## 安全管理（主要功能：监测设备和安全事件）

**设备监测（二级目录）**

通过策略配置、设备监控、审计预警、安全响应等功能组成安全闭环，协助用户实时掌握信息系统的使用运行状态，实时监测各种安全事件，及时应对安全威胁，实现用户网络的整体安全，全面实现统一管理、统一预警和全局审计。

分2个模块 ：上面显示设备状态 下面显示安全事件

**拓扑管理（二级目录）**

## 流量管理（ 主要功能：监测流量）

**流量监测（二级目录）**

指定IP查询：按时间段、按IP，查询结果排序

全网查询：对所有IP可以按时间间隔（小时、天、月）进行排序查询。

结果可以按照日基线、月基线等多种流量基线模型。

## 3.资产管理（主要功能：查看目前的设备）

**设备管理 （二级目录）（包括安全设备、工控设备和在线设备）**

设备列表内容：

自动检测在线设备及安全设备并添加到设备列表中

显示在线、离线、告警状态。

设备升级。

日志备份。

划分安全域

查看设备详情

**防护软件管理（二级目录）**

统一下发（支持以上）？？？？

## 策略管理（主要功能：自定义白名单规则以及出现异常时的告警方案）

**白名单方案管理（二级目录）**

（增删改查）

白名单规则（学习时间可配置）

白名单学习协议例外功能

网络白名单学习的端口映射编辑功能

基于端口的私有协议定义和学习功能

对告警事件一键加入基线，后续将不再产生同类的告警

**设备策略管理（二级目录）**

支持以单个设备和多个设备为单位进行策略管理（包括策略下发、设备操作等）

**白名单管理（二级目录）**

（增删改查

## 5.告警管理（主要功能：设置告警方式）

先自定义一个默认告警方案

**告警设置（二级目录）**

事件实时告警，事件相关综合分析

**告警日志（二级目录）**

日志监控功能设置（监管工控安全网关日志记录功能、监管监测设计系统日志记录功能、监管工作站卫士系统的日志记录功能）

未知设备监测设置（有未知设备接入时进行告警，并迅速发现系统中存在的非法接入）

违法使用USB存储设备进行报警设置（支持声音告警、短信告警）

当产生相应级别的告警时，可以按照号码分组、警告级别发送给相应的接收人。

## 6.报表及展示管理

**报表管理（二级目录）**

要求支持多种格式的显示

生成方法：1.手工报表2.自动报表（按照每小时、每天、每月、每年等周期的方式生成）

提供多种展现仪表盘：包括柱状图、折线图、饼状图、提供用户可定制TOP N展示图标，并支持报表下载。

## 7.系统管理

**系统监控（二级路面）**

系统自身状态监控（包括CPU,内存、硬盘使用率、网口IP地址等）

系统运行参数配置：（包括响应事件、策略管理、设备运行参数等相关信息）

系统各组件服务状态监控

**日志管理（二级目录）**

日志存储空间溢出预警（日志可设定自动备份）

**权限分配（二级目录）**

用户角色配置（包括系统管理员、系统安全员、系统审计员、普通管理员)系统管理员可以分配权限给不同的角色

~~支持多种响应和报警方式，能够对用户关注的满足特定条件的事件进行自动的响应，支持邮件、界面提示等多种响应方式。~~

管理平台与被管理设备之间采用加密传输（只是要求，不写入目录）

**IP拦截（二级目录）**

支持远程登录IP限制功能，仅允许特定的IP可以登录平台。

显示所有被拦截的IP