电力监控系统网络安全态势感知

主站系统技术规范

（试行）

中国南方电网系统运行部

二零一八年四月

目　次

1　范围 1

2　规范性引用文件 1

3　术语和定义 1

3.1　电力监控系统网络安全态势感知主站系统 1

3.2　电力监控系统网络安全态势感知厂站装置 1

4　总体架构 1

5　平台功能 2

5.1　数据采集 2

5.1.1　采集范围 2

5.1.2　采集内容 3

5.1.3　采集频率 4

5.2　纵向通信 4

5.2.1　传输模式 4

5.2.2　传输内容 4

5.3　横向通信 5

5.3.1　跨区同步 5

5.3.2　与 OMS 互联 5

5.4　平台管理 5

5.4.1　平台运行状态监视 5

5.4.2　通信监视 6

5.4.3　资产信息管理 6

5.4.4　区域配置管理 6

5.4.5　厂商管理 7

5.4.6　处置方案管理 7

5.4.7　日志管理 7

5.4.8　通信参数配置 7

5.4.9　用户管理 7

5.4.10　值班管理 7

6　应用功能 7

6.1　实时监视 7

6.1.1 安全概况 8
6.1.2 告警监视 8
6.1.3 上下级调阅监视 12
6.1.4 设备状态监视 13
6.1.5 拓扑监视 14
6.1.6 威胁监视 15
6.1.7 合规监视 17

6.2 综合审计 18
6.2.1 行为审计 18
6.2.2 关联分析 18
6.2.3 沙箱 19
6.2.4 统计分析 20

6.3 预测分析 22
6.3.1 全局风险评估 22
6.3.2 威胁场景算法 22
6.3.3 大数据分析 23

7 硬件部署要求 23

7.1 主站系统硬件部署架构 23

7.2 主站系统硬件清单 23

7.3 设备配置要求 24

8 性能及安全性要求 24

8.1 性能要求 24

8.2 安全要求 25

8.3 其它 25

附录 A 电力监控系统网络安全态势感知系统信息采集规范 1

表 A.1 主机设备采集信息表 1

表 A.2 网络设备采集信息表 2

表 A.3 纵向加密装置采集信息表 4

表 A.4 正反向隔离装置采集信息表 5

表 A.5 硬件防火墙设备采集信息表 6

表 A.6 入侵检测系统采集信息表 7
表 A.7 数据库采集信息表 7
附录 B 电力监控系统网络安全态势感知系统安全告警分类规范 1
B.1 告警定义 1
表 B.1 安全事件类告警表 1
表 B.2 运行异常类告警表 1
表 B.3 设备故障类告警表 2
附录 C 电力监控系统网络安全态势感知系统上下级通信规范 1
C.1 概述 1
C.2 实时数据传输内容 1
C.2.1 传输方式 1
C.2.2 报文格式 1
C.2.3 传输内容 1
C.3 调阅数据信息 1
C.3.1 传输方式 1
C.3.2 数据集定义 2
附件 D 主站系统与厂站装置 104 通信协议 1
D.1 通讯规约定义 1
D.2 基本报文格式 1
D.3 认证请求报文 2
D.4 认证应答报文 3
D.5 认证确认报文 3
D.6 事件上传报文 4
D.7 事件确认报文 4
附录 E 主站系统与厂站装置 TCP 通信协议 1
E.1 通讯规约定义 1
E.2 历史采集信息调阅 1

E.3 历史事件调阅 3

E.4 基线核查 4

E.5 命令控制 5

E.6 配置管理 6

E.7 软件升级 9

E.8 监控对象参数管理 10

E.9 返回值/错误码定义 10

1 范围

本规范规定了电力监控系统网络安全态势感知主站系统的功能、硬件部署、性能及安全性等技术要求，其中功能包括平台功能（数据采集、纵向通信、横向通信、平台管理）及应用功能（实时在线监视、历史综合审计、预测分析）。

本规范适用于南方电网各级单位,可用于指导电力监控系统网络安全态势感知主站系统的规划、设计、建设及验收等工作。

2 规范性引用文件

下列文件中的条款通过本规定的引用而成为本规定的条款。凡注明日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规定。凡未注明日期的引用文件，其最新版本适用于本规定。

《电力系统安全防护规定》（国家发改委 2014 第 14 号令）

《电力监控系统安全防护总体方案和评估规范》（国能安全[2015]36 号）

GB/T 20272 信息安全技术操作系统安全技术要求

GB/T 20273 信息安全技术数据库管理系统安全技术要求

GB/T 22239 信息系统安全等级基本要求

Q/CSG212001-2015 中国南方电网电力监控系统安全防护管理办法

Q/CSG1204009-2015 中国南方电网电力监控系统安全防护技术规范

3 术语和定义

3.1 电力监控系统网络安全态势感知主站系统

电力监控系统网络安全态势感知主站系统（下简称“主站系统”）是指部署在各个调控中心（监控、检修中心），具备网络安全数据采集、安全监视、安全审计、预测分析等功能的系统。

3.2 电力监控系统网络安全态势感知厂站装置

电力监控系统网络安全态势感知厂站装置（下简称“厂站装置”）是指部署在厂站电力监控系统局域网网络内部,对厂站电力监控系统网络安全数据进行采集、分析处理并与主站系统通信的装置。

