构建工控网络安全预警态势感知平台

演讲人：饶志波

水利部机电所工控安全测评中心

目录 / Contents

目录 CONTENTS

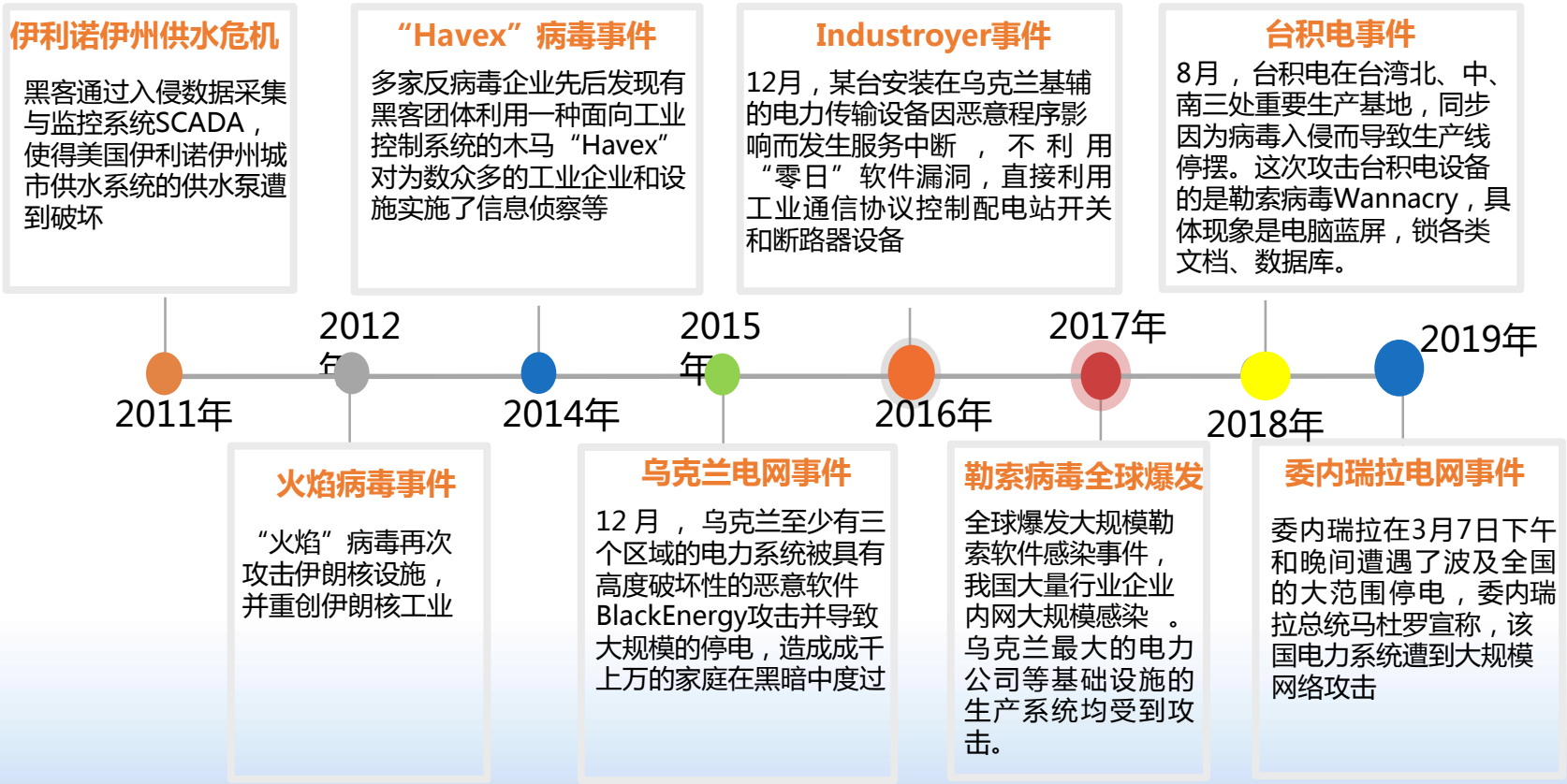
01 构建预警态势感知平台背景及政策支持

02 预警态势感知平台建设的总体设计

03 预警态势感知部署方案

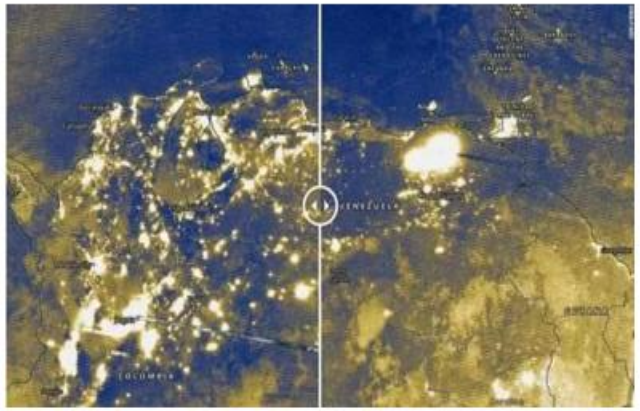
04 预警态势感知部署的典型案例

工控网络安全威胁日益突出



委内瑞拉电力系统大范围停电事件分析

委内瑞拉停电后的现状(卫星图)



背景

委内瑞拉遭遇大面积停电，整个国家几乎都陷入黑暗之中。大量民众涌入首都加拉加斯表示对停电的不满，甚至有部分极端的抗议者与警方发生了严重的肢体冲突。但有更多的民众选择走出家门，表达对总统马杜罗的支持，并谴责国内外反动势力对和平的蓄意破坏。

