智能变电站一体化安全防护体系设计

启明星辰集团 朱少敏

❶ 安全分区 ❷ 网络专用 ❸ 横向隔离 ❹ 纵向认证

网络安全法执法检查

全国人大常委会网络安全法、全国人大常委会关于加强网络信息保护的决定（简称“一法一决定”）执法检查组第一次全体会议25日在京举行，正式启动“一法一决定”执法检查。执法检查组将组成6个小组，于9月至10月分赴**内蒙古、黑龙江、福建、河南、广东、重庆**等6省（区、市）开展检查，同时委托北京、天津、河北、辽宁、江苏、安徽、湖北、广西、四川、云南、甘肃、新疆等12个省（区、市）人大常委会分别对本行政区域内“一法一决定”实施情况进行检查。

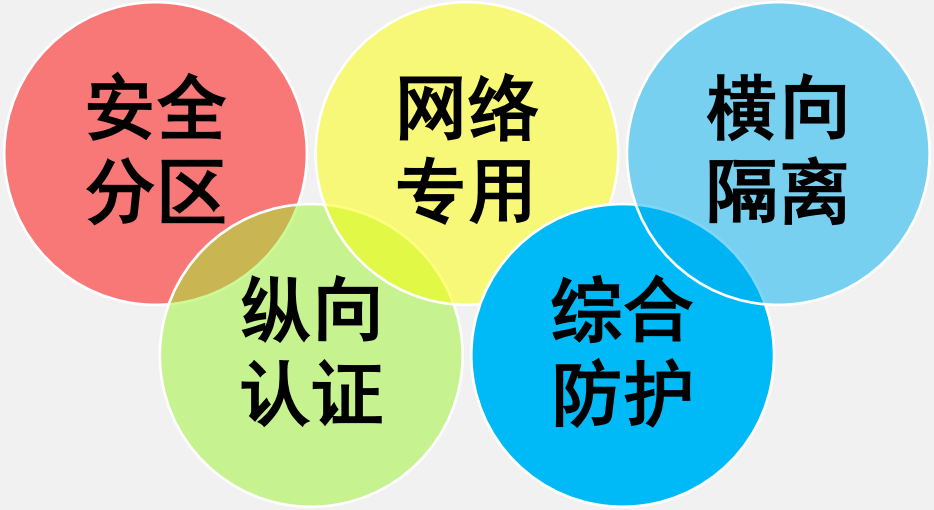
《网络安全法》正式实施
（20170601）

“一法一决定”执法检查
（20170825）

依法依规　严格执法

2017年3月28日，山东省各级调度机构按照《关于对存在重大隐患的新能源场站解除并网的通知》（鲁监能安全〔2017〕37号）要求，对发现的存在严重**电力监控系统安全**隐患的**18家新能源场站**陆续解除并网，切断与上级调度数据网的联络。

11	沂安中广风电场	临沂	集控中心使用电信运营商网络监控所辖风电场，集团集控中心交换机直连站内Ⅰ区远动、Ⅰ区风机监控、Ⅱ区风功率预测。 风功率预测系统中安全Ⅲ区天气预报服务器与互联网直连，未部署防火墙进行访问控制和逻辑隔离。
12	沙沟中广风电场	临沂	集控中心使用电信运营商网络监控所辖风场，集团集控中心交换机直连站内Ⅰ区远动、Ⅰ区风机监控、Ⅱ区风功率预测。 风功率预测系统中安全Ⅲ区天气预报服务器与互联网直连，未部署防火墙进行访问控制和逻辑隔离。
13	汤泉节能光伏电站	临沂	光功率预测系统中安全Ⅲ区天气预报服务器与互联网直连，未部署防火墙进行访问控制和逻辑隔离。
14	坦埠三峡光伏电站	临沂	生产控制大区与管理信息大区之间未部署物理隔离装置。
15	常路东大光伏电站	临沂	光功率预测外网服务器通过软件teamviwer进行远程运维。 光功率预测系统中安全Ⅲ区天气预报服务器与互联网直连，未部署防火墙进行访问控制和逻辑隔离。
16	费县熠峰光伏电站	临沂	光功率预测系统中安全Ⅲ区天气预报服务器与互联网直连，未部署防火墙进行访问控制和逻辑隔离。
17	朱田节能光伏电站	临沂	生产控制大区内部Ⅰ区和Ⅱ区之间未部署防火墙。 光功率预测系统中安全Ⅲ区天气预报服务器与互联网直连，未部署防火墙进行访问控制和逻辑隔离。
18	朝阳金城光伏电站	临沂	光功率外网服务器通过软件teamviwer进行远程运维。 生产控制大区内部Ⅰ区和Ⅱ区之间绕过防火墙。 光功率预测系统中安全Ⅲ区天气预报服务器与互联网直连，未部署防火墙进行访问控制和逻辑隔离。
19	库山国电风电场	日照	厂站监控系统与所属公司集控中心之间未部署隔离装置。



电力监控系统安全防护检查

按照《国家能源局关于开展电力系统安全防护专项检查的通知》要求，各级调度实现各调控机构、变电站、并网发电厂、配电网的全覆盖核查。本次专项检查中也发现了电力监控系统安全防护工作中存在的一些问题和薄弱环节。主要体现在：**体系结构、系统本体、全方位安全管理**等方面。

存在的主要问题和薄弱环节

启明星辰

体系结构安全

- 生产控制大区与互联网直连
- 纵向加密未全面完成
- 策略不严格（空闲端口，弱口令）

系统本体安全

- 未使用调度数字证书
- 移动介质接入管控不到位
- 主机口令、账号权限配置不当
- 主机安全加固不到位
- 变电站日志审计缺失

全方位安全管理

- 制度不健全，执行不严
- 运维管理执行不到位
- 等级保护存在未（漏）定级、定级不准和测评缺失
- 缺乏网络安全监测预警措施，无法全面监测

设计思路

智能变电站作为智能电网的核心支撑资源，针对暴露出安全防护问题，参考智能变电站一体化监控系统设计规范，提出**智能变电站一体化安全防护体系(Intelligent Substations Integrated Security Operations Center，IS-ISOC)**，重点在于及时发现各类网络安全风险以及非法指令、非法访问事件；实现智能变电站一体化安全防护和安全信息纵向贯通，实现网络安全闭环管理，全面提高电力监控系统网络安全防护的整体水平。

设计思路

目录

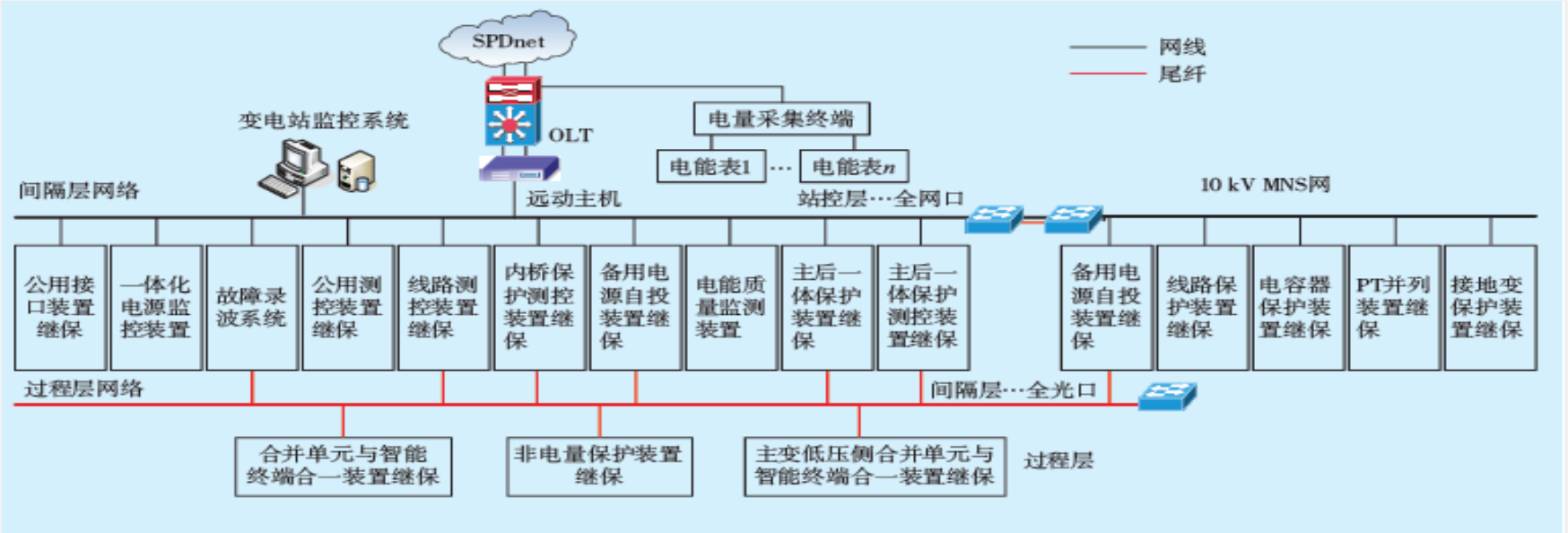
P01
IS-ISOC架构

P02
IS-ISOC 特色

P03
积累与能力支撑

智能变电站结构

根据国家电网公司《智能变电站技术导则》定义，智能化变电站是采用先进的传感器、信息、通信、控制、智能等技术，以一次设备参量数字化和标准化、规范化信息平台为基础，实现变电站实时全景监测、自动运行控制、与站外系统协同互动等功能，达到提高变电可靠性、优化资产利用率、减少人工干预、支撑电网安全运行、可再生能源“即插即退”等目标的变电站。物理结构上可划分为站控层、间隔层、过程层。