4 总体架构

全网电力监控系统网络安全态势感知系统的总体部署架构如下图所示：

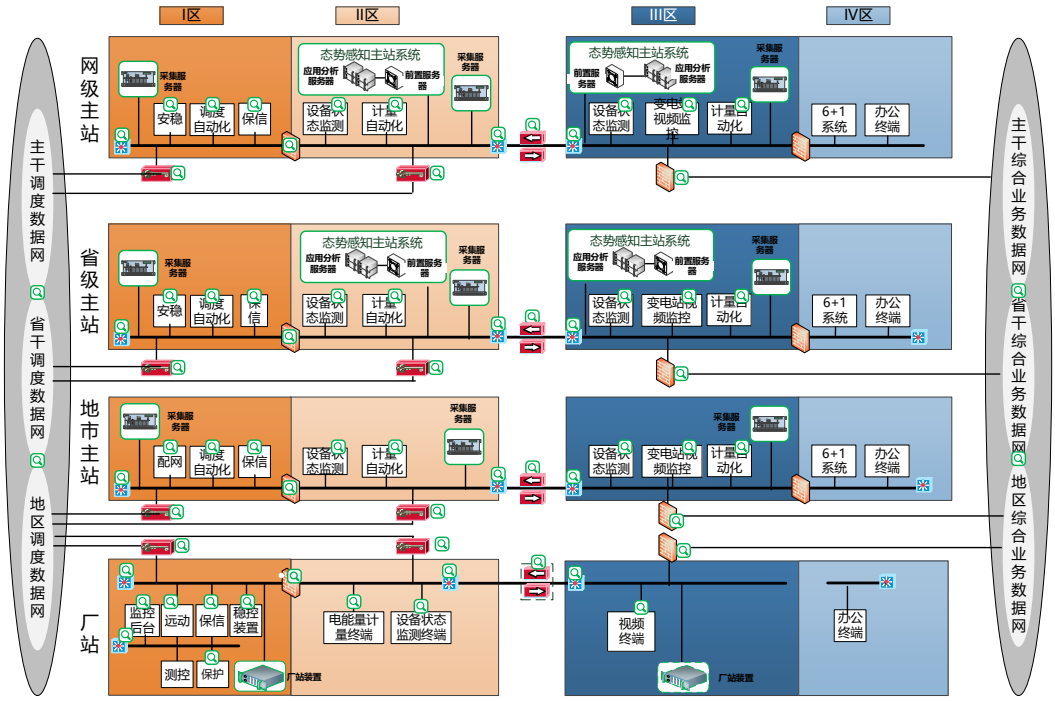

图 4-1 电力监控系统网络安全态势感知系统总体部署架构示意图

电力监控系统网络安全态势感知主站系统、厂站装置在生产控制大区的态势感知数据信息通过调度数据网非实时 VPN 进行交互；主站系统、厂站装置在管理信息大区的态势感知数据信息通过综合数据网进行交互。

在网、省级主站部署电力监控系统网络安全态势感知主站系统。网级主站系统实现对网级电力监控系统主站系统、各省市电力监控系统以及厂站电力监控系统网络安全态势感知数据的汇总、分析以及展示；省级主站系统实现对省级电力监控系统主站系统、各地市电力监控系统以及厂站的态势感知数据的汇总、分析以及展示；在地市级及以下主站端部署态势感知采集服务器，实现对本地市局本部电力监控系统及厂站态势感知数据采集，上送至省级主站系统进行统一汇总、分析及展示。试点建设地级主站系统参照省级主站系统建设。

在厂站端部署厂站装置实现电力监控系统态势感知数据的采集。

5 平台功能

5.1 数据采集

5.1.1 采集范围

主站系统采集范围包括主站内部的主机设备（服务器、工作站等）、网络设备（交换机、路由器等）、安全设备（纵向加密认证装置、正反向隔离装置、硬件防火墙、IDS 设备等）以及数据库。

厂站装置采集范围包括变电站调度数据网边界、站控层及发电厂涉网部分的主机设备（服务器、工作站、远动机、保信、测控装置、设备在线监测、计量自动化等）、网络设备（交换机、路由器等）和安全设备（纵向加密认证装置、硬件防火墙设备等）。

5.1.2 采集内容

主站系统及厂站装置采集内容包括运行状态信息、配置信息、流量传输信息及安全告警信息。

5.1.2.1 主机设备日志

采集内容包括主机登录信息、运行信息等，详细采集内容参见附件 A 表 A.1《主机设备采集信息表》。

5.1.2.2 网络设备日志

采集内容包括网络设备的运行信息、网络连接信息，详细采集内容参见附件 A 表 A.2《网络设备采集信息表》。

5.1.2.3 安全设备日志

a）纵向加密认证装置设备采集信息：应包括装置的操作信息、运行信息、安全事件及配置信息等，信息采集内容参见附件 A 表 A.3《纵向加密认证装置采集信息表》。

b）正反向隔离装置采集信息：应包括装置的系统信息、安全事件等，参见附件 A 表 A.4《正反向隔离装置采集信息表》。

c）硬件防火墙设备采集信息：应包括防火墙的操作信息、运行信息、安全事件等，详细参见附件 A 表 A.5《硬件防火墙设备采集信息表》。

d）入侵检测系统设备采集信息：应包括入侵保护事件，详细参见附件 A 表 A.6《入侵检测系统采集信息表》。

5.1.2.4 网络设备流量

网络设备镜像流量，流探针在不影响网络设备运行的前提下，进行 monitor

采集流量,包括原始流量采集和流量元数据上报。

5.1.2.5 数据库信息

数据库信息采集包括运行信息及安全日志,由数据库完成信息采集并发送到主站系统。详细采集内容参见附件 A 表 A.7《数据库采集信息表》。

5.1.3 采集频率

数据采集频率应分为事件触发、周期采集两种：

a) 事件触发：被采集设备自动触发，主动上送实时数据；

b) 周期采集：对被采集设备进行周期数据轮询采集，周期采集可采用随机函数进行随机周期。

5.2 纵向通信

纵向通信包括主站间通信及主厂站通信。

主站间通信采用自定义 TCP 协议，指标统计类、紧急告警等通过 TCP 长链接上送给上级主站，上级主站通过自定义 TCP 协议调取模型、资产类信息。主站间通讯技术要求详见附录 C。

主厂站通信采用自定义 TCP 协议和 104 协议,其中告警类信息通过 104 协议由厂站装置上传给主站，模型、资产类信息通过自定义 TCP 协议由主站系统主动调阅获取。主厂站通讯技术要求详见附录 D、E。