攻击手段初步分析

① 利用电力系统的漏洞植入恶意软件。

② 发动网络攻击干扰控制系统引起停电。

③ 干扰事故后的维修工作。

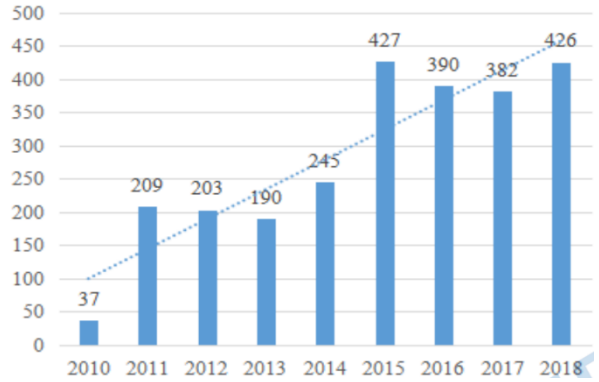
事件回顾

2019年3月7日到3月9日，连续三天，委内瑞拉电力系统出现3次大范围停电事件。此次事件是该国家自 2012 年以来时间最长、影响地区最广的停电。

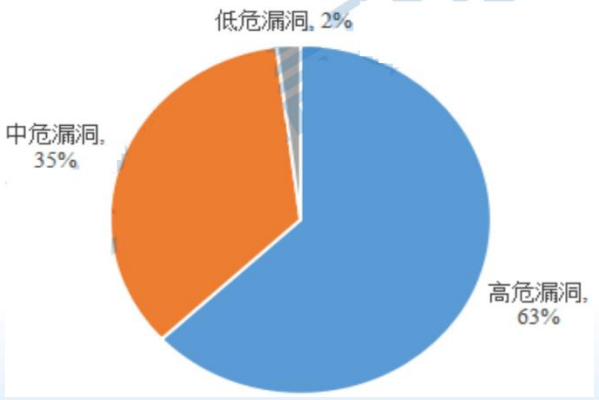
事件反思-前车之鉴，加强国内的电力系统工控安全建设

从委内瑞拉遭受的此次攻击来看，通过网络攻击打击对手的国家电力基础设施，整个电力系统的多个环节都遭受攻击，并且攻击的渠道也呈现多样化。就我国而言，电力系统体系庞大、系统复杂，如何做好安全防护就需要引起我们进一步的思考。