总体架构

启明星辰

展现层

深度持续监控　核心场景预警　全站风险评估　全局可视化

表示逻辑层

资产管理　事件管理　通信报文分析　告警管理

仪表板　基线管理　报表管理　自身维护管理

业务逻辑层

功能组件

安全事件分析　静态基线分析　动态基线分析　业务健康建模　业务指标分析

操作行为审计　态势评估与预测　业务流量分析　安全事件回溯　多维数据分析

基础组件

搜索引擎

关联分析引擎

事件处理引擎

告警服务　报表服务　日志服务

数访问取服务

数据存取服务

存储节点　存储节点　存储节点

数据采集层

流采集　事件采集　报文采集　终端采集　配置采集

数据源

网络设备

安全设备

IBM WebSphere

中间件

主机

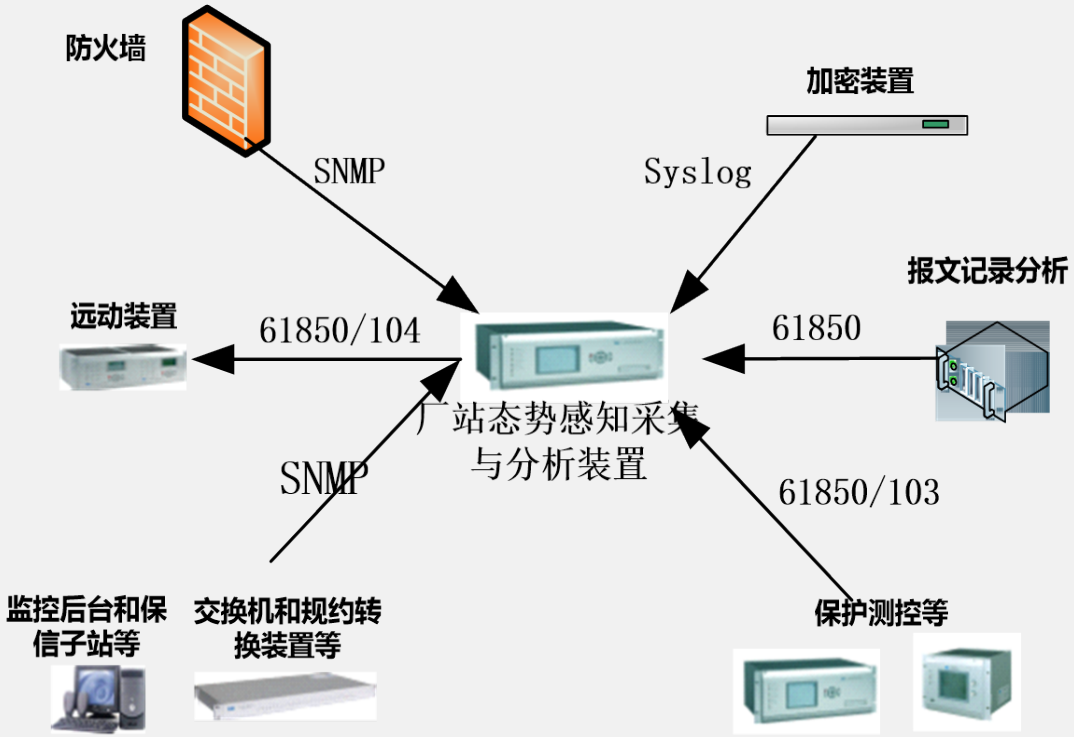
数据库

平台数据接口

数据采集

变电站数据采集对象

对象类型	对象名称
二次设备	远动装置
	保护装置
	监控后台
	测控装置
	规约转换装置
	站控层交换机
	防火墙
	纵向加密装置
网络数据	网络拓扑数据
	网络报文数据



深度持续监控

– 监控核心应用的执行过程：远方遥控，监测遥控命令在各个节点的执行情况，关联执行结果信息，展示整个执行过程的情况；

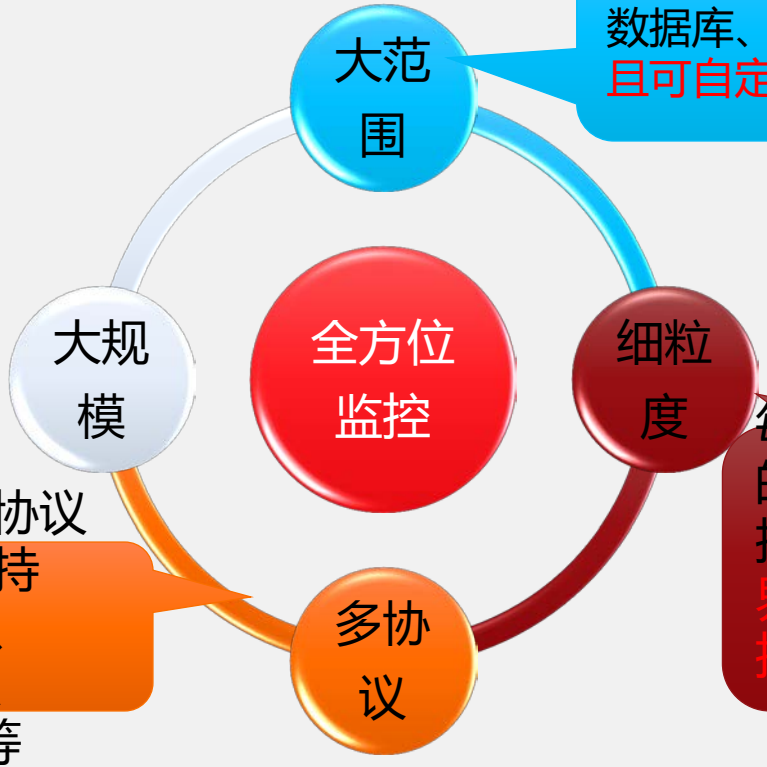
– 流量监控：流量大小、流量方向、流量路径

– 基础设施可用性监控：CPU、内存、端口利用率预警；

– 资产增减监控：资产指纹识别、多网络节点资产增减进行监测；

– 脆弱性监控：资产弱口令、资产漏洞利用预警。

深度持续监控-运行监控



监控范围涵盖网络设备、安全设备、存储、主机、数据库、中间件、应用，且可自定义监控类型。

采用分布式监控技术，支持对上千个节点的并行监控

每种设备都有丰富的监控指标，并支持扩展，支持通过界面进行SNMP监控指标的自定义

采用多种网络协议实施监控，支持SNMP、SSH、ODBC、JMX、WebService等

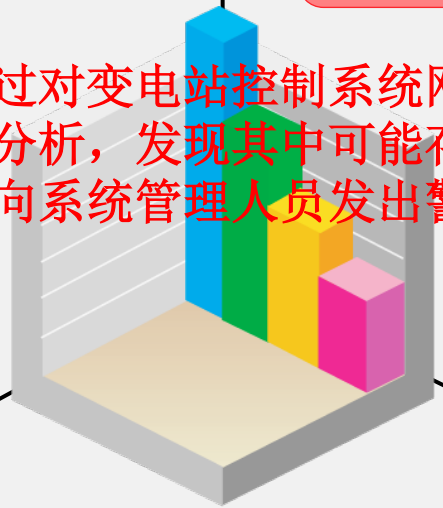
深度持续监控-网络行为监控

以时间、空间、特征为基础，对网络流量进行多维度、细粒度的分析，并通过形象地的图表曲线帮助客户实现流量行为的可视化

特征维

特征：总流量、进流量、出流量、流量的协议/应用组成

空间：全网、路由设备、路由设备组、路由器接口组、服务器流量群组、主机、自治域



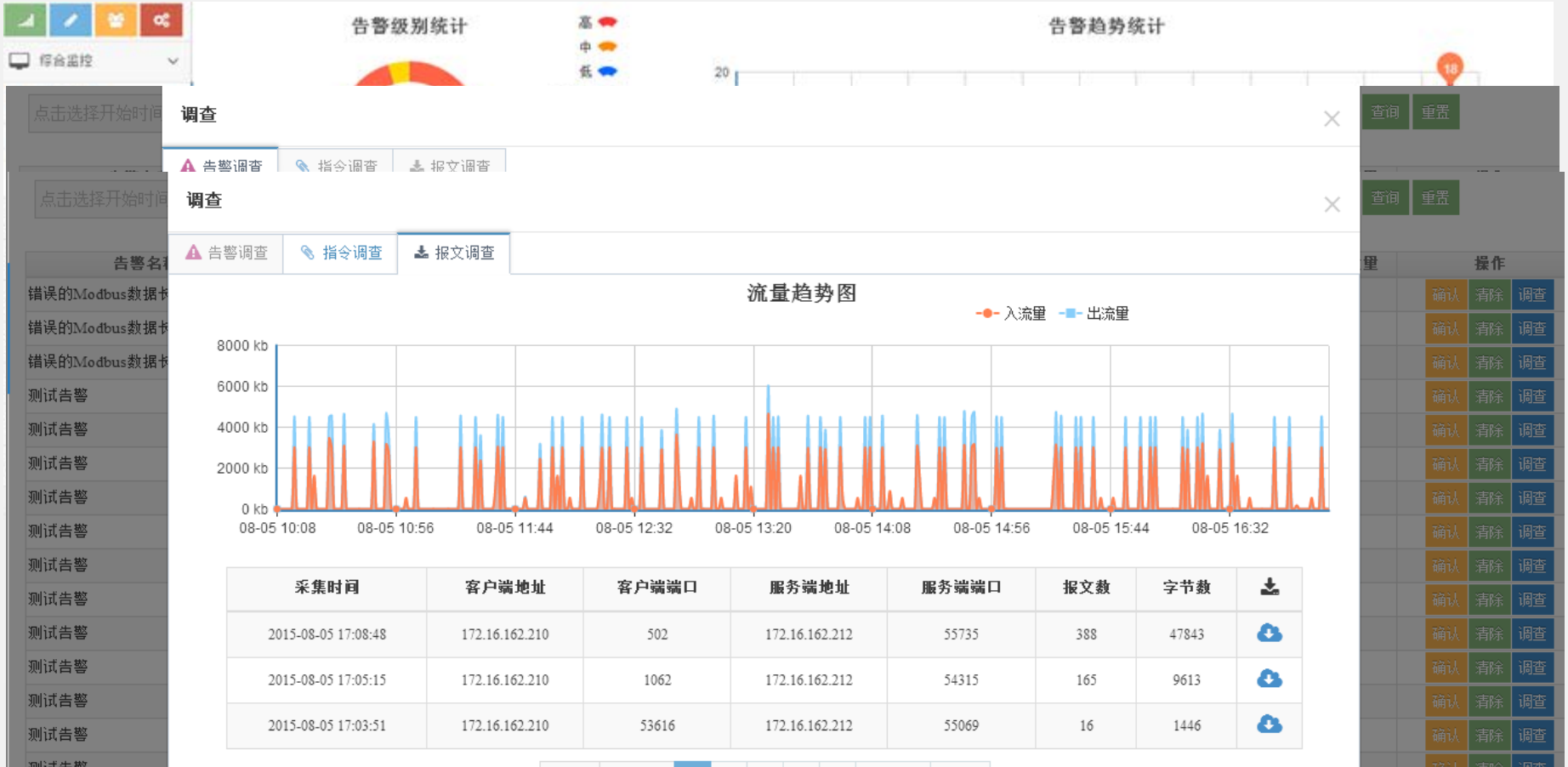
通过对变电站控制系统网络中的流量进行实时分析，发现其中可能存在的恶意入侵行为，并向系统管理人员发出警报

时间：分钟、小时、天、月；实时、历史

空间维

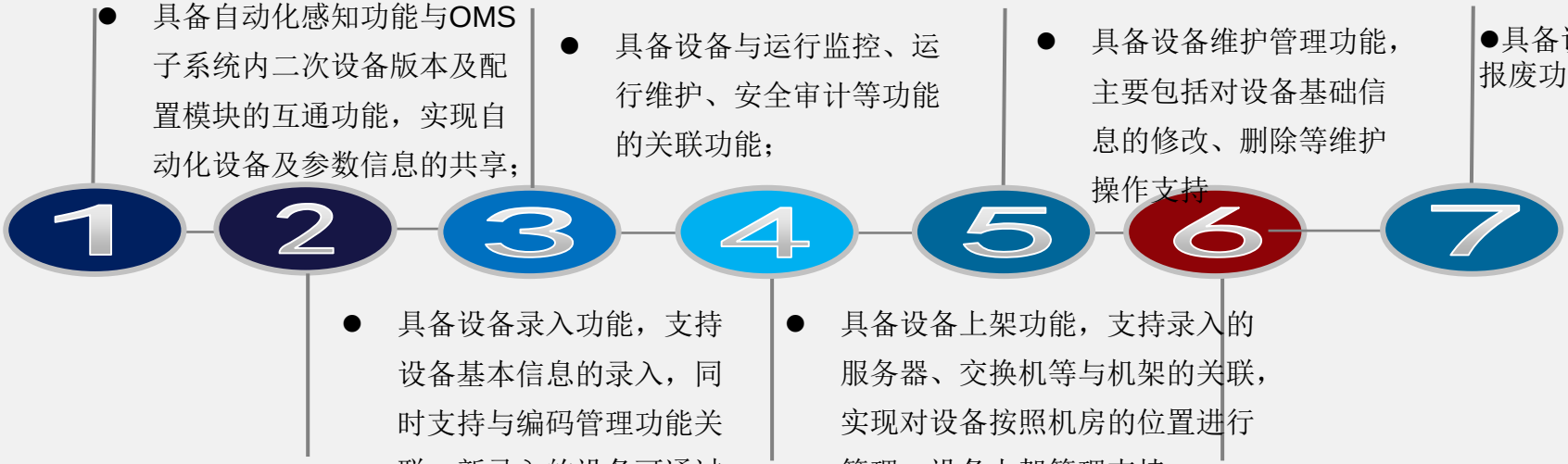
时间维

深度持续监控-网络行为监控



深度持续监控-资产指纹监控

通过主动发现、导入或创建的方式来识别和梳理调度数据网中要被防护的资产及业务对象。所获得并维护的被防护对象信息将在整个态势分析呈现过程中，被其他维度的感知所利用，成为面向安全对象安全态势分析的基础。信息来源有三个方面：①通过自动发现、②手工录入、③与OMS系统接口。