5.2.1 传输模式

上下级主站间、主厂站间的数据传输分为以下两种模式：

a) 针对实时监视数据，下级主站或厂站装置采用主动周期（5 分钟）推送方式完成数据的交互；

b) 针对统计及审计数据，上级平台通过指令主动调取方式实现数据的交互。

5.2.2 传输内容

传输内容主要如下：

a) 周期上报信息包括安全指数、资产运行信息、接入设备数、离线设备数、安全告警数量、未确认告警数量及告警信息实时统计数据等；

b) 上级平台主动调取下级平台信息包括如下内容：

1) 告警信息统计：包括设备类型、厂站类型、设备厂商、告警等级、

处理状态等信息；

2) 设备数量统计：包括设备类型、厂站类型、设备厂商、在线状态、设备数量等信息；

3) 设备运行信息统计：包括设备类型、厂站类型、设备厂商、离线次数、离线总时长、运行总时长等信息；

4) 纵向密通情况统计：包括厂站类型、设备厂商、明通数据量、密通数据量等信息；

5) 其它：资产信息、拓扑信息、参数配置信息等

5.3 横向通信

5.3.1 跨区同步

各级主站系统在安全 II、III 区分别独立部署，实现由 II 区子系统向 III 区子系统单向数据同步，安全 III 区子系统可全面感知主站系统安全态势。数据同步内容主要如下：

a) 资产信息；

b) 拓扑信息；

c) 告警信息；

d) 设备运行信息；

e) 基线核查及漏洞扫描结果信息；

f) 历史数据。

5.3.2 与 OMS 互联

当态势感知系统发现异常情况时，首先定位出现违规行为或者出现网络安全风险的设备，在对违规行为或者网络安全风险分析的基础上，并根据系统设备的网络安全风险或者违规行为自动生成工单，发送给 OMS 系统，触发网络安全风险处置流程。

5.4 平台管理

提供主站系统自身管理、配置功能，主要如下：

5.4.1 平台运行状态监视

平台运行状态监视包括：

a） 监视后台进程服务运行状态；

b） 监视服务器负载情况；

c） 监视数据库服务器磁盘使用情况。

5.4.2 通信监视

5.4.2.1 主站间通信监视

下级主站（客户端）周期发送心跳报文到上级主站(服务端)：

a） 客户端周期性(周期可配置,默认值为 30s)发送心跳报文，服务端根据接收到的报文信息判断通信状态；

b） 若连续 3 个心跳周期心跳报文未发送成功，则生成形成告警信息推送至客户端主站系统并记录日志。

5.4.2.2 主厂站通信监视

采用 104 规约通信监视机制实现主厂站通信监视。

5.4.2.3 II、III 区通信监视

II 区（客户端）周期发送心跳报文到III区(服务端)：

a） 客户端周期性(周期可配置,默认值为 30s)发送心跳报文；

b） 若连续 3 个心跳周期心跳报文未发送成功，则生成形成告警信息推送至客户端主站系统并记录日志。

5.4.3 资产信息管理

资产信息管理包括：

a） 资产信息添加、删除、修改等功能；

b） 资产信息导入、导出等功能；

c） 资产信息筛选、检索等功能。

5.4.4 区域配置管理

区域配置管理包括：

a） 区域配置添加、删除、修改等功能；

b） 区域配置导入、导出等功能；

c） 区域配置筛选、检索等功能。

5.4.5 厂商管理

管理平台中各个设备类型的生产厂商相关信息,包含厂商名称、设备型号等。

5.4.6 处置方案管理

处置方案管理用于存储告警信息的处理方案，为同类告警提供处理方案参考，处置方案管理包括：

a) 告警解决方案的添加、删除、修改等功能；

b) 告警解决方案的导入、导出等功能。

5.4.7 日志管理

日志管理提供对平台自身最近 6 个月操作记录的管理，日志管理包括：

a) 系统操作日志的记录、查询功能；

b) 系统操作日志的导出功能。

5.4.8 通信参数配置

应具备对主站系统通信参数的配置功能,支持用户配置本级主站系统的各种参数和与上下级主站系统的调阅信息。主要包括：

a) 支持本级平台与上下级平台的数据传送通道的 IP 和端口号的配置功能；

b) 支持配置上下级调阅参数，具备上下级调阅参数的编辑功能，可配置主动调阅下级平台的定制数据。

5.4.9 用户管理

a) 用户信息的添加、删除、口令修改等功能；

b) 用户登录身份验证功能；

5.4.10值班管理

a) 告警处理情况交接；

b) 设备运行情况交接；

c) 当天工作报告填写。

6 应用功能

6.1 实时监视

6.1.1 安全概况

实时监视功能重点关注电力监控系统的网络安全风险，包括自身可被利用造成损害的漏洞，也包括来自外部的威胁。

安全概况功能即系统首页，基于系统整体的安全数据，宏观展示全网网络安全的脆弱性和威胁度。脆弱性包括合规监视和设备状态监视，用以描述电力监控系统资产及其防护措施在安全方面的不足；威胁度用以描述电力监控系统资产可能受到来自外部安全侵害的可能及影响；同时，在告警监视模块实时展示全网告警总数；以地图或列表的模式，展示出全网的安全指数，用以描述脆弱性与威胁度共同影响下的安全状况。