工控网络面临的主要威胁统计

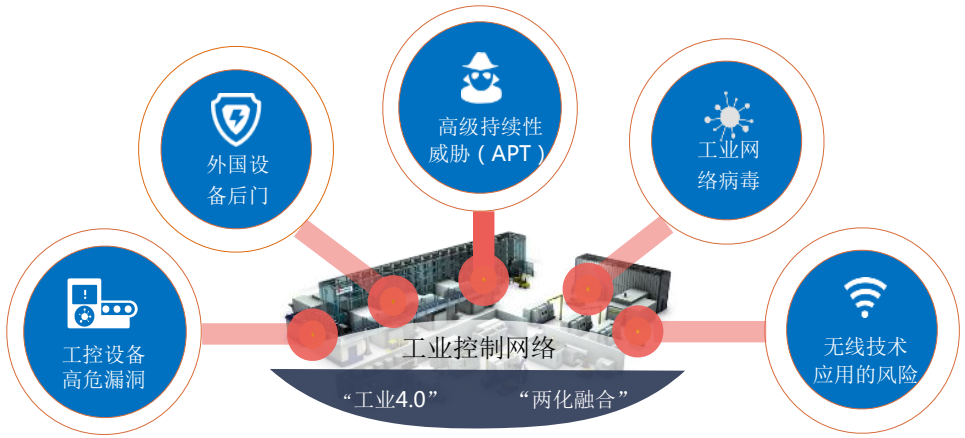


2010-2018年全球工控系统漏洞数量



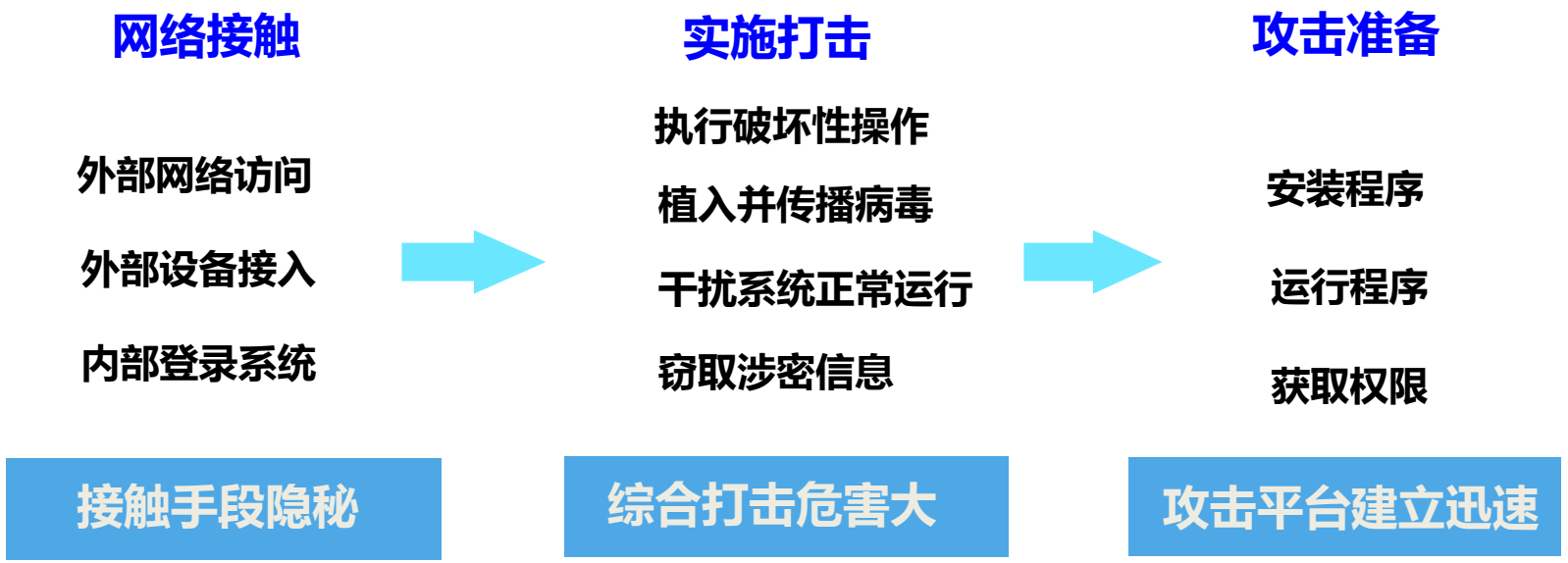
2018年全球工业控制系统漏洞分布

资料来源：美国ICS-CERT



随着“工业4.0”时代的来临和“两化融合”脚步的加快，越来越多的网络安全隐患被带入了工业控制系统。

工业网络攻击技术发展迅速



因此，网络攻击的防御必须及早开展，及早监测，事前完成安全风险的预防预控，事中需要在接触之时发现，破坏之前消灭。针对工控系统的安全监控，更要建立起针对工控网络攻击的态势预警感知平台。