深度持续监控-脆弱性监控

资产弱点：包括了漏洞脆弱性和配置脆弱性两个部分

脆弱性监控集成了配置核查的结果，称为“配置脆弱性”，并与漏扫结果（“漏洞脆弱性”）一并参与“综合脆弱性”计算

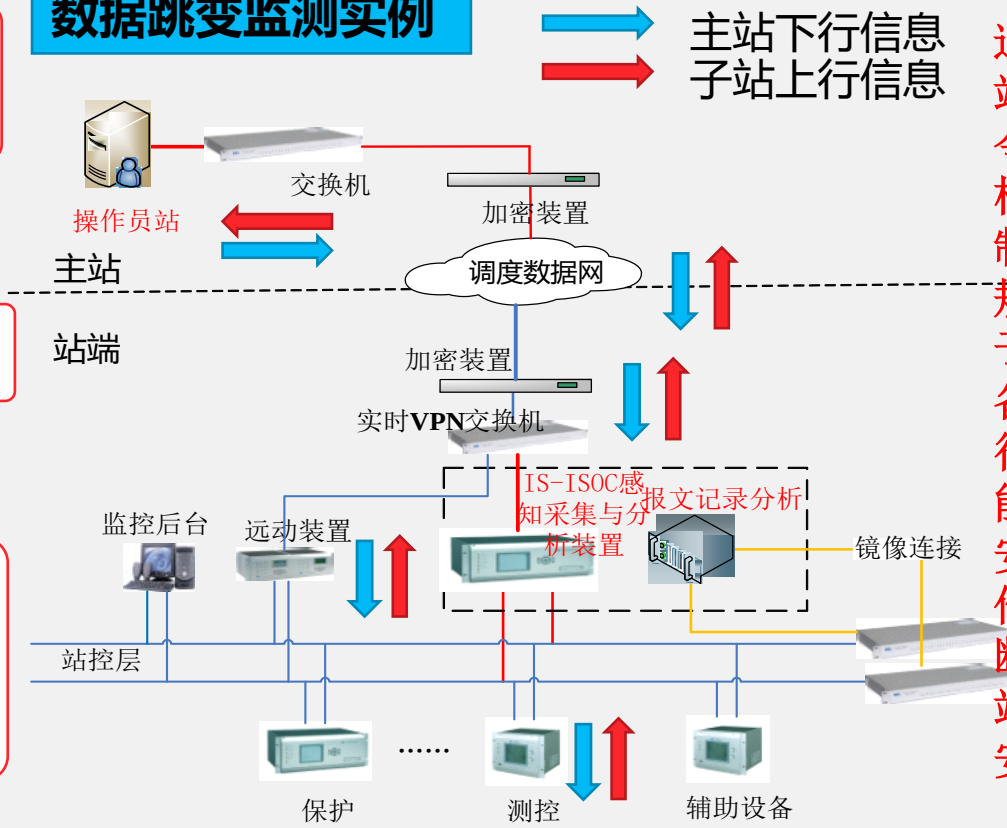
核心监控场景：指令异常

厂站端装置对二次设备收发报文情况进行采集

分析并可视化获得报文实际传输路径

针对信息点及其传输路径进行跟踪，进而实现“数据跳变”、远动“遥控失败”的等应用

数据跳变监测实例



通过构建变电站控制系统指令进行分析，构建变电站控制系统操作合规性模型，对于网络中的设备操作行为进行分析，对可能危及变电站安全运行的操作行为及时阻断，保障变电站控制系统的安全运行

核心场景预警：安全配置

登录/运行脚本

获取配置信息

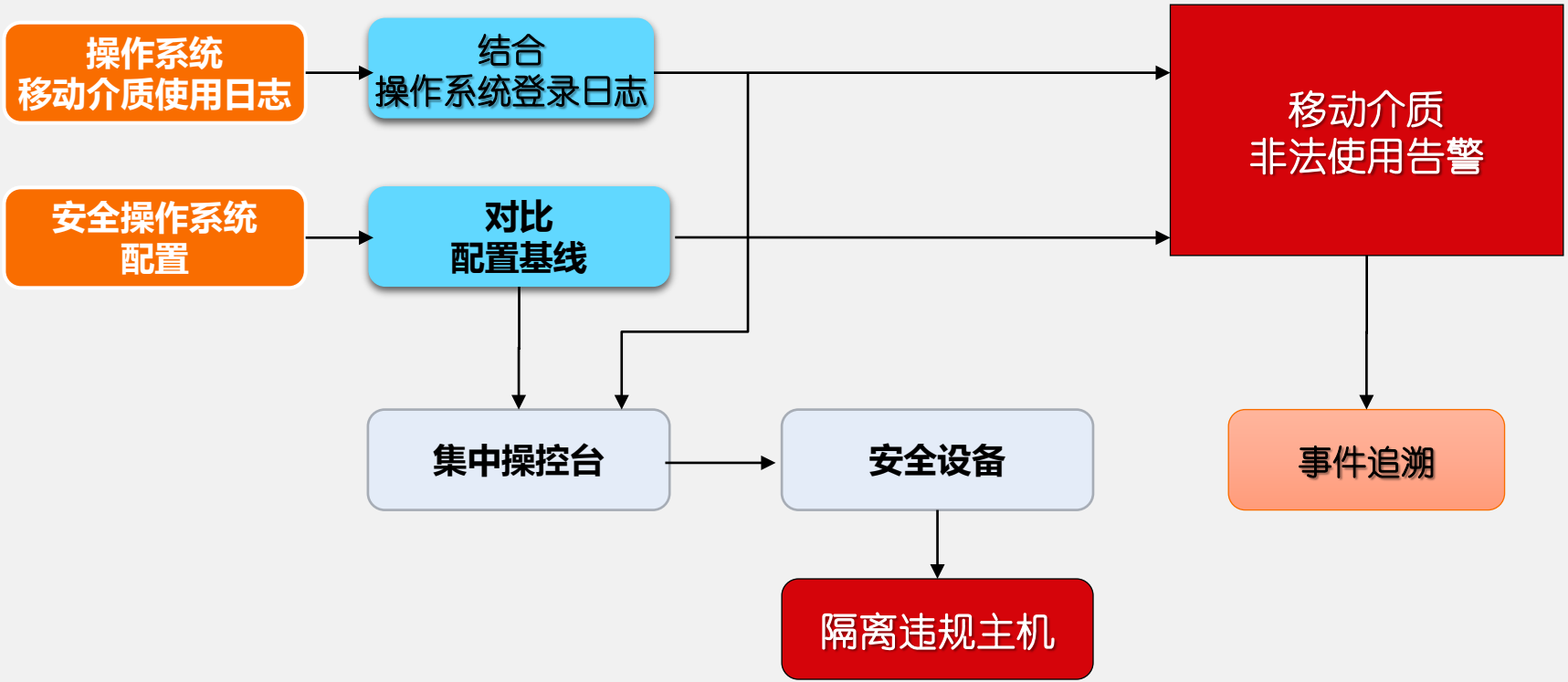
设备台账
安全配置基线库

基线核查

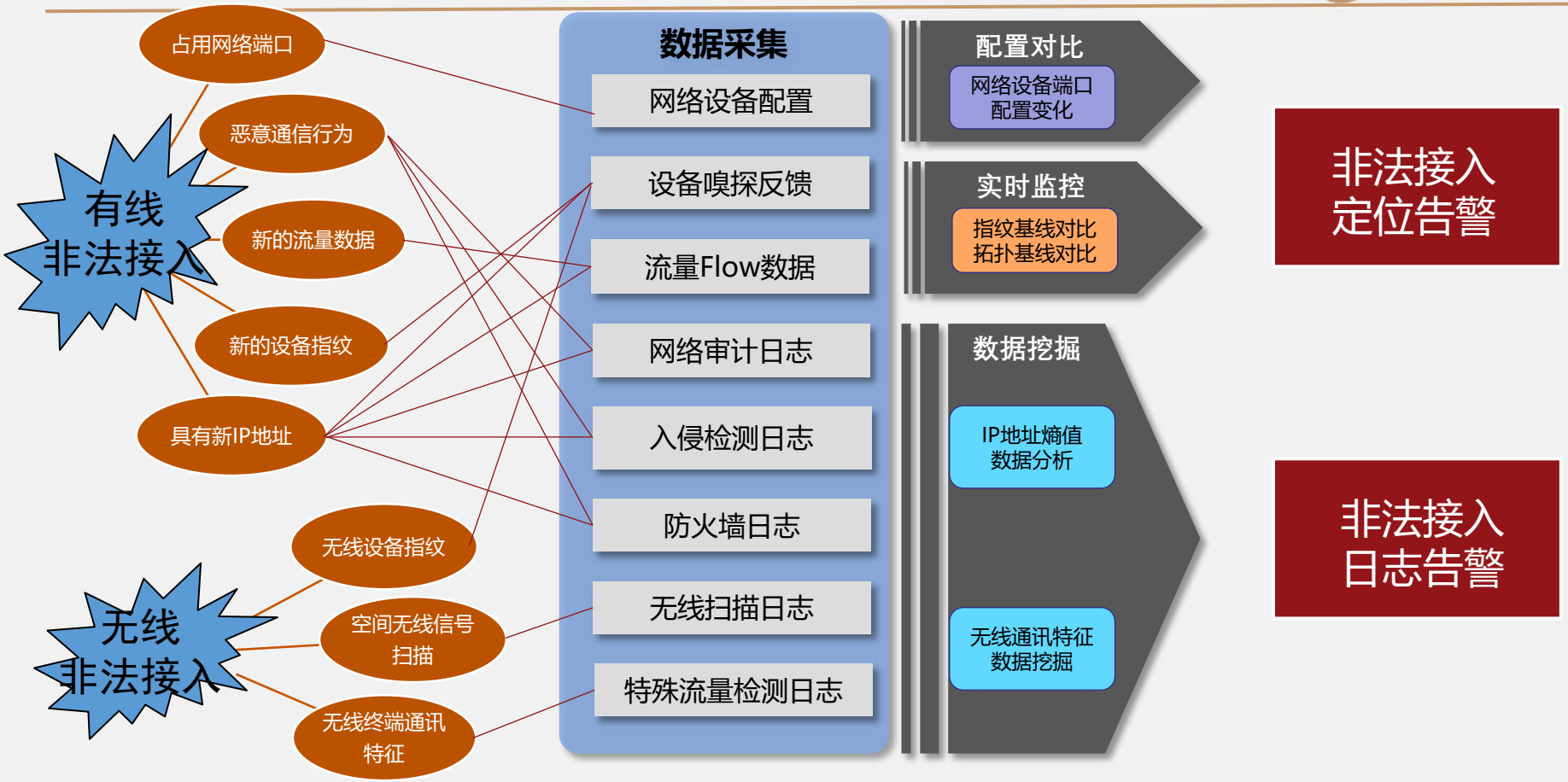
模拟人工核查的过程，围绕PDCA建模：登录信息获取→登录设备（P）→执行脚本→获得结果（D）→和要求值对比（C）→加固方案（A）→复查（P）