安全概况主要内容包括：

a) 合规概况：展示最近一次安全合规性检测项的检测不符合数/检测项总数和合规率。

b) 设备概况：实时展示本级平台所监视的电力监控系统的设备在线率、在线设备数、总设备数，监视范围包括：主机操作系统监视、网络设备监视、安全设备监视。

c) 告警概况：实时展示本级平台所监视的电力监控系统的告警情况。告警情况分未处理和已处理两种状态，分别以紧急、重要、一般三种告警级别统计（详见附件 B）。

d) 威胁监视：实时展示本级平台所监视的电力监控系统可能形成入侵的威胁行为次数（外设接入、网络接入、设备登录操作）和网络流量异常次数。

e) 安全指数：由合规率、设备监视结果、告警监视结果、威胁监视结果通过安全指数算法计算所得。通过点击安全指数，查看指数明细信息，并根据着色显示对指数的影响程度。

6.1.2 告警监视

提供对实时告警信息的监视功能，主要如下：

a) 支持告警推送提醒功能，通过颜色标记、声音提醒、告警内容语音播报、短信推送等手段提示新告警产生；

b) 支持告警确认功能，能够为告警添加已阅标记，便于操作人员关注新发

生告警，防止遗漏；

c）提供告警解决方案，用于在告警解决后消除实时告警信息。在提交解决告警时可选择或手动输入解决方案；

d）提供告警筛选功能，根据告警的各个属性进行筛选；

e）提供总告警数及不同类型的告警数的统计信息。

6.1.2.1 告警列表

a）告警事件以列表方式集中展现，系统清晰显示详细告警信息；系统提供自动刷新、直观的当前告警列表，按照告警级别重要性以不同颜色排序显示告警信息；

b）不同用户根据角色配置，可查看职责范围内的告警信息；

c）提供告警的查询功能，可按照告警源、时间范围、告警状态、告警级别、告警类型、告警内容等组合查询告警；

d）提供告警统计功能，以表格和图形方式进行显示。

e）实时显示事件内容包括：接收时间、事件类型、事件名称、报警级别、来源 IP、目的 IP、设备类型、设备来源 IP 等。

f）查看事件详细信息和原始信息。

g）可以显示一段时间的动态事件移动图，能够在图上显示每个时间切片的事件数量、等级，并能够在图上显示总的事件数和每秒事件数。用户点击每个时间切片，可以查看该切片内的事件。

h）可以对事件依据其源目的 IP 和端口信息进行深入的事件追踪调查。

i）对于关联事件，可以钻取出导致该关联事件的原始事件。

j）可以对选中的事件源/目的 IP 地址进行地图定位。

k）可以对选中的事件进行行为分析，并可视化的展示一幅描述事件之间相互关系的行为图。

l）系统提供了准实时监视与审计视图，通过仪表板和查询条件，管理员可进行交互式分析，管理员可以根据内置或者自定义的安全事件分析策略，从事件的任意维度实时观测安全事件的走向，也可以通过交互式查询，任意输入格式化字段和原始信息关键字等查询条件，通过组合、嵌套等多种方式进行事件的搜索、关联和收敛，并可以进行事件的调查、钻取

和统计，并进行事件行为分析和来源定位等。

m) 系统提供了事件实时和历史统计统一视图，管理员可以根据内置或者自定义的事件分析策略，系统提供对分析策略过滤出的事件进行统计分析，可设置 2 个统计条件，统计图样支持堆积柱状图和饼图，可对事件数量、持续时间、发送字节数、接收字节数和总流量等内容进行统计，支持 TopN 统计；根据统计结果可直接钻取符合条件的事件从事件的多个维度实时进行安全事件统计分析，并以柱图、饼图、堆积图等形式进行可视化的展示。用户点击事件任意属性字段，可以该字段为条件对事件进行统计分析。

n) 用户可自定义查询策略，基于时间、名称、地址、端口、类型等各种格式化事件属性条件进行组合查询，也可以象搜索引擎那样输入关键字和正则表达式进行原始事件的全文搜索，快速获取查询结果。系统具备基于任务的查询调度功能。

o) 系统具备事件关联分析功能，提供了可视化的规则编辑器。用户可以定义基于逻辑表达式的关联规则，所有日志字段都可参与关联。系统支持单事件关联、多事件关联、逻辑关联和统计关联。

p) 系统能够将安全事件与当前网络和业务的实际运行环境进行关联，透过更广泛的信息相关性分析，识别安全威胁。系统支持基于弱点的情境关联、基于资产的情境关联、基于威胁情报的情境关联、基于网络告警的情境关联、基于预警与风险的情境关联、基于拓扑的情境关联。

q) 系统具有对海量历史事件的规则关联分析功能，能够对海量的历史事件进行基于规则的关联分析，识别过去已发生的入侵和违规。

r) 管理员能够根据关联分析的结果将可疑或者需要关注的信息加入观察列表，并可以继续对观察列表中的信息进行关联，也可以被任何规则引用。

6.1.2.2 告警详情

6.1.2.2.1 安全事件类告警

安全事件类告警指监视对象运行过程中监视到非法访问、操作时产生的安全事件。监视对象检测到该类安全事件时需要立即产生告警并上报。安全事件类告警包括如下内容，详见附件 B 表 B.1：

a) 设备跨区互联告警（紧急）；

b) 主机设备非法外联告警（紧急）；

c) 纵向加密认证装置、正反向隔离装置、硬件防火墙设备拦截到的不符合安全策略的访问（重要）；

d) 平台基于访问端口对不符合安全策略的访问进行分析后产生的异常访问告警（重要）；

e) 主机设备发现的用户异常操作告警(普通)；

f) 主机设备发现的非法链路告警(普通)；

g) 主机设备关键目录权限变更（重要）；

h) 主机设备发现的非法设备接入告警（重要）；

i) 网络设备发现的非法网络接入告警（重要）；

j) 主机设备、网络设备、安全设备发现的非法登录尝试告警（普通）；

k) 网络传输可疑文件、可执行文件告警（重要）；

l) 主机设备外设设备接入告警（重要）；

m) 网络明文传输账号告警（重要）；

n) FTP 传输协议告警（重要）；

o) 网络扫描行为告警（重要）。

6.1.2.2.2 运行异常类告警

运行异常类告警指监视对象自身运行产生的安全事件。主要来源为监视对象自身检测发现的运行异常告警和平台通过监视对象运行信息分析出的设备运行异常告警。运行异常类告警包括如下内容，详见附件 B 表 B.2：

a) 纵向加密认证装置检测到的隧道建立错误告警（重要）；

b) 纵向加密认证装置检测到的备机心跳丢失告警（重要）；

c) 平台通过监视对象 CPU 利用率信息分析出的 CPU 使用越限告警（普通）；

d) 平台通过监视对象内存利用率信息分析出的内存使用越限告警（普通）；

e) 平台通过主机设备未关闭的 TCP 连接数分析出的未关闭 TCP 连接过多告警（普通）；

f) 平台通过主机设备僵尸进程数分析出的主机存在大量僵尸进程告警（普通）；

g) 网络设备检测到的流量突变告警（普通）;