构建针对工控系统态势预警感知平台必要性

-通用网络安全态势感知监测技术不是最佳选择

通用的态势预警平台中的安全监测产品一般基于网络流量和报文分析技术，主要对互联网通用服务和协议进行监测、分析，对于网络空间隔离、设备和用户相对确定、网络服务私有可控的工业控制系统而言，不是最佳选择 。

对比项	通用安全监测技术	工控系统专用安全监测技术
监测对象	WEB等通用网络服务的数据报文	各工业控制系统监控系统中的设备，协议，日志等
监测手段	网络流量及报文内容分析	基于被监测对象自身感知的设备级监测
监测内容	利用已知漏洞的攻击行为	外部网络访问、外部设备接入、用户登录、人员操作等事件
典型设备	IDS、防火墙等	网络安全监测装置

迫切需要研发适合工业监控系统、面向设备事件的网络安全监测技术的工业控制系统安全预警态势感知平台。

构建针对工控系统态势预警感知平台必要性

现状

仅覆盖网络边界上的防护设备

仅能对跨边界的网络安全事件进行监视告

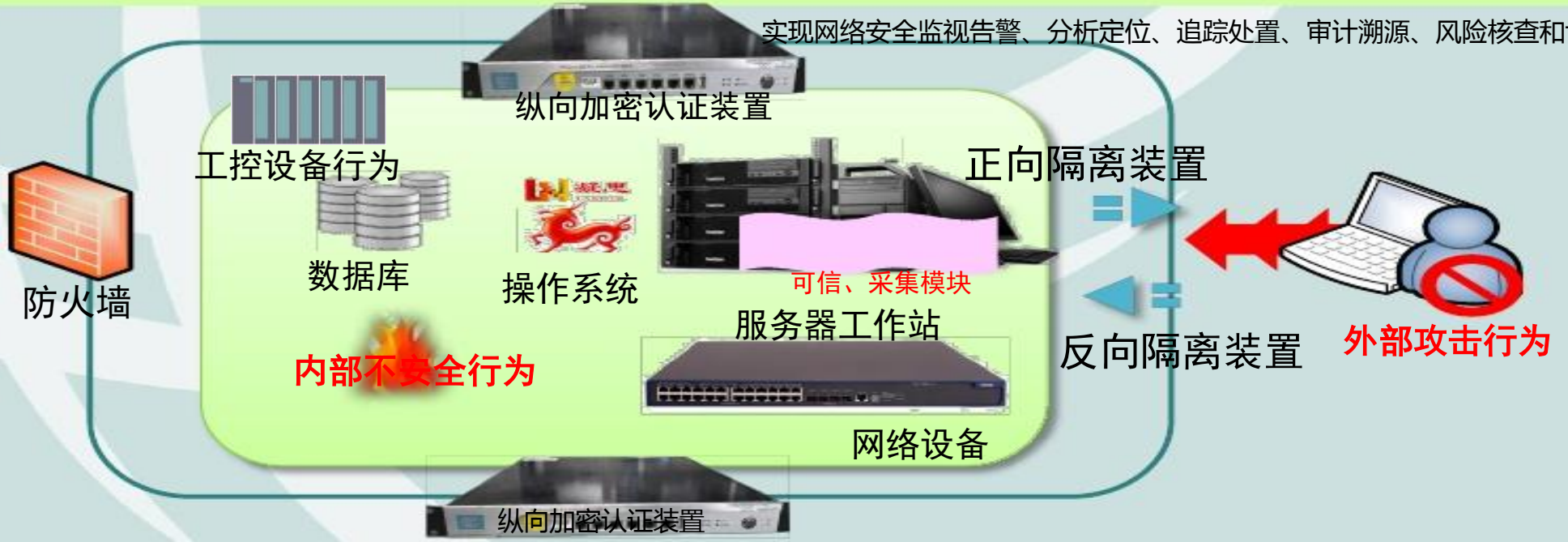
需求

采集对象：采集来自可信模块的审计告警信息，支持传统IT信息系统的采集，如访问控制系统，防毒系统，防火墙，入侵检测，漏洞扫描等。也支持工控控制系统的采集，如PLC、隔离网闸，工业交换机等。

监测事件：覆盖系统内部的服务器、工作站、工控设备/工控协议行为和网络设备。

应用功能：全面监测外部网络访问、外部设备接入、用户登录、人员操作等事件。

实现网络安全监视告警、分析定位、追踪处置、审计溯源、风险核查和协同管控。



国家政策指导

2014年：没有网络安全就没有国家安全

习近平强调，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。要树立正确的网络安全观，**加强信息基础设施网络安全防护**，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。**要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。**