对于变电站控制网络中的设备状态情况进行在线监测，及时发现网络中出现的设备新增、设备配置变更等行为，确保变电站控制系统设备安全可控

核心场景预警：移动介质


操作系统
移动介质使用日志
结合
操作系统登录日志
移动介质
非法使用告警
安全操作系统
配置
对比
配置基线
集中操控台
安全设备
事件追溯
隔离违规主机

核心监控场景：非法接入


占用网络端口
恶意通信行为
有线
非法接入
新的流量数据
新的设备指纹
具有新IP地址
无线设备指纹
无线
非法接入
空间无线信号
扫描
无线终端通讯
特征
数据采集
网络设备配置
设备嗅探反馈
流量Flow数据
网络审计日志
入侵检测日志
防火墙日志
无线扫描日志
特殊流量检测日志
配置对比
网络设备端口
配置变化
实时监控
指纹基线对比
拓扑基线对比
数据挖掘
IP地址熵值
数据分析
无线通讯特征
数据挖掘
非法接入
定位告警
非法接入
日志告警

全站风险评估

一级指标

总体

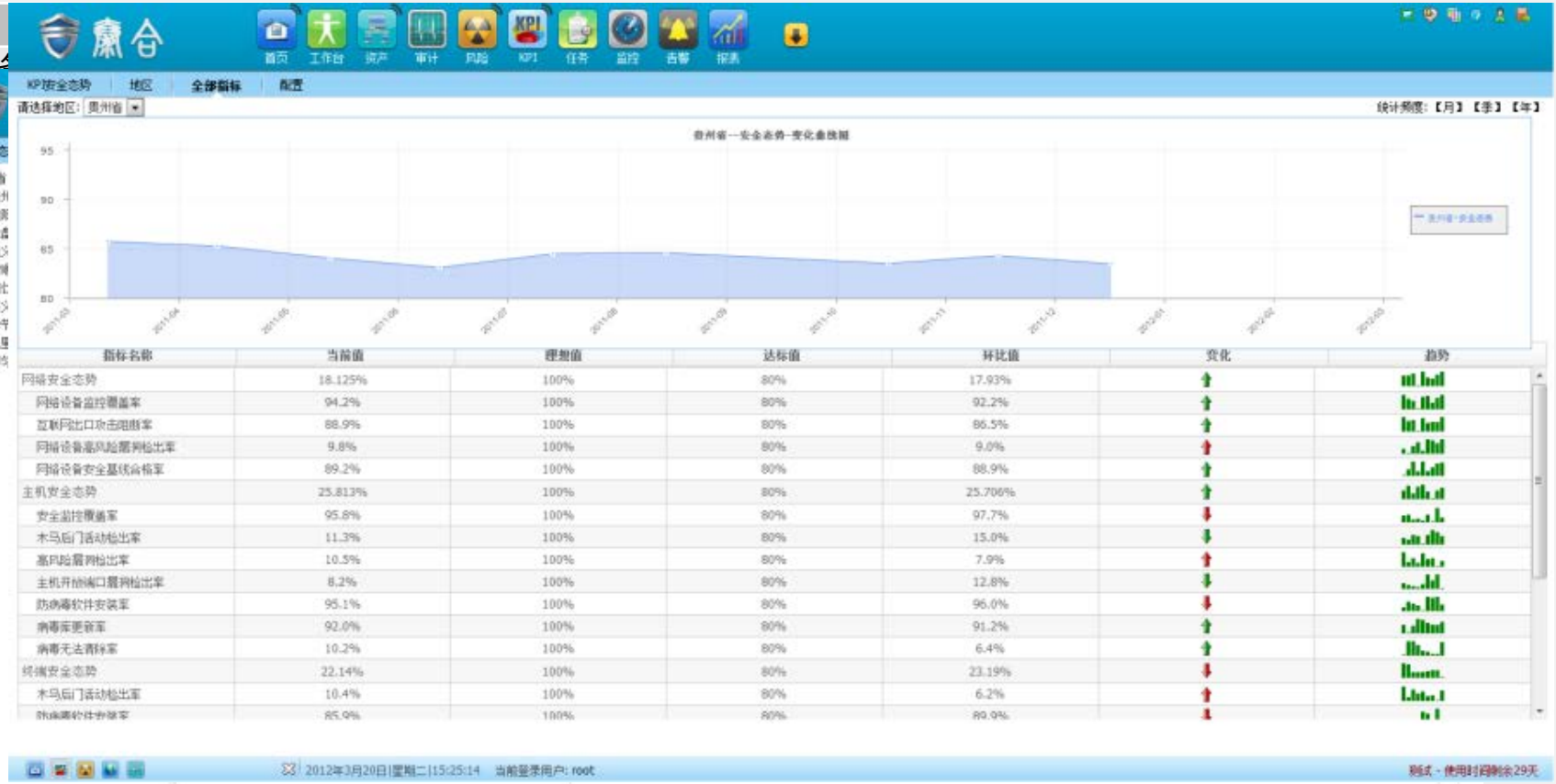
结

设

应

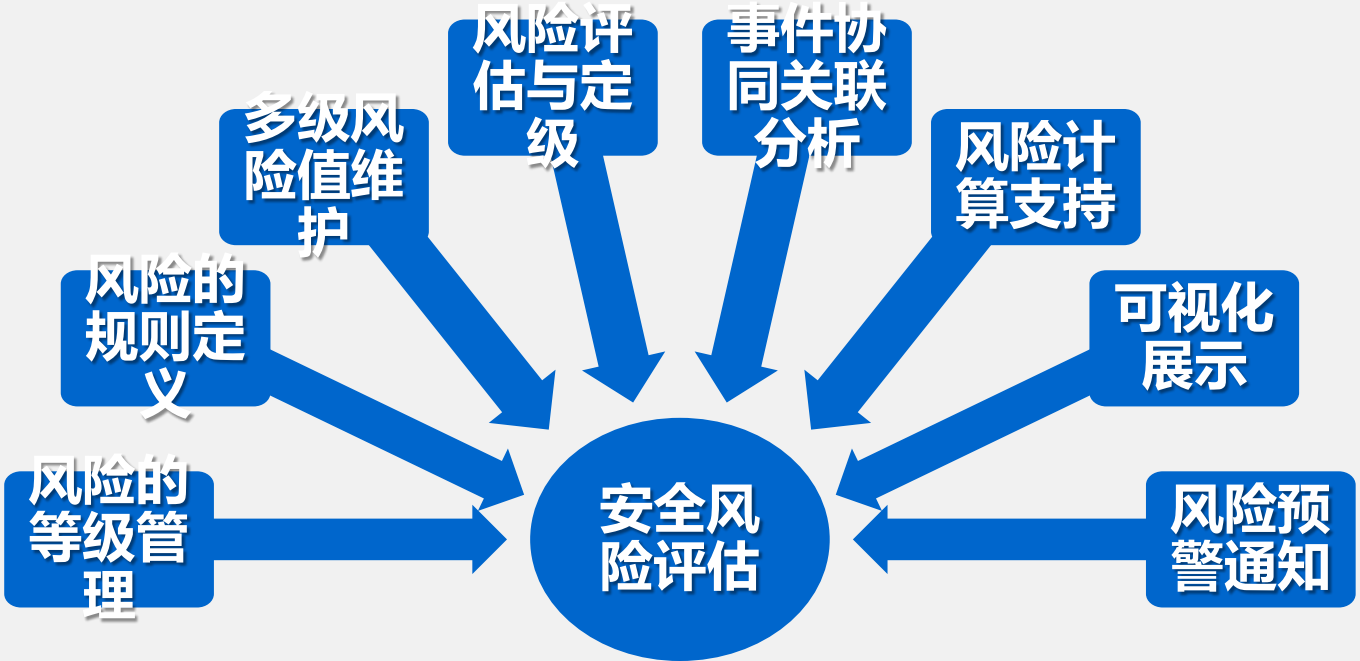
数

安



全站风险评估

风险评估是从风险的角度来衡量电力监控系统的安全态势，综合资产价值、安全属性、脆弱性、攻击威胁等风险要素，基于风险模块内置的风险计算模型，进行全站、各安全域及各业务系统的风险量化评估和风险赋值。



