之间支持 GB/T 31992，DL/T 860 MMS，DL/T 634.5104、GOOSE 等多种标准进行数据通信。

多种采集协议：支持 SNMP、SNMP TRAP、SYSLOG、GB/T 31992、服务器监测协议、SSH、TELNET、PING 等多种采集方式对监测对象进行采集。

分级管理：安全监测装置具有独立的厂站级的分析展现功能。

采集负载均衡：系统可采用多前置负载均衡的数据采集网的方式对各网络设备进行数据采集。可按照均衡算法自动分配前置的采集负荷，保证系统采集效率。

多部署方式：系统单机单网双机双网模式可配。

性能指标

- 支持用户个数>= 256 个；
- 支持厂站装置数>=256 个；
- 系统处理点数百万级；
- 采集信息吞吐量 ≥10000 条/s；
- 监管对象数量 ≥200；
- 采集/分析信息保存周期 ≥12 个月；
- 系统实时数据扫描时间周期为 1～10 秒可调；
- 数据刷新同步时间 ≤5s；
- 本地日志审计记录条数 ≥10000 条；
- 平均故障间隔时间（MTBF）≥50000h。
- 对时精度 IRIG-B≤1μs SNTP≤100ms；
- 支持 Web 客户端>=256 个

系统部署

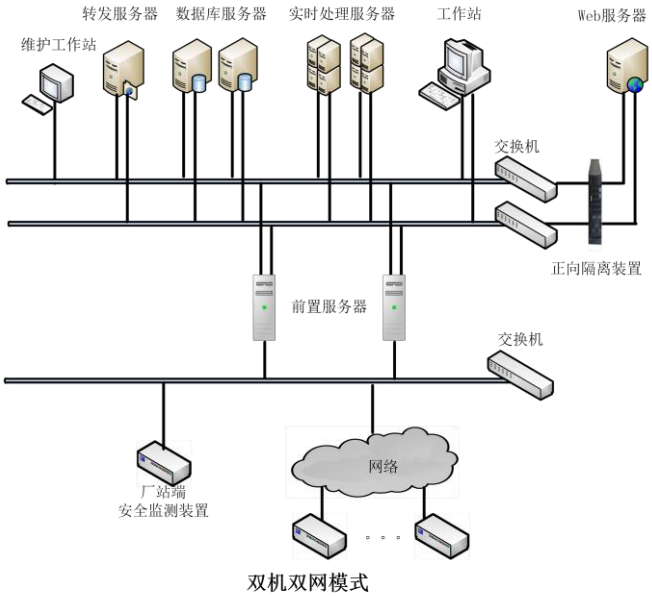
系统主要硬件组成如表所示：

序号	名称	说明
1	DBS	数据库服务器
2	RTDS	实时处理服务器
3	FEP	前置服务器
4	WORKSTATION	工作站
5	FWD	转发服务器
6	WEB	WEB 服务器
7	ENG	系统维护工作站

系统部署模式可采用单机单网、单机双网、双机单网、双机双网的模式。这几种模式的系统稳定性及可靠性逐步提高。采用哪种模式根据要求而定。双机双网架构即双实时处理服务器，双前置机，双数据，双以太网络，具有很高的系统的稳定性，可靠性。

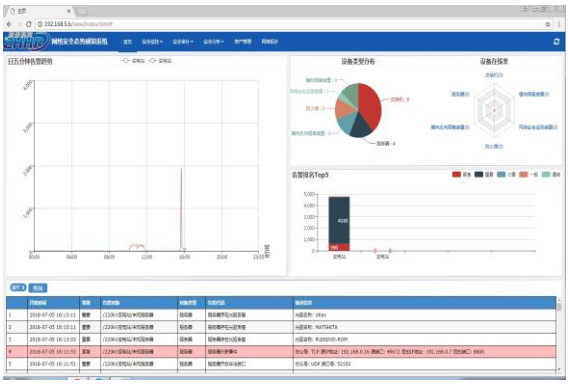
软件系统通过本地以及调度数据网与各个厂站端设备进行通信。

网络安全态势感知系统双机双网结构部署如图所示。

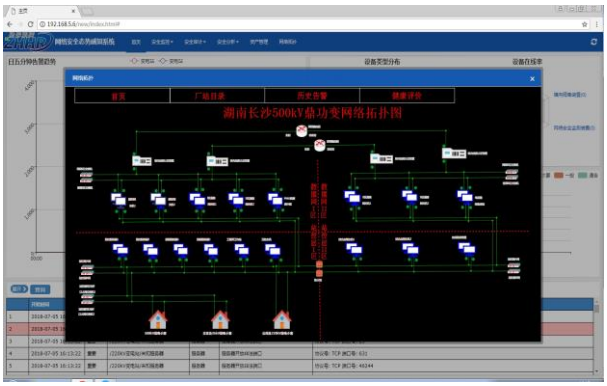


双机双网模式

运行实例

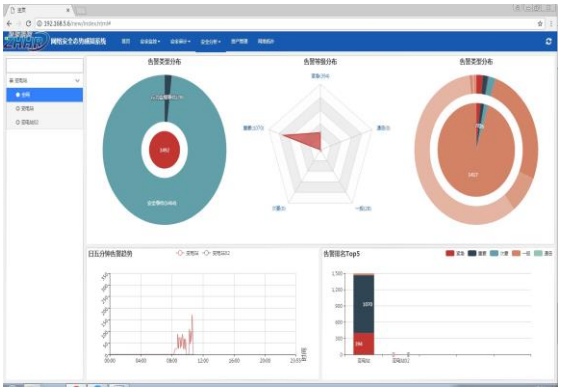


系统首页

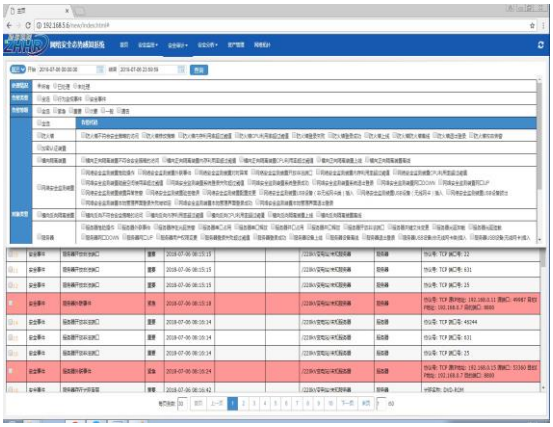


系统拓扑图

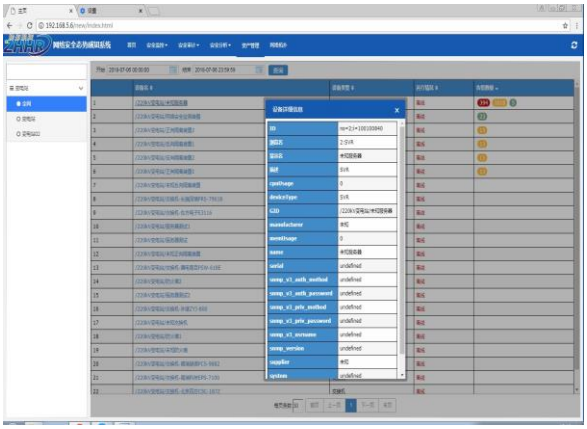
安全概况



安全分析



安全审计



资产管理