2016年：朝着建设网络强国目标不懈努力

要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候**全方位感知网络安全态势**，增强网络安全防御能力和威慑能力

习近平总书记在主持中央政治局集体学习时强调，加快推进网络信息技术自主创新，加快提高网络管理水平，**加快增强网络空间安全防御能力，朝着建设网络强国目标不懈努力。**

2018年：自主创新推进网络强国建设

习近平在全国网络安全和信息化工作会议上强调，敏锐抓住信息化发展历史机遇，自主创新推进网络强国建设。

行业政策指导

2014年之前

经贸委[2002]30令《电网和电厂计算机监控系统及调度数据网络安全防护规定》**电监会5号令《电力二次系统安全防护规定》**
工信部[2011]451号《关于加强工业控制系统信息安全管理的通知》

2014年

发改委14号令《电力监控系统安全防护规定》（同时废止电监会5号令）
国能安全]387号《国家能源局综合司关于开展电力工控PLC设备信息安全隐患 排查及漏洞整改工作的通知》

2015年

国能安全36号《电力监控系统安全防护总体方案》附1-附4

2016年

国能综安全92号《电力监控系统安全防护专项检查》
工信部信软338号《工业控制系统信息安全防护指南》及解读

2017年之后

2017年水利信息化工作要点 办信息【2017】62号 编制水利工程工业控制系统网络安全技术防护方案
2017年《网络安全法》第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。
加快推进电力监控系统网络安全管理平台建设的通知-国家电网调
工业和信息化部关于印发《工业控制系统信息安全事件应急管理工作指南》
工业和信息化部关于印发《工业控制系统信息安全行动计划（2018-2020年）》
2018年水利网信工作要点 〔2018〕35号 加强水利关键信息基础设施网络安全保护
国家能源局关于加强电力行业网络安全工作的指导意见-国能发安全〔2018〕72号

2018年水利网信工作要点〔2018〕35号 加强水利关键信息基础设施网络安全保护

加强水利关键信息基础设施网络安全保护。印发《水利关键信息基础设施名录》，宣贯《水利网络安全事件应急预案》，指导关键信息基础设施主管单位完善网络安全管理制度、开展应急预案及专项预案编制。

抓好网络安全监督检查。按照中央网信办、公安部等国家网络安全主管部门部署，组织开展水利网络安全检查，在各单位自查基础上开展抽查。

开展水利工控系统网络安全防护。认真组织实施**国家信息安全专项 - 丹江口水利关键信息基础设施网络安全态势感知示范工程。**编制水利工程工业控制系统网络安全技术防护指导意见，推进有关建设工作。

落实网络安全等级保护工作。督促流域机构全面完成重要信息系统等级保护改造项目的测评和竣工验收工作。推进水利行业加快完成已建信息系统的定级备案和建设整改工作，组织关键信息基础设施运营单位完成系统等级保护定级备案。

国家能源局关于加强电力行业网络安全工作的指导意见-国能发安全〔2018〕72号

国家能源局文件

国能发安全〔2018〕72号

国家能源局关于加强电力行业网络安全工作的指导意见

各省、自治区、直辖市、新疆生产建设兵团发展改革委（能源局）、经信委（工信委）、国家能源局各派出监管机构，全国电力安全生产委员会各企业成员单位：

为深入贯彻党的十九大精神，全面落实习近平总书记关于网络强国战略的重要论述，按照《中华人民共和国网络安全法》《电力监管条例》及相关法律法规要求，健全电力行业网络安全责任体系，完善网络安全监督管理体制机制，加强关键信息基础设施安全保护，提升电力监控系统安全防护水平，强化网络安全防护体系，提高自主创新及安全可控能力，防范和遏制重大网络安全事件，保障电力系统安全稳定运行和电力可靠供应，提出以下意见。

— 1 —

提高网络安全态势感知、预警及应急处置能力

（一）推进网络安全态势感知、预警能力建设。**建立行业、企业网络安全态势感知预警平台**，加强电力监控系统、重要管理信息系统、互联网出口的全面监测，加强网络安全信息的汇集、研判。（二）加强网络安全应急处置能力建设。建立电力行业网络安全应急智慧平台，完善网络安全应急预案。加强网络安全应急队伍、应急资源库建设，组织开展实战型网络安全应急演练，提升网络安全事件应急快速响应能力