h) 平台通过监视对象磁盘利用率信息分析出的磁盘使用越限告警（重要）;

i) 主机设备检测到的硬盘存储空间不足告警（重要）;

j) 设备开启高危网络服务告警（重要）。

6.1.2.2.3设备故障类告警

设备故障类告警指监视对象自身硬件状态异常时产生的安全事件。设备故障类告警包括如下内容，详见附件 B 表 B.3：

a) 监视对象自身检测到的电源故障告警（重要）;

b) 监视对象自身检测到的风扇故障告警（重要）;

c) 监视对象自身检测到的网口状态异常告警（重要）;

d) 监视对象自身检测到的温度异常告警（重要）。

6.1.3 上下级调阅监视

6.1.3.1 主站系统监视

主站系统应支持对下级主站系统页面的调阅，其中网级主站系统支持跨级调阅，能够查看省、地两级主站系统页面；省级主站能查看调管范围内地级主站系统页面。调阅查看的页面范围包括：实时监视、综合审计。

拥有上下级调阅权限的用户应区别于系统普通用户，并具备专门的安全身份认证机制。

上下级调阅数据传输过程中，应采用相应的通信加密技术确保通信的机密性和数据的完整性，防止恶意截获、篡改数据、恶意破坏等。

6.1.3.2 厂站监视

a) 厂站监视主要包括厂站的通道状态监视和资产信息、拓扑信息、历史告警的数据跨级调阅监视;

b) 上级主站周期性调阅下级厂站 “资产信息”，下级厂站收到上级主站调阅请求后开始组装最新站内资产信息，并通过自定义 TCP 通道以 E 格式上送至主站系统，主站系统将厂站资产信息入库并展示。在执行下一次调阅请求前，界面上将一直展示本次调阅的数据;

c) 上级主站周期性调阅下级厂站 “拓扑信息”，下级厂站开始组装最新站

内拓扑信息，并通过自定义 TCP 通道以 E 格式上送至主站系统，主站系统将厂站拓扑信息入库并展示。在执行下一次调阅请求前，界面上将一直展示本次调研的数据；

d) 上级主站根据设置告警类型和起始时间调阅站内 “历史告警”数据，下级厂站根据上级主站调阅请求开始组装相应的站内历史告警信息，并通过自定义 TCP 通道以 E 格式上送至主站系统，主站系统将厂站历史告警信息入库并展示。在执行下一次调阅请求前，界面上将一直展示本次调阅的数据。

6.1.4 设备状态监视

设备状态监视包括主机操作系统监视、网络设备监视、安全设备监视。设备监视以图形的方式分别实时展示各类设备的在线率。其中，在线率算法为非离线资产在总资产中的比率。

6.1.4.1 主机设备监视

主机设备监视功能包括如下功能：

a) 运行状态监视包括在线状态、CPU 利用率、内存利用率、磁盘使用率、电力监控系统核心应用的关键进程、僵尸进程数、未关闭的 TCP 连接数；

b) 告警信息监视包括告警数、未确认告警数；

c) 操作信息监视包括登录用户数，活跃用户数（正在操作的用户）；

d) 外设设备使用情况监视包括 USB 接口插拔状态 USB 接入数、并口使用情况（是/否）、串口使用情况（是/否）、光驱使用情况（是/否）；

e) 设备异常监视网口状态（UP/DOWN）、电源模块状态(正常/异常)等。

6.1.4.2 网络设备监视

网络设备监视功能包括如下功能：

a) 运行状态监视包括设备在线状态、CPU 利用率、内存利用率；

b) 告警信息监视包括告警数、未确认告警数；

c) 设备异常监视包括网口状态。

6.1.4.3 安全设备监视

安全设备监视包括如下内容：

a) 纵向加密认证装置监视包括如下内容:

1) 运行状态监视包括设备在线状态、CPU 利用率、内存利用率、主备机状态（正常/异常）、明/密通隧道数量、明/密通策略数量、设备密通率;

2) 告警信息监视包括告警数、未确认告警数;

3) 设备异常监视包括网口状态（UP/DOWN)。

b) 正反向隔离装置监视包括如下内容:

1) 运行状态监视包括设备在线状态、CPU 利用率、内存利用率、传输状态(通/断);

2) 告警信息监视包括告警数、未确认告警数;

c) 硬件防火墙设备监视包括如下内容:

1) 运行状态监视包括在线状态、CPU 利用率、内存利用率;

2) 告警信息监视包括告警数、未确认告警数;

3) 设备异常监视网口状态、电源模块状态、风扇状态。

6.1.5 拓扑监视

拓扑监视功能以拓扑图的形式展示监视对象的整体运行状态,同时提供以设备为单位的管理功能，将平台的日常功能集成，统一进行展示，主要如下:

a) 支持资产自动发现功能,主站数据采集服务器支持通过 IEC61850、IEC103（含扩展部分)、IEC104、SNMP、SNMP Trap、Syslog、SSH、端口镜像等标准协议，实现对主机设备、网络设备、安全设备等的资产自动发现，根据采集数据自动形成新的资产台账，并可根据预配置的 IP 范围，自动将新设备划分到对应的安全分区;

b) 资产可以按安全区、所在区域、资产类型等属性进行筛选，同时支持资产查询、人工更新资产部分属性;

c) 支持拓扑图生成功能，能够将网络中大部分设备根据网络连接关系生成拓扑图，支持对拓扑进行手动微调，支持拓扑分层展示，可以放大缩小。设备在拓扑中可以自由的设置位置、调整显示方式，形成完整的拓扑关系;