目录

P01
IS-ISOC架构

P02
IS-ISOC 特色

P03
积累与能力支撑

IS-ISOC 特色列表

面向厂站端的就地分析与存储能力

面向高实时性的海量异构数据融合处理能力

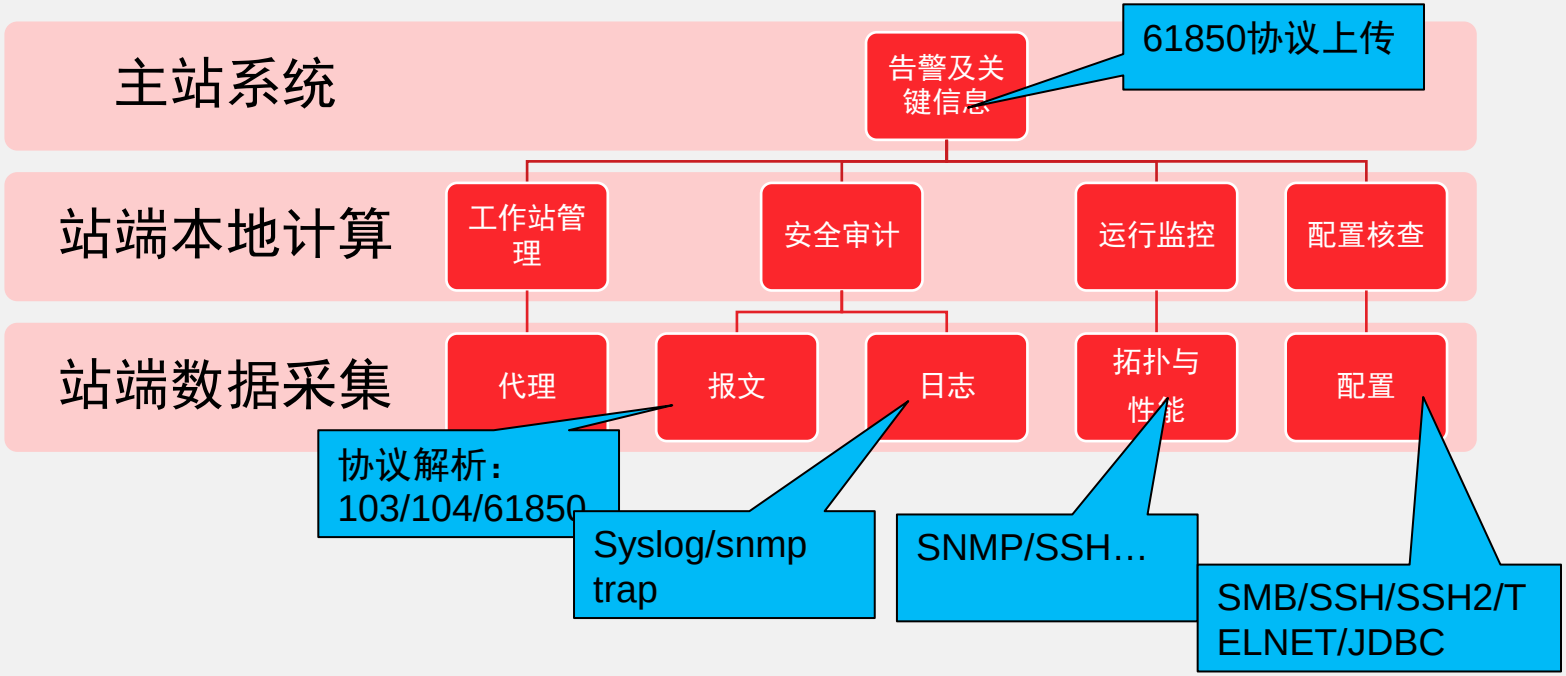
面向规则关联的安全事件智能分析能力

面向业务健康度的风险评估能力

面向日常运维的一体化合规平台

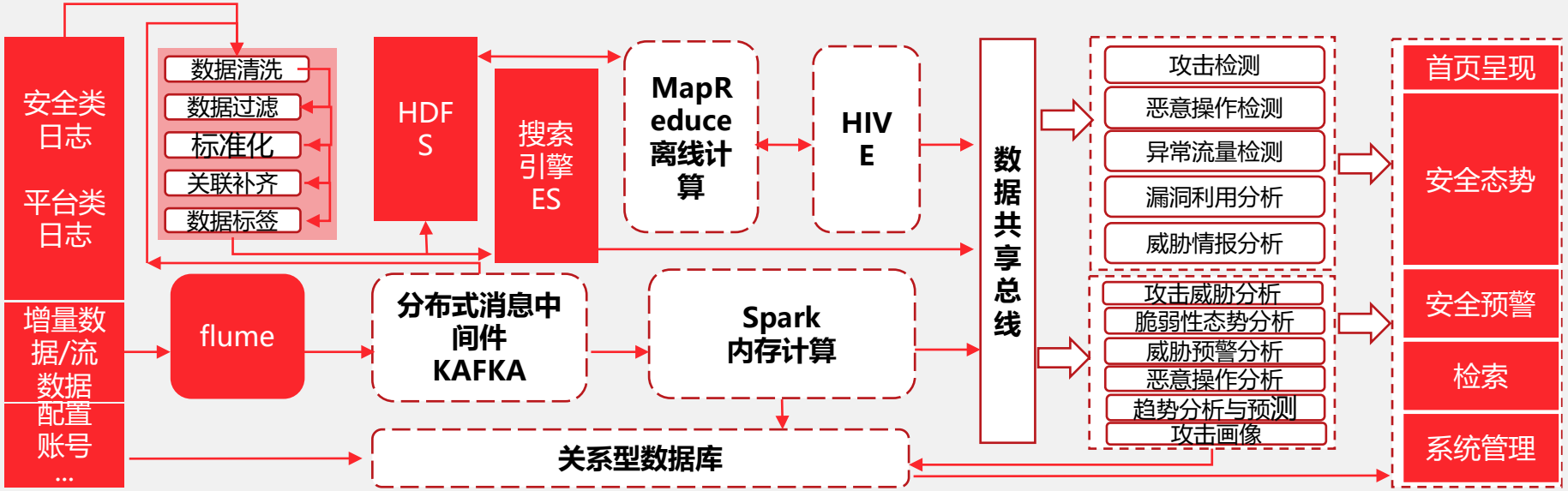
特色1：面向厂站端的就地分析与存储能力

由于调度数据网带宽有限，要求厂站端态势感知装置不仅采集相关数据，同时具有一定能力的就地计算分析能力，以便将分析结果传输到上级主站协同操控。**具备实现高性就地分析计算能力，通过实时数据时间精度在毫秒级；业务规则文件召唤满足响应时间小于1min；分析结果数据通过OSB封装后与主站协同。硬盘存储空间≥500G；具备《网络安全法》日志存储6个月要求条件。**



特色2：面向高实时性的海量异构数据融合处理能力

电力监控系统高实时性特点，要求其网络安全态势感知采集的海量异构数据（运行监测数据和日志数据），必须采用流式数据处理方式在不同的时间窗口内完成融合处理任务。具备：当前主流的分布式大数据存储架构，并经过面向安全大数据分析过程的数据质量优化，形成自有的CupidDB数据库架构，可实现海量安全信息的**高效处理和并行扩展**。同时根据不同的数据结构和信息处理特点，还具备处理非结构化数据的情境数据库以及与用户业务信息相关的基础信息处理库，以及具有高性能流式实时分析的内存数据库。



特色3：面向规则关联的安全事件智能分析能力

智能化的安全事件分析主要透过智能化的安全事件关联分析来体现。事件关联是指找出大量事件中存在的关系，并从这些大量事件中抽取出真正重要的少量事件。借助先进的智能事件关联分析引擎，系统能够实时不间断地对所有范式化后的日志流进行安全事件关联分析。系统为分析师提供了三种事件关联分析技术，分别是：基于规则的关联分析、基于情境的关联分析和基于行为的关联分析。

特色3：面向规则关联的安全事件智能分析能力

监视 → 统计 → 查询 → 追溯 → 处置 → 报告

Syslog
Trap
OPSEC
File
WMI
FTP
ODBC
XML
…

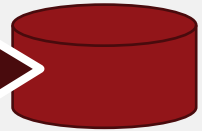
异构海量日志采集 → 日志范式化与分类 → 事件过滤归并 → 关联分析 → 告警

领导
- 掌握整体安全态势
- 审核等保与内控
- 评估安全有效性

安全经理
- 建立审计策略
- 制定任务计划
- 出具日志审计报告

审计人员
- 采集和存储日志
- 日志审计与分析
- 任务处理与告警响应

加密 → 存储 → 压缩 → 备份 → 恢复



特色3：面向规则关联的安全事件能力分析能力

逻辑关联

基于逻辑表达式的规则

目的IP=XX &（ 目的端口=80 || 目的端口=8080 ）

统计关联

基于统计条件的规则

一分钟内某个源IP连续登录某个目的IP失败的次数大于6次

资产关联

事件与资产属性关联

针对内网的目的IP事件，且这些目的IP的操作系统是Windos XP

弱点关联

事件与资产弱点关联

针对某些目的IP攻击事件，且这些目的IP具有某个特定弱点

威胁情报关联

事件与威胁情报关联

来自某些源IP攻击事件，且这些源IP被威胁情报标识为有组织黑客所掌握的恶意IP

拓扑关联

事件与网络拓扑关联

来自某些IP的性能故障事件发生时间存在先后，在网络拓扑上的映射符合故障的传播特性

网络告警关联

事件与网络告警关联

IDS报告某个IP正在遭受攻击且该IP的CPU利用率及端口流量告警

周期性行为

同比分析

与以往每天早上9点钟相比，今天早上9点的防火墙阻断次数偏高

行为预测

环比分析

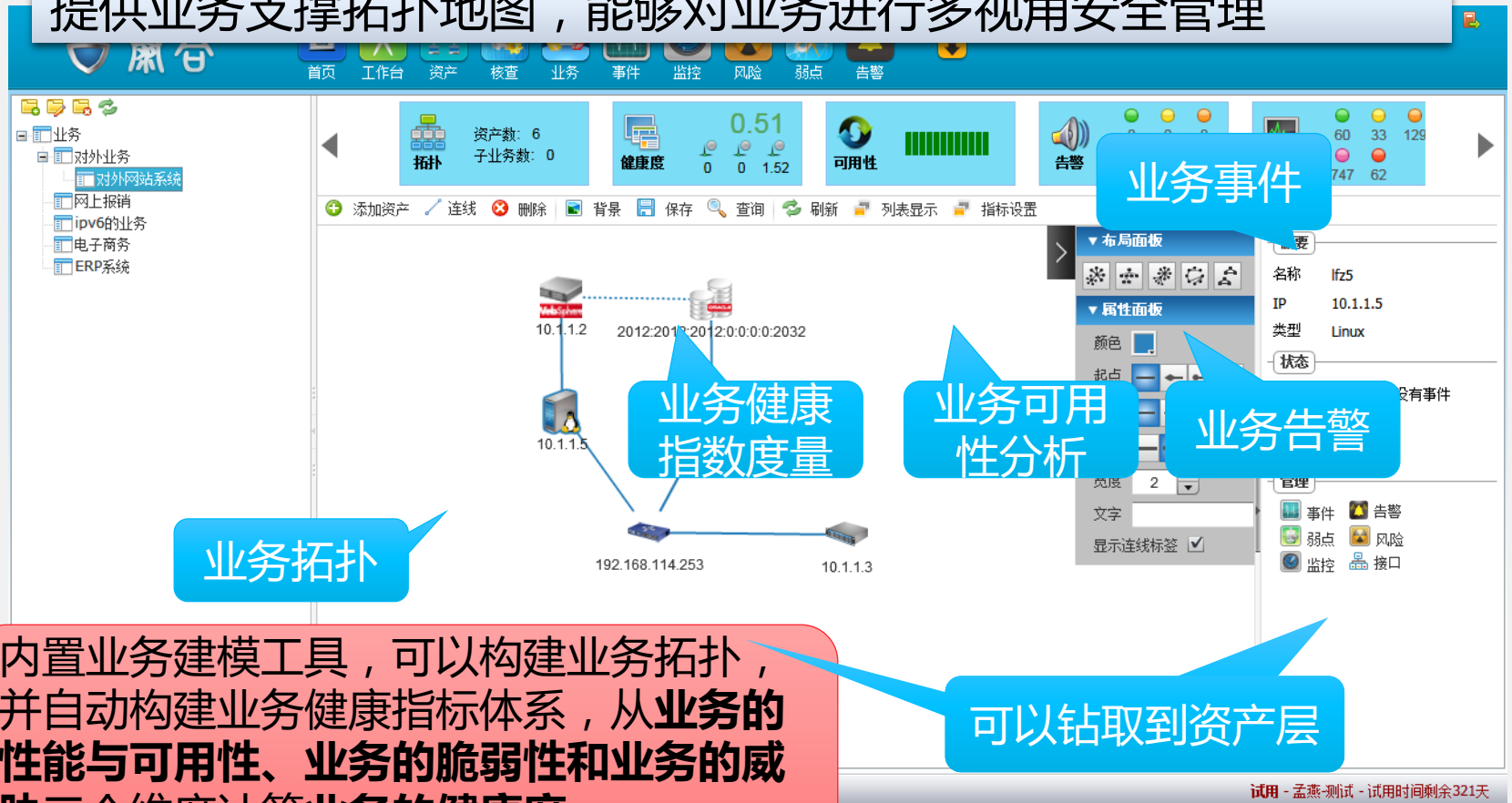
今天的IDS高等级告警次数与根据之前10天的走势做出的预测相比偏高

特色3：面向规则关联的安全事件分析能力

- 发现疑似感染蠕虫的主机
- 多设备关联的典型网络攻击
- 发现过度报警的监控设备
- 绕过堡垒机的远程控制活动
- 溢出攻击导致的服务异常

特色4：面向业务健康度的安全风险评估能力

提供业务支撑拓扑地图，能够对业务进行多视角安全管理



内置业务建模工具，可以构建业务拓扑，并自动构建业务健康指标体系，从**业务的性能与可用性、业务的脆弱性和业务的威**

可以钻取到资产层

特色4：面向业务健康度的安全风险评估能力

特色5：面向日常运维的一体化合规平台

特色5：面向日常运维的一体化合规平台

方面	类	第一级	第二级	第三级	第四级
技术要求	物理安全			•物理安全监控与告警	•物理安全监控与告警
	网络安全	•拓扑管理 √	•拓扑管理 •设备和应用监控 •IP地址管理 •安全审计 √	•拓扑管理 •设备和应用监控 •IP地址管理 •安全审计 √ •流量监控 •地址欺骗监控	•拓扑管理 •设备和应用监控 •IP地址管理 •安全审计 •流量监控 √ •地址欺骗监控
	主机安全		•安全审计 √	•安全审计 •资源监控 √	•安全审计 •资源监控 √
	应用安全		•安全审计	•安全审计 •资源监控	•安全审计 •资源监控
	数据安全	•信息完整性保护	•信息完整性保护 √	•信息完整性保护 √	•信息完整性保护 √
管理要求	系统运维管理	•资产管理 √	•资产管理 •设备管理 •网络监控 •设备配置信息监控 √ •日志审计 •告警事件存储	•资产管理 •物理环境监控 •设备管理 •网络监控 •设备配置信息监控 √ •日志审计 •告警事件统计 •安全管理中心 •权限管理	•资产管理 •物理环境监控 •设备管理 •网络监控 •设备和应用配置信息监控 •日志审计 √ •告警事件统计 •安全管理中心 •权限管理