建设网络安全仿真验证环境

适应电力行业网络安全研究、测试、演练等应用需求，整合现有资源，建立覆盖发、输、变、配、用、调度全环节的网络**安全仿真验证环境，开展重大网络安全事件模拟验证、漏洞挖掘、攻防演练、业务培训**等工作。建设行业网络安全重点实验室。

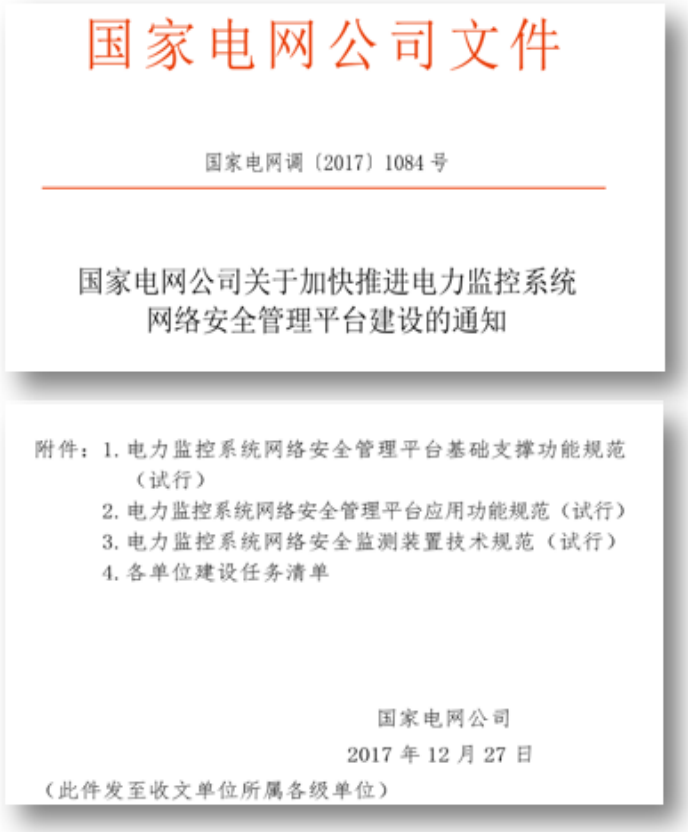
网络安全自主创新与安全可控

（一）坚持关键领域安全可控。推动电力专用安全防护设备升级换代，**加快推进专用系统与装备、通用软硬件产品安全可控替代及应用。坚持新能源、配电网及负荷管理等领域智能终端、智能单元安全可控。**加强安全可控产品的研制与应用，鼓励开展前沿性技术应用研究。

（二）加速推进核心技术攻关与应用。加强体系化技术布局，完善制度、市场环境，推进电力系统网络安全核心技术突破。**重点在电力系统关键系统、重大装备、防护体系、专用芯片、密码应用、攻防对抗和检测技术等领域**，加强自主创新与应用突破。支持电力专用芯片研发和使用。

（三）做好新技术、新业务网络安全保障。关注能源生产、经营、消费等领域发展带来的网络安全问题，**加强对“大云物移智”**等新技术、以及微电网、充电基础设施、车联网、“互联网+”等新业务的**网络安全风险研究，为行业发展提供网络安全保障。**

加快推进电力监控系统网络安全管理平台建设的通知



国家电网公司文件

国家电网调〔2017〕1084号

国家电网公司关于加快推进电力监控系统网络安全管理平台建设的通知

附件：1. 电力监控系统网络安全管理平台基础支撑功能规范（试行）
2. 电力监控系统网络安全管理平台应用功能规范（试行）
3. 电力监控系统网络安全监测装置技术规范（试行）
4. 各单位建设任务清单

国家电网公司
2017年12月27日

（此件发至收文单位所属各级单位）

建设目标：

按照“设备自身感知、监测装置就地采集、平台统一管控”的原则，地级以上调控机构建设网络安全管理平台，变电站（站控层）部署网络安全监测装置，运用实时监控、预警告警、定位溯源、审计分析、闭环管控等先进适用功能，全面监控网络空间内计算机、网络设备、安防设备等设备的安全行为，进一步完善电力监控系统安全防护体系，推动网络安全管理从“静态布防，边界监视”向“实时管控、纵深防御”的转变，全面实现“外部侵入有效阻断、外力干扰有效隔离、内部接入有效遏制、安全风险有效管控”的防控目标。