d) 拓扑中展示电力监控系统内的全部监视对象，包含服务器、交换机、路

由器、纵向加密设备、横向隔离装置、硬件防火墙设备等；

e）根据资产类型能够与如下功能进行关联：

1）告警，显示该资产的告警详情；

2）资产，显示该资产的属性详情；

3）连接，显示该资产的连接情况；

4）核查，提供对该资产进行安全配置核查的功能；

5）评估，提供对该资产进行安全风险评估的功能；

6）行为，显示资产的行为监视详情；

f）在发生如下情况时，资产上要有直观的展示：资产离线及检修、发生告警、外设接入、跨区互联等。其中跨区互联监视是对于具备跨区互联特征的设备，在网络拓扑图中使用指定的告警图标、颜色等显示对应的设备、端口、互联连接线等，并提供跨区互联相关的取证信息；

g）要能够实时展示资产的运行信息，如 IP、CPU 和内存使用率、流量等。

6.1.6 威胁监视

威胁监视包括用户外设接入行为监视、网络接入行为监视、设备登录行为监视、以及网络流量监视。该功能分别统计本级和下级单位未处理的威胁行为次数。

6.1.6.1 外设接入行为监视

外设接入行为监视应实现实时监视主机外设接口接入行为的安全事件(非法 USB 接入、非法光驱接入)，非法接入后未拔出视为威胁未处理。

6.1.6.2 登录行为监视

登录行为监视功能实现实时监视当天内主机、网络设备、安防设备登录成功的事件，及登录时间内相关设备的操作指令。

登录行为包括本地登录和远程登录两种。本地登录包括 console 接口登录、串口登录、TTY 登录等多种登录方式；远程登录包括 telnet、ssh 等远程协议的登录。

6.1.6.3 网络接入监视

设备行为监视主要对主机设备、网络设备、安全设备的设备网络行为进行监视。采集网络设备网口 up/down 状态变化信息 ，将网络设备端口运行状态信息

形成告警信息，判断为网络接入。

支持自动检测不同安全区域之间的非法跨区互联分析，包括站内安全 I/II 区非法互联、生产控制大区与生产管理大区非法互联、与外网的直接互联等网络安全风险分析，能自动对跨区互联的设备进行网络安全取证，取证信息包括设备信息、网络连接信息等。

6.1.6.4 网络流量监视

网络流量监视通过流量探针对原始网路流量进行特征提取和预处理，并对当天网络中流量情况的分析展现，包括：流量大小监视、通讯会话监视、流量异常监视三个功能需求。

a） 流量大小统计

1） 支持以折线图的方式展现当天流量大小统计变化

- 图形展现横轴为时间点；纵轴为流量大小；
- 横轴起点为当天 00:00，时间点间隔为 5 分钟；
- 展示时，仅展示当前一个小时以内的流量变化，可通过拖动方式查看当天历史流量；
- 当存在多个流量采集点时，可进行不同采集点的选择展现；
- 可添加某 IP 流量折线图进行对比；
- 支持自动刷新。

2） 支持以列表方式展现当天所有 IP 流量大小情况

- 按照 IP 地址、上行流量、下行流以及总占比进行统计展示；
- 支持基于 IP 的查询功能；
- 支持各列的升降排序功能；
- 统计周期起点为当日 0 点，结束为当前时间；
- 支持自动刷新。

b） 通讯会话监视

1） 支持以列表方式展示当日所有通讯会话基本信息，要求如下：

- 列表包含五元组、应用识别、最新发现时间、次数、操作；
- 支持点击次数弹窗显示详情（当天），详情中包括当日每一次会话的

起止时间以及通讯持续时长；

- 支持各列的升降排序功能；
- 支持自动刷新；
- 列表支持基于列名的组合筛选功能。

c） 流量异常监视

1） 支持以饼图方式按照攻击类别分类展示当日异常流量，具体要求如下：

- 统计当日所发现异常流量的总次数；
- 根据不同类型的攻击方式统计攻击次数并展示。

2） 支持以条形图方式对当日基于攻击源以及攻击目标攻击次数统计的 TOP10 展示。

3） 支持以列表方式展示当天网络流量异常情况，具体要求如下：

- 根据不同类型的攻击方式统计攻击次数并展示
- 列表包括攻击源、攻击目标、攻击方式、描述、最新发现时间、次数；
- 支持点击次数显示当日历史详情，包括攻击起止时间，攻击详情、攻击持续时长；
- 支持自动刷新。
- 列表支持基于列名的组合筛选功能

6.1.7 合规监视

合规监视综合分析各单位电力监控系统合规评价结果数据，通过合规率计算公式得出本级平台的合规率，在界面展示合规率和部分检查项检测不合规的个数。

支持合规评价标准的创建、导入、发布，支持依照标准创建对应的评价任务。

通过系统采集网络安全数据（主机配置信息、漏洞及补丁安装情况）、自动化计算系统合规性情况，通过模型、公式得出全网合规率数据，对部分需要人工参与合规性判别的测评项，通过网络安全数据采集，结合人工评判，实现系统半自动化合规率分析。