目录

P01
IS-ISOC架构

P02
IS-ISOC 特色

P03
积累与能力支撑

公司介绍

启明星辰信息技术集团总部位于北京市中关村软件园启明星辰大厦，公司员工3150人，技术团队千人，在全国各省、市、自治区设立分支机构六十多个，拥有覆盖全国渠道体系和技术支持中心。公司于2010年6月23日在深圳中小板挂牌上市。

2017年9月7日，工信部公布2017年(第16届)中国软件业务收入前百家企业。启明星辰信息技术集团股份有限公司成为百强榜单中唯一一家的民营专业安全厂商。


启明星辰安全架构
安全系统集成
涉密局域网
安全系统集成
涉密广域网
安全系统集成
涉密专网
安全系统集成
办公内网
安全系统集成
骨干网
安全系统集成
安全产品
威胁检测类
天阗入侵检测与管理系统
天阗威胁检测与智能分析系统
天清入侵防御系统
安全工具类
天镜脆弱性扫描与管理系统
安星远程安全检查服务
安全网关类
天清汉马一体化安全网关
天清汉马防火墙
应用监管类
天玥合规性审计系统
天玥互联网审计系统
天珣内网安全管理系统
安全管理平台
ZSOC 安全域管理平台
4ASOC 4A 平台
ASOC 综合审计平台
MSOC 监控管理平台
TSOC 综合信息安全运营中心
安全服务
PSS 安全管理咨询服务
MSS 安全管理监控服务
PSS 安全风险评估服务
PSS 应用系统安全评估服务
CSS 客户化安全服务

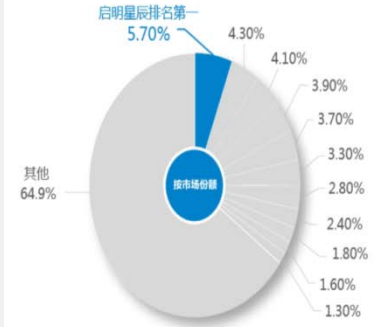
产品能力支撑

启明星辰

CCID：2016启明星辰集团继续领跑中国网络信息安全市场

根据《2016-2017年中国网络信息安全市场研究年度报告》显示，2016年中国网络信息安全市场规模达到336.2亿元，启明星辰集团以5.7%的市场份额，排名第一，并在多个细分市场排名中名列前茅。

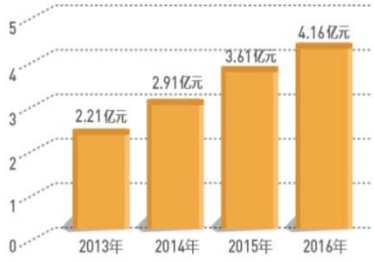
自2012年起，启明星辰集团已连续五年领跑中国网络信息安全市场。



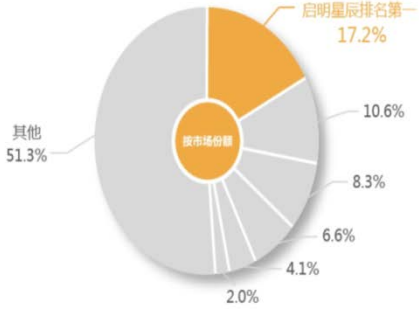
2016年中国网络信息安全产品品牌市场结构

IDS/IPS产品连续15年市场排名第一

2016年IDS/IPS产品市场规模达到24.2亿元，启明星辰集团以17.2%的市场份额，排名第一.



启明星辰IDS/IPS产品市场规模年度比（2013年—2016年）

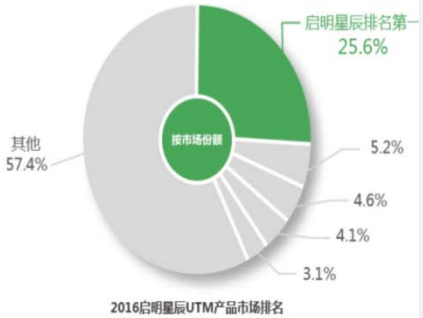


2016启明星辰IDS/IPS产品市场排名

UTM产品连续10年排名第一

2016年UTM产品市场规模达到19.5亿元，启明星辰集团以25.6%的市场份额，排名第一.

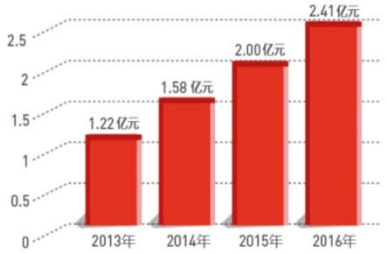
启明星辰UTM产品市场规模年度比（2013年—2016年）



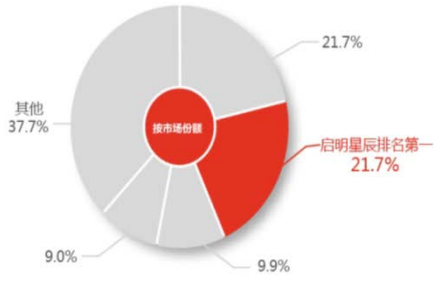
2016启明星辰UTM产品市场排名

安全管理平台（SOC）产品连续9年市场排名第一

2016年安全管理平台产品市场规模达到11.1亿元，启明星辰集团以21.7%的市场份额，排名第一.



启明星辰安全管理平台产品市场规模年度比（2013年—2016年）



2016启明星辰安全管理平台产品市场排名

产品能力支撑

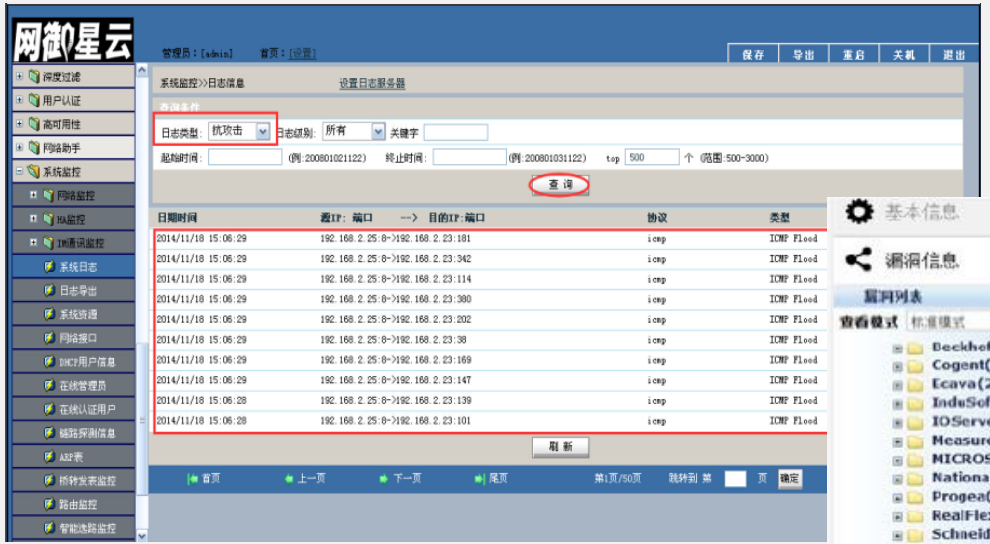
工控安全	漏洞扫描系统	安全管理系统	异常检测系统	运维审计系统	防火墙系统	网闸系统	网络流秩序分析诊断系统
云安全	云端防火墙	云端入侵检测	云端入侵防御	云端WEB应用防护	云端数据库审计	云端防病毒	
数据安全	数据防泄密	数据库审计	分布式数据库	大数据安全分析			
应用安全	未知威胁检测	WEB应用防护	应用安全交付	安全数据交换	视频安全接入	电子签章系统	
主机安全	终端安全管理	设备性能监控	内网安全管理	云子可信系统			
网络安全	防火墙	综合威胁管理	网络准入控制	VPN	防病毒网关	安全隔离交换	单向光闸	无线安全防护	异常流量监测	入侵防御系统
物理安全	电磁屏蔽机柜	电磁屏蔽机桌	低泄射电脑	电磁屏蔽机房	电磁屏蔽帐篷	保密会议室	微波防护			

安全管理

- 网络安全审计
- 运维审计系统
- 安全域流监控
- 互联网行为管控
- 入侵检测系统
- 脆弱性扫描
- 安全配置核查
- 安全运营管理
- 网络行为分析

产品能力支撑

- 集团成功申请国家发改委工业应用软件漏洞扫描产品和工业防火墙产业化课题，通过了测试审核，成功列入2013年信息安全专项。



服务能力支撑


安全评估加固类服务
漏洞扫描
安全配置审计
技术安全评估
信息安全风险评估
渗透测试
信息安全管理评估
安全加固
安全检查
等级保护类服务
等级保护级别定咨
等级保护咨询服务
等级保护理咨询
等级保护差距评估
等级保护建设咨询
应用安全类服务
应用开发安全咨询
代码安全咨询
应用安全测试服务
应用安全咨询
应用安全评估
安全咨询类服务
安全管理制度咨询
安全规划咨询
ISMS安全管理体系
安全资质服务
ISO27001认证咨询
安全防护体系设计咨询
SOX安全规范咨询
行业合规审计咨询
安全域防护咨询
安全审计咨询类服务
PCI合规审计咨询
日志审计服务
综合类类服务
软课题研究咨询
技术应用研究咨询
定制安全服务
综合安全服务
组合安全服务
安全技术专项培训
行业化安全服务
电子银行评估咨询
银行其他业务合规咨询
证券业务合规服务
其他行业
银行科技风险管理评估
银行科技风险管理咨询
中国电信合规服务
中国移动合规服务
新型安全服务模式
信息泄露监测
数据安全治理咨询
异常流量过滤
产品租赁与服务合
在线安全测试
在线评估服务
在线威胁检测服务
新兴服务领域
云计算安全服务
工控系统安全评估
工控系统安全管理咨询
工控系统安全测试
物联网安全服务

资质能力支撑

启明星辰

企业荣誉(700余项)