建设原则：

1、继承现有防护优势；
2、创新发展监控技术；
3、建设先进实用功能。

建设内容：

1、调控机构建设网络安全管理平台
2、场站部署网络安全监测装置
3、其他电力监控系统网络安全事件接入。

目录 / Contents

目录 CONTENTS

01 构建预警态势感知建设背景及政策支持

02 预警态势感知平台建设的总体设计

03 预警态势感知部署方案

04 预警态势感知部署的典型案例

构建预警态势感知平台设计原则及目标

原则	业务目标	功能目标
继承优势 • 巩固现有工控系统静态布防的安全策略和防护手段，通过闭环管理手段进一步强化。	外部侵入有效阻断	支持安全策略和安全保护措施的闭环管理
创新发展 • 监视技术和分析手段更丰富，同时具备必要的响应处置手段	外力干扰有效隔离	支持工业控制网络安全事件的全方位监视和控制
先进实用 • 面向设备基于事件的监视技术，分布式的工业控制网络安全管理体系	内部介入有效遏制 安全风险有效管控	支持工业控制网络网络安全态势的只能分析

工控网络安全预警态势感知平台是电力监控系统网络安全闭环管理的专用技术支撑手段，是发现并反制工控系统网络有害行为的重要工具。同时也满足《网络安全法》及等级保护相关标准规范的技术要求。

构建预警态势感知平台的技术路线

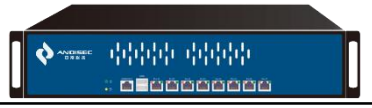
面向设备、基于事件的网络安全监测与管理

各类网络安全事件，总是从接触、控制的第一台设备开始发展、蔓延。做好网络监管，必须将监测关口从网络边界前移到服务器、工作站、交换机、PLC/DCS/RTU、SCADA软件设备等具体设备，从每一台设备的网络访问、设备接入、人员登录、设备操作、未知程序运行五类可疑事件入手，及早发现并处置网络攻击、病毒感染等各类安全事件。基于此，可以采用感知、采集、管控的三层模式来建立工控系统预警态势感知平台。