支持按单位归属、业务系统、业务系统安全等级等维度实现全网电力监控系统网络安全合规率综合展现，呈现全网网络安全态势。

6.2 综合审计

6.2.1 行为审计

6.2.1.1 外设接入行为

a）提供外设设备（usb/光驱、串口/并口）接入信息的记录，查询功能，可查询昨天、本周、近一月数据；

b）接入信息应包含设备类型、接入时间、拔出时间等；

c）点击接入次数、拔出次数可查看详细告警信息；

d）支持生成安全报告，安全报告应包括外设接入信息、接入明细信息。

6.2.1.2 主机登录行为

a）主机登录行为审计应包括对 SSH 登录、X11 协议登录以及本机登录信息；

b）审计信息应包含链路信息、目标主机、链路时间、退出时间、登录用户、操作命令数；

c）支持相关行为关联审计的回溯；

d）支持查看链路的操作命令及回显信息。

6.2.1.3 网络接入行为

a）提供交换机设备网口 up/down 信息的记录、查询等功能；

b）接入信息应包含交换机信息、接入设备 IP、接入时间、断开时间等；

c）审计存在跨区互联行为、非法网络接入行为

d）用图元的形式呈现非法网络接入、跨区互联行为。

6.2.1.4 网络通信行为

a）提供网络通信记录、查询等功能；

b）基本信息应包括 IP 五元组（源 IP、源端口、目的 IP、目的端口、传输协议）、流量大小、通信开始时间、通信结束时间、时长；

c）点开数据展示详情：列表或图元展示某主机在时间段内访问了哪些主机、某主机在时间段内被哪些主机访问、流量大小、访问时长；

d）展示一个链路流量基于时间段分析曲线图；。

6.2.2 关联分析

关联分析是对设备相关操作行为的关联分析及操作路径的回溯，主要包括审计资产、溯源分析、通信链路、设备告警、登录行为五大模块。

a) 审计资产：基于系统的维度展示当前系统包含的设备

b) 溯源分析：通过拖拽审计资产和通信链路中的设备到溯源分析模块中基于指定时间段的告警信息、操作行为信息自动展示设备间的通信关联图。在溯源分析模块中选中某设备同步刷新通信链路、设备告警、登录行为模块的信息。

c) 通信链路：展示与溯源分析模块中选中的设备，且与该设备有过通信的设备

d) 设备告警：展示溯源分析模块选中设备指定时间段的告警信息

e) 登录行为：展示溯源分析模块选中设备指定时间段的登录行为信息。

6.2.3 沙箱

沙箱审计功能应能够对网络中捕获的文件进行各种统计分析以及展现，包括文件统计、执行分析两个功能模块。

6.2.3.1 文件统计

文件统计是对统计周期内发现的文件进行多维度统计展现，具体功能要求如下：

a) 统计周期包括最近 24 小时、最近 1 周、最近 1 个月、最近 3 个月、最近 1 年以及自定义时间。

b) 统计内容包括：文件检测结果占比、恶意文件占比、恶意文件传播次数趋势、TOP 恶意文件传播数量、恶意文件数量（按协议类型）、恶意文件数量（按照威胁类型；

- 文件检测结果占比：对于总文件按照威胁等级（安全、高危、中危、低危）以饼图方式分类统计展现；
- 恶意文件占比：对于恶意文件按照文件类型以饼图方式分类统计展现；
- 恶意文件传播次数趋势：对于恶意文件按照危险级别（高危、中危、低危）基于时间以折线图的方式分类统计展现；
- TOP 恶意文件传播数量：对于恶意文件按照具体文件的传播统计次数以条形图的方式排序展现（最多只展现到 TOP10）；

- 恶意文件数量（按协议类型）:对于恶意文件按照协议类型（恶意文件传递的方式）以条形图的方式分类统计展现；
- 恶意文件数量（按照威胁类型）：对于恶意文件按照威胁类型以条形图的方式分类统计展现。。

6.2.3.2 执行分析

执行分析是对恶意文件的危害以及发现详情的集中分析，具体要求如下：

a) 按照统计周期展现恶意文件的明细，统计周期包括最近 24 小时、最近 1 周、最近 1 个月、最近 3 个月、最近 1 年以及自定义时间；

b) 以文件列表方式展现恶意文件明细，列表名称包括：检测结果、威胁类型、文件名称、文件类型、文件 MD5、文件大小（字节）、协议、检测次数、首次发现时间、最近发现时间、操作。点击操作显示详情，详情包括：文件威胁行为、文件传播信息。

- 文件威胁行为展现恶意文件的危害详情，支持危害详情导出功能；
- 文件传播信息展现恶意文件的发现详情，详情列表名称包括检测结果（威胁等级）、提交时间、文件名称、源 IP、目的 IP、文件来源、协议、邮件发件人、邮件主题、父文件 MD5；

c) 支持父子文件关联展示功能；

d) 支持恶意文件的筛选功能。。

6.2.4 统计分析

6.2.4.1 端口使用统计分析

基于时间维度，提供主机上端口使用情况的统计分析。统计分析内容包括：

a) 某段时间内按单位时间统计某端口开启、关闭次数；

b) 某段时间内按单位时间统计某个设备某端口被连接次数；

c) 某段时间内按单位时间统计多个设备某端口总共被连接次数；

d) 其中，统计的端口：21、22、80、135、139、445、3389、4489 等；

e) 单位时间：小时、天、月

6.2.4.2 登录行为统计分析

基于时间维度，提供所有设备的登录事件的统计分析，统计的指标为登录时

间、登录的用户。

a）统计汇总

- 默认按周统计 7 天（单位天）内所有设备的登录成功、登录失败总次数；
- 支持按小时统计（单位小时）内所有设备的登录成功、失败次数总次数；
- 支持按月时统计（单位天）内所有设备的登录成功、失败次数总次数；
- 支持按年统计（单位月）内所有设备的登录成功、失败次数总次数；

b）针对单台设备的登录信息查询

- 支持用户输入 IP 搜索设备，系统需要对 IP 的合理性进行校验。当用户点击搜索按钮时，展现该台设备的登录成功、失败的次数的统计信息；
- 支持按小时统计（单位小时）设备的登录成功、失败次数的统计；
- 支持按周统计（单位天）7 天内设备的登录成功、失败次数的统计；
- 支持按月统计（单位天）设备的登录成功、失败次数的统计；
- 支持按年统计（单位月）设备的登录成功、失败次数的统计。

c）按设备统计登录成功失败的总次数

- 支持查询选定天数内的设备登录成功总数、失败总次数降序排列展示，分页显示前 10 条、前 50 条、前 100 条登录成功、登录失败信息。
- 支持显示单台设备的登录成功失败统计。

d）按设备统计该设备登录成功失败的总次数

- 支持查询选定天数内的选定设备所有用户的登录成功总数、失败总次数降序排列展示，分页显示前 10、前 50 条、前 100 条登录成功信息。

6.2.4.3 用户账户统计分析

基于时间维度，提供设备账户的统计分析统计的指标包括用户权限变更，用户密码变化、增删用户等

a）统计汇总

- 默认按周统计 7 天（单位天）内设备主机设备、网络设备、安全设备的用户权限变更，用户密码变化、增删用户的总次数；

- 支持按小时统计（单位小时）内主机设备、网络设备、安全设备的用户权限变更，用户密码变化、增删用户的总次数；
- 支持按月时统计（单位天）内主机设备、网络设备、安全设备的用户权限变更，用户密码变化、增删用户的总次数；
- 支持按年统计（单位月）内主机设备、网络设备、安全设备的用户权限变更，用户密码变化、增删用户总次数；