- 连续四次入选“国家级网络安全应急服务支撑单位”
- 中关村国家自主创新示范区“十百千工程” 重点培育企业
- “最佳企业安全品牌排行榜”第一名
- 北京软件和信息服务业25年突出贡献企业奖
- 国家高技术产业化示范工程
- 促进国家安全科学技术进步工作突出贡献集体奖
- 中关村国家自主创新示范区核心区优秀博士后工作站分站
- 中国信息安全值得信赖品牌
- 最佳信息化安全服务商
- ……

企业资质（50余项）

- 国家认定企业技术中心
- 信息系统集成一级资质
- 国家火炬计划重点高新技术企业
- 计算机信息系统集成资质（二级）
- 涉及国家秘密的计算机信息系统集成资质（甲级）
- 装备承制单位注册证书
- 国家规划布局内重点软件企业
- 国家信息安全认证信息安全服务资质
- 信息安全应急处理服务资质（一级）
- 信息安全风险评估服务资质（一级）
- ……

具有安全厂商中最全、最高级别的资质

科技创新能力支撑

中国电力科学技术奖

获奖证书

奖项名称：中国电力科学技术进步奖

获奖项目：电网信息安全主动防御关键技术与自主可控装备

获奖等级：一等

获 奖 者：启明星辰信息技术集团股份有限公司

奖励年度：2015年

发证机构：中国电机工程学会
中国电力科学技术奖励工作办公室

证书号：2015-J-1-05-D04

辽宁省科学技术奖励

证 书

项目名称：大型供电企业综合信息安全平台建设及关键技术研究

奖励等级：一等

获 奖 者：北京启明星辰信息技术股份有限公司

证 书 号：2015J-1-09-06

为表彰辽宁省科学技术奖获得者，特颁发此证书。

辽宁省科学技术奖励委员会
二〇一五年十二月

荣誉证书

北京市科学技术奖

为表彰在推动科学技术进步、对首都经济建设和社会发展作出贡献的集体和个人，特颁此证，以资鼓励。

获奖项目：面向电力信息系统的安全可控性仿真验证体系研究与应用

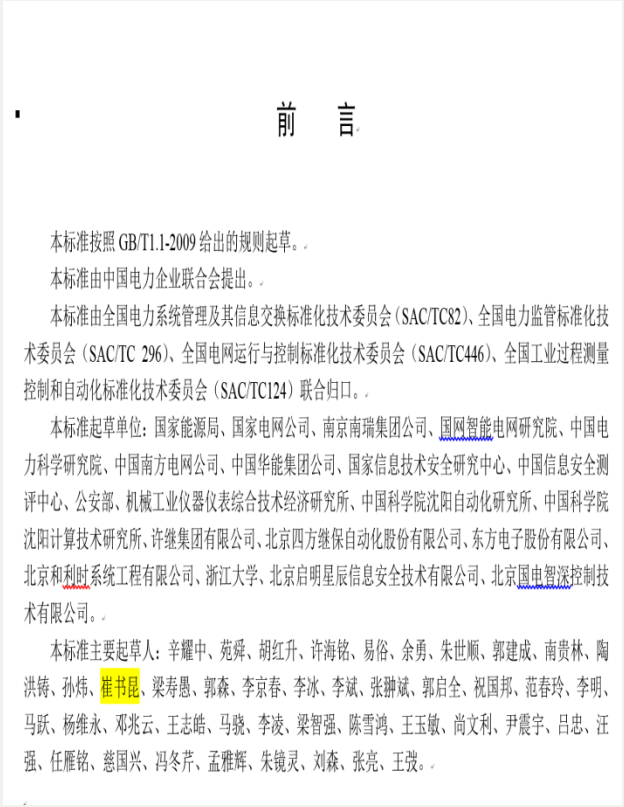
获奖等级：贰等奖

获奖单位：国网信息通信有限公司、中国科学院高能物理研究所、中国电力科学研究院、北京启明星辰信息安全技术有限公司、全球能源互联网研究院

NO. 2016 计-2-001

二〇一六年十一月

科技创新能力支撑



前　言

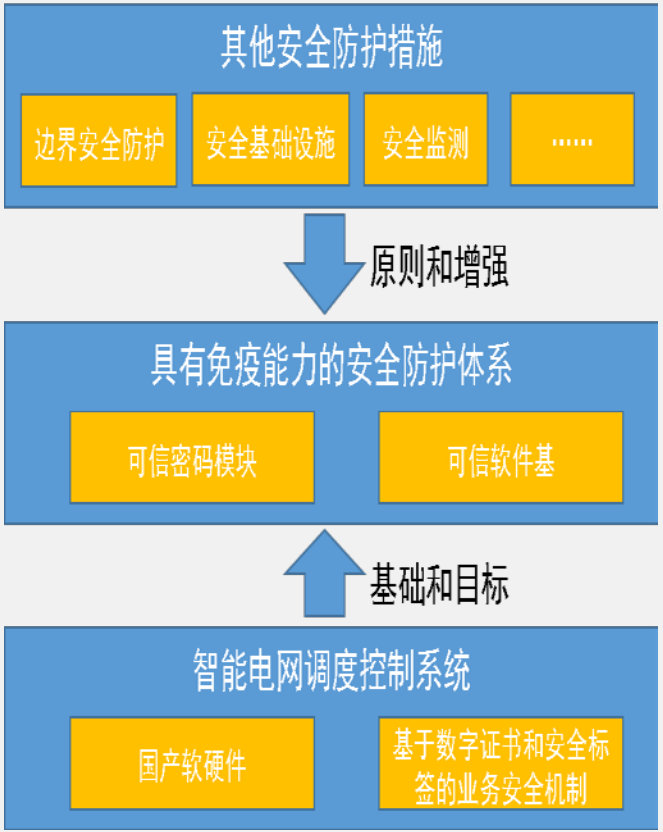
本标准按照 GB/T1.1-2009 给出的规则起草。

本标准由中国电力企业联合会提出。

本标准由全国电力系统管理及其信息交换标准化技术委员会（SAC/TC82）、全国电力监管标准化技术委员会（SAC/TC 296）、全国电网运行与控制标准化技术委员会（SAC/TC446）、全国工业过程测量控制和自动化标准化技术委员会（SAC/TC124）联合归口。

本标准起草单位：国家能源局、国家电网公司、南京南瑞集团公司、国网智能电网研究院、中国电力科学研究院、中国南方电网公司、中国华能集团公司、国家信息技术安全研究中心、中国信息安全测评中心、公安部、机械工业仪器仪表综合技术经济研究所、中国科学院沈阳自动化研究所、中国科学院沈阳计算技术研究所、许继集团有限公司、北京四方继保自动化股份有限公司、东方电子股份有限公司、北京和利时系统工程有限公司、浙江大学、北京启明星辰信息安全技术有限公司、北京国电智深控制技术有限公司。

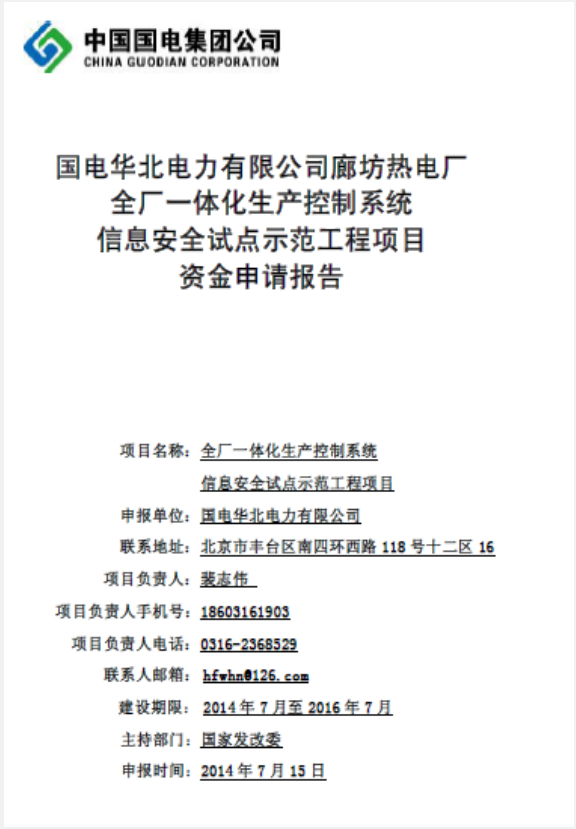
本标准主要起草人：辛耀中、苑舜、胡红升、许海铭、易俗、余勇、朱世顺、郭建成、南贵林、陶洪铸、孙炜、崔书昆、梁寿愚、郭森、李京春、李冰、李斌、张翀斌、郭启全、祝国邦、范春玲、李明、马跃、杨维永、邓兆云、王志皓、马骁、李凌、梁智强、陈雪鸿、王玉敏、尚文利、尹震宇、吕忠、汪强、任雁铭、慈国兴、冯冬芹、孟雅辉、朱镜灵、刘森、张亮、王弢。



国家标准《电力监控系统网络安全防护导则》制定

国家发改委信息安全专项智能电网调度控制系统安全免疫示范项目

科技创新能力支撑



中国国电集团公司
CHINA GUODIAN CORPORATION

国电华北电力有限公司廊坊热电厂
全厂一体化生产控制系统
信息安全试点示范工程项目
资金申请报告

项目名称：全厂一体化生产控制系统
信息安全试点示范工程项目
申报单位：国电华北电力有限公司
联系地址：北京市丰台区南四环西路 118 号十二区 16
项目负责人：裴志伟
项目负责人手机号：18603161903
项目负责人电话：0316-2368529
联系人邮箱：hfwhn@126.com
建设期限：2014 年 7 月至 2016 年 7 月
主持部门：国家发改委
申报时间：2014 年 7 月 15 日

国电集团一体化生产控制系统安全示范项目

1 范围
2 规范性引用文件
3 术语和定义
3.1 工业控制系统(...)
4 大唐集团工业控制系统概述
5 威胁和脆弱性分析
6 工业控制系统信息安全防护体系架构
7 SCADA系统安全技术要求
8 DCS系统安全技术要求
9 PLC系统安全技术要求
10 其他系统安全技术要求
附录A 工业控制系统信息安全技术要求和措施

《大唐集团工业控制系统安全技术规范》项目

科技创新能力支撑

255项
国家发明专利

180项
计算机软件软件著作权

专利号	专利名称
200710177198.0	一种数据库操作响应时间测算方法及系统
200710303985.5	一种恶意注入脚本网页检测方法和系统
200810101525.9	TELNET用户操作过程静态数据的保存回放方法
200810102849.4	一种基于网络数据流的网络病毒检测方法及装置
200810102850.7	一种内、外网络报文的识别方法
200810104320.6	一种通过回显解析telnet协议的方法及系统
200810104321.0	一种基于报文流数据的无缓存模式匹配方法
200810104344.1	DB2数据库操作的信息提取和审计方法及其装置、系统
200810104416.2	一种并行多模式匹配的方法和系统
200810104417.7	一种计算机网络入侵定位系统和方法
200810106233.4	元件标识分发方法及基于该元件标识的应用层路由方法

科技创新能力支撑

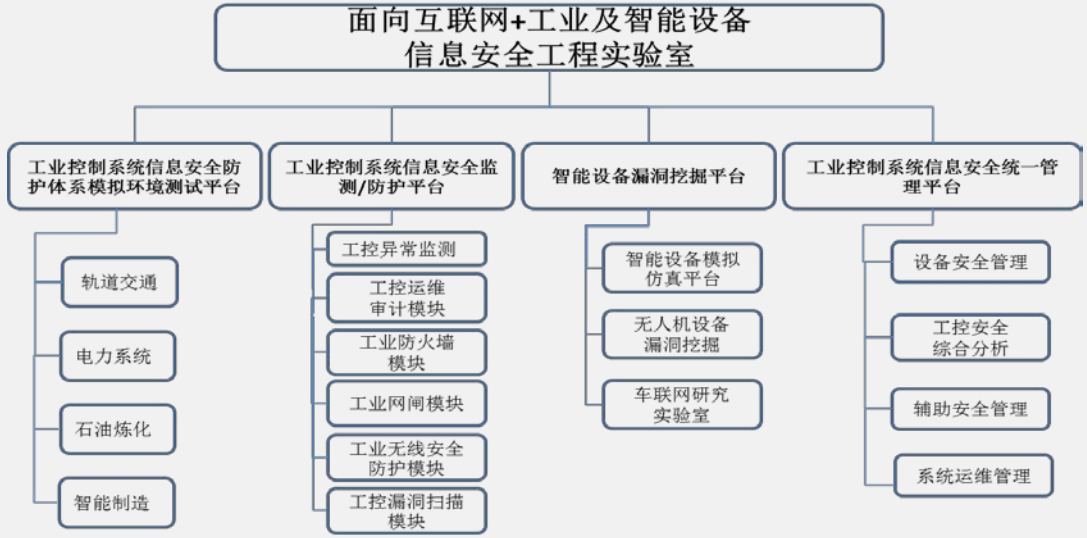
北京市发展和改革委员会文件

京发改（审）〔2016〕203号

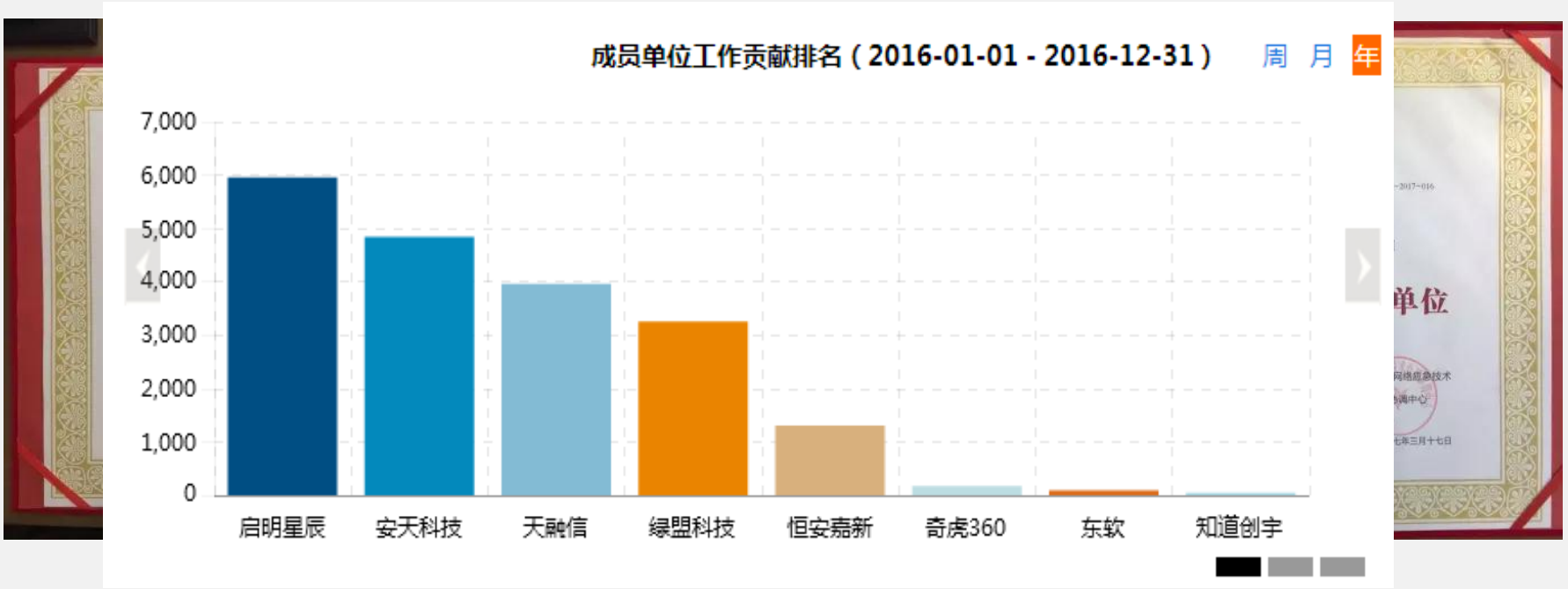
北京市发展和改革委员会
关于面向互联网+工业及智能设备信息安全
北京市工程实验室创新能力建设
项目资金申请报告的批复

海淀区发展改革委：

你单位《关于面向互联网+工业及智能设备信息安全北京市工程实验室创新能力建设项目资金申请报告的请示》（京海淀发改[审][2016]42号）收悉。经2016年4月29日我委主任专题会审议通过，现就有关事项批复如下：



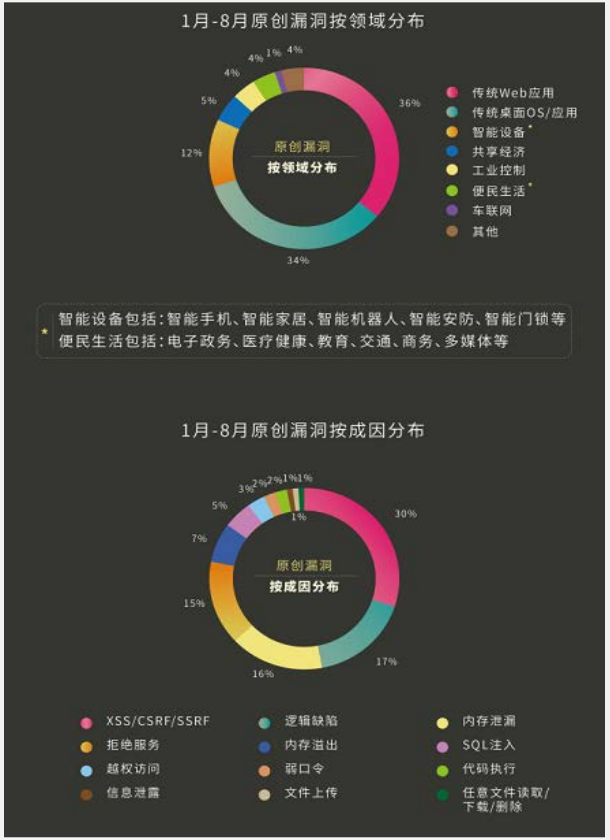
核心竞争力支撑



2016年启明星辰位居“成员单位工作贡献排名”榜首，并向CNVD提交原创漏洞100个，其中高危漏洞9个，中危漏洞91个，涵盖传统桌面应用系统安全、Web安全、移动智能终端安全、IoT安全和工控系统安全等领域。

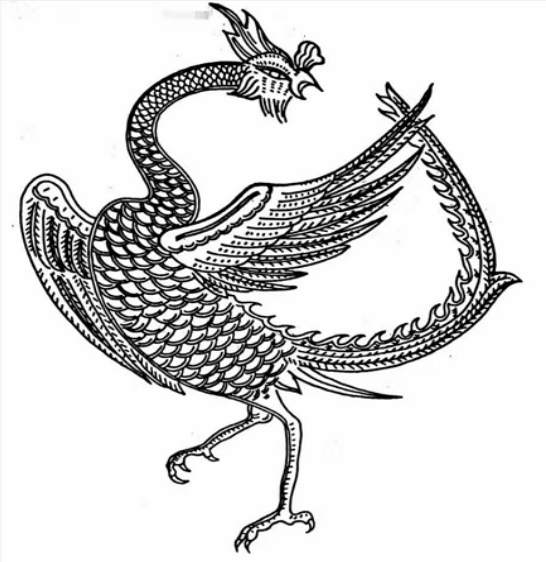
核心竞争力支撑


2017年1月-8月，已确认原创漏洞174个。
目前“CNVD企业单位原创积分排名”第一。
CNVD企业单位原创积分排名
1800
1600
1400
1000
800
600
400
200
0
启明星辰
XXX
XXX
XXX
XXX
XXX
XXX
XXX
XXX
XXX
1月-8月CNVD/CNNVD原创漏洞
2%
13%
CNVD/CNNVD
高危漏洞23个
中危漏洞148个
低危漏洞3个
高危漏洞
中危漏洞
低危漏洞


1月-8月原创漏洞按领域分布
4%
1%
4%
4%
5%
12%
36%
34%
原创漏洞
按领域分布
传统Web应用
传统桌面OS/应用
智能设备*
共享经济
工业控制
便民生活*
车联网
其他
* 智能设备包括：智能手机、智能家居、智能机器人、智能安防、智能门锁等
便民生活包括：电子政务、医疗健康、教育、交通、商务、多媒体等
1月-8月原创漏洞按成因分布
3%
2%
2%
1%
1%
1%
5%
7%
15%
16%
17%
30%
原创漏洞
按成因分布
XSS/CSRF/SSRF
拒绝服务
越权访问
信息泄露
逻辑缺陷
内存溢出
弱口令
文件上传
内存泄漏
SQL注入
代码执行
任意文件读取/下载/删除

核心竞争力支撑

2017年5月9日，启明星辰ADLab发现Linux内核存在远程漏洞“Phoenix Talon”（取凤凰爪四趾之意），涉及**CVE-2017-8890**、CVE-2017-9075、CVE-2017-9076、CVE-2017-9077，可影响几乎所有Linux kernel 2.5.69 ~Linux kernel 4.11的内核版本、**对应的发行版本以及相关国产系统**。可导致远程 DOS，且在符合一定利用条件下可导致 RCE，包括传输层的TCP、DCCP、SCTP以及网络层的IPv4和IPv6协议均受影响。



漏洞编号	漏洞描述	攻击条件	漏洞评级
CNVD-2017-07509、CVE-2017-9077	Linux kernel中net/ipv6/tcp_ipv6.c文件的‘tcp_v6_syn_recv_sock’函数存在拒绝服务漏洞，该漏洞源于程序未能正确的处理继承。本地攻击者可借助特制的系统调用利用该漏洞造成拒绝服务。	本地	中危
CNVD-2017-07508、CVE-2017-9076	Linux kernel中net/dccp/ipv6.c文件的‘dccp_v6_request_recv_sock’函数存在拒绝服务漏洞，该漏洞源于程序未能正确的处理继承。本地攻击者可借助特制的系统调用利用该漏洞造成拒绝服务。	本地	中危
CNVD-2017-07507、CVE-2017-9075	Linux kernel中net/sctp/ipv6.c文件的‘sctp_v6_create_accept_sk’函数存在拒绝服务漏洞，该漏洞源于程序未能正确的处理继承。本地攻击者可借助特制的系统调用利用该漏洞造成拒绝服务。	本地	中危
CNVD-2017-07386、CVE-2017-8890	Linux内核中net/ipv4/inet_connection_sock.c中的inet_csk_clone_lock函数存在拒绝服务漏洞。远程攻击者可利用该漏洞通过接受系统调用造成拒绝服务	远程	高危

总结

启明星辰集团希望结合电力监控系统网络安全新需求，以创新思维解决核心难题，共同面对新挑战，落实《网络安全法》各项要求，夯实本质安全建设，共同确保电力监控系统安全稳定可靠。




Venustech

THANKS!

谢谢观看

启明星辰集团