b）针对单台设备

- 支持用户输入 IP 搜索设备，系统需要对 IP 的合理性进行校验。当用户点击搜索按钮时，展现该台设备的登录成功、失败的次数的统计信息；
- 支持按小时统计（单位小时）设备的用户权限变更，用户密码变化、增删用户的统计；
- 支持按周统计（单位天）7 天内设备的用户权限变更，用户密码变化、增删用户的统计；
- 支持按月统计（单位天）设备的用户权限变更，用户密码变化、增删用户的统计；
- 支持按年统计（单位月）设备的用户权限变更，用户密码变化、增删用户的统计。
- 支持按 Word、Excel 文件格式导出功能。

6.3 预测分析

网络安全分析预测主要包括全局风险评估、威胁场景算法、大数据分析平台等安全功能。

6.3.1 全局风险评估

结合系统台账以及威胁情报，对网络中的技术漏洞及安全风险进行扫描，实现全局风险评估。

6.3.2 威胁场景算法

根据人工分析经验，总结归纳出网络安全风险模型，实现威胁场景的自动匹配。支持在原有的算法模板上调整进化生成新的网络安全风险分析算法。

6.3.3 大数据分析

采用电力监控系统网络安全大数据分析技术，基于流量、日志、设备配置、设备运行信息等各类数据，为网络安全高级分析提供技术支持。

7 硬件部署要求

7.1 主站系统硬件部署架构

电力监控系统网络安全态势感知主站系统部署架构如下图所示：

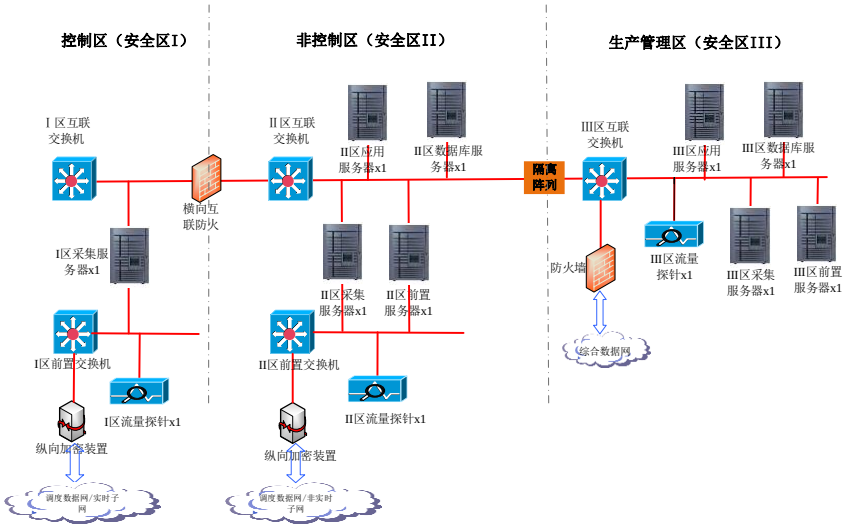

图 6-1 电力监控系统网络安全态势感知主站系统部署架构示意图

主要内容包括：

a) 在 I、II、III 区分别部署采集服务器及流量探针服务器，主要实现对主站电力监控系统数据采集、处理及通信等，其中 II、III 区采集服务器还负责收集所管辖范围内所有厂站装置的上报事件信息，并可调用厂站装置提供的服务实现远程的控制与管理。

b) 在 II、III 区部署平台及应用，为数据存储、平台支撑、安全应用等功能提供支撑，根据不同应用的业务特性来配置相应的应用服务器群。

7.2 主站系统硬件清单

系统配置清单如下：

表 6 **错误!文档中没有指定样式的文字。**-1 主站系统平台硬件配置清单

编号	设备材料名称	部署要求	配置档次	单位	数量
1	探针服务器	I、II、III 区	二档	台	3
2	采集服务器	I、II、III 区	二档	台	3
3	前置服务器	II、III 区	二档	台	2

4	应用服务器	II、III 区	二档	台	2
5	数据库服务器	II、III 区	一档	台	2

7.3 设备配置要求

服务器统一采用 PC 服务器,其中

1）一档服务器应不低于以下配置：

CPU：Intel Xeon E5-2650 V4 处理器或以上,主频≥2.20GHz,每颗 CPU 内核数≥12，配置≥2 颗物理 CPU；

内存：≥256G；

硬盘：至少配置 480GB SSD 硬盘和 25T SAS 硬盘；

网卡：4 块双口千兆以太网卡，支持网络捆绑，支持 TOE 或 IOAT；

PCI 插槽 ≥6 个 PCI-Express 插槽；

电源及风扇：满足 2N 冗余；

有条件可为数据库服务器配置磁盘阵列。

2）二档服务器应不低于以下配置：

CPU：Intel Xeon E5-2650 V4 处理器或以上,主频≥2.20GHz,每颗 CPU 内核数≥12，配置≥2 颗物理 CPU；

内存：≥256G；

硬盘：至少配置 960GB SSD 硬盘和 7T SAS 硬盘；

网卡：4 块双口千兆以太网卡，支持网络捆绑，支持 TOE 或 IOAT

PCI 插槽 ≥6 个 PCI-Express 插槽。

8 性能及安全性要求

8.1 性能要求

平台软硬件性能应满足如下要求：

a) 支持分布式采集，单台服务器采集不少于 500 个设备；

b) 关键设备平均无故障时间（MTBF）＞20000 小时；

c) 支持每秒至少处理 10000 条网络安全数据；

d) 并发用户数不少于 100 个；

e) 系统实时数据扫描时间周期为 1～10 秒间可调；数据刷新同步时间≤5 秒。