构建预警态势感知平台的技术路线

工控系统预警态势感知平台的三层逻辑结构按照设备自身感知、监测装置分布采集、管理平台统一管控的原则，构建网络安全管理的 感知、采集、管控三层逻辑结构。

统一管控



工业网络行为管理平台

分布采集

工业网络行为分析系统（安全网关机）　工业网络行为分析系统（安全网关机）

自身感知

服务器工作站

数据库

PLC/DCS等工业设备

网络设备　防火墙、IDS　纵向加密认证、正/反向隔离

监管平台

实现网络安全在线实时监视、预警、告警、分析、审计、核查等功能的集成。

监测装置

实现对调控机构、厂级、车间、设备层等监控系统相关设备网络安全数据的采集，以及与管理平台的通信和交互。

监测对象

实现服务器、工作站、交换机、纵向加密、正/反向隔离等设备自身可信计算和网络安全数据的感知及上报，并具体执行安全核查。

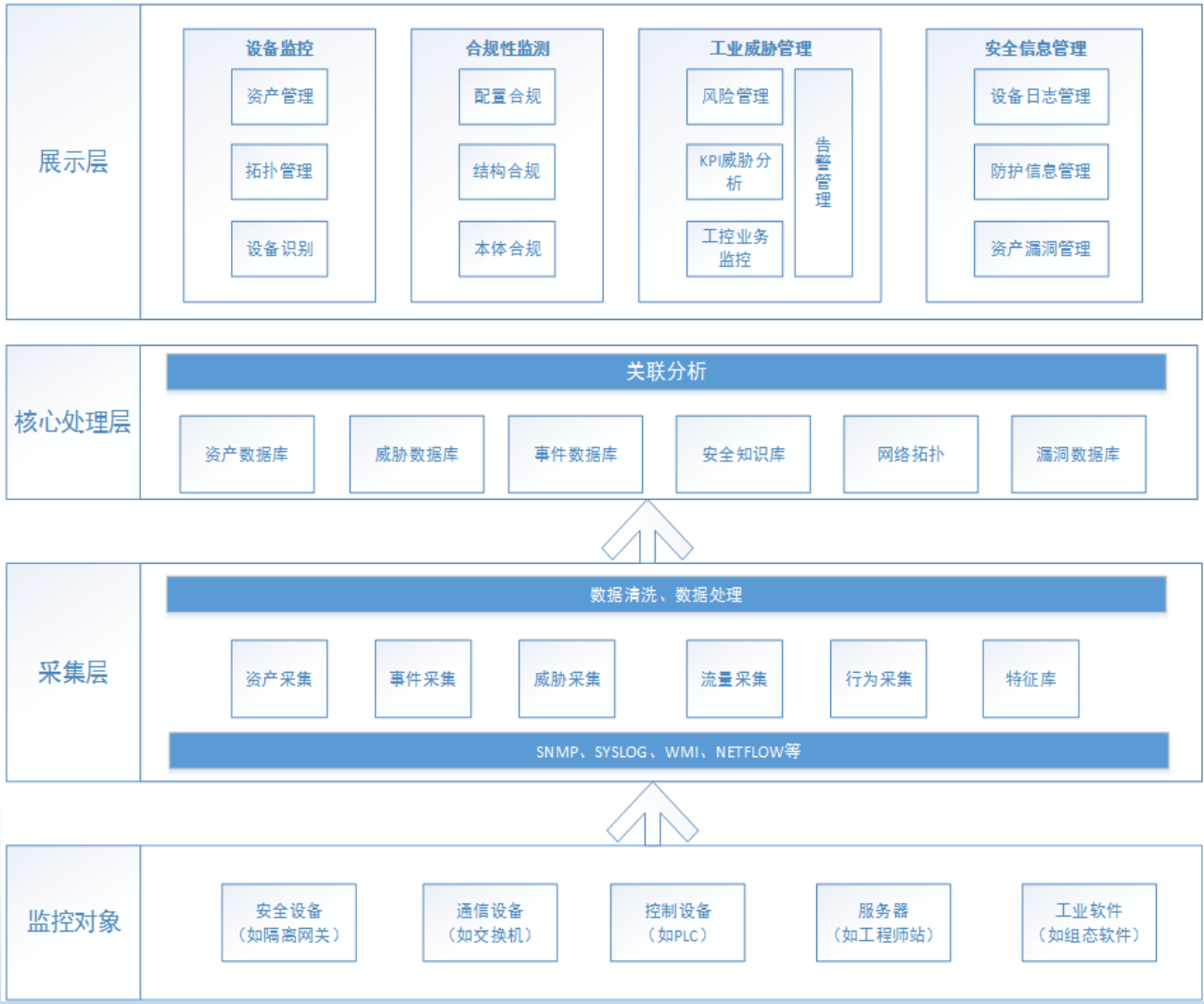
构建预警态势感知平台产品架构

第1层，属于数据采集层，使用各种采集技术采集流量信息、日志、各种资产信息，经过归一化处理后传入核心层。该层体现安全事件来源，入侵检测、防火墙、重要主机发出的日志都是安全事件来源，它们按发出机制分为两类：模式侦查器和异常监控（两者都采集警告信息，功能互补）由它们采集的安全事件，再被Agent转换为统一的格式发到服务器。

第2层，属于核心处理层，主要实现对各种数据的深入加工处理，包括运行监控、安全分析、策略管理、风险评估、关联分析、安全对象管理、脆弱性管理、事件管理、报表管理等。该层主要功能是安全事件的集中并对集中后的事件进行关联分析、风险评估及严重性标注等。所谓的集中就是以一种统一格式组织所有系统产生的安全事件告警信息（Alarms）并将所有的网络安全事件告警存储到数据库，这样就完成了对网络中所产生事件的一个庞大视图。系统通过事件序列关联和启发式算法关联来更好的识别误报和侦查攻击的能力。

本质上通过对各种探测器和监控产生的告警进行格式化处理，再进行关联分析，通过后期这些处理能提高检测性能，即减少告警数量，减小关联引擎的压力，从整体上提高告警质量。

第3层，属于数据展现层，主要负责完成与用户之间的交互，达到安全预警和事件监控、安全运行监控、综合分析的统一展示，形式上以图形化方式展示给用户。，其实就是系统对外的门户站点，它主要由仪表盘、事件管理、用户管理、资产管理系统策略等部分组成。



构建预警态势感知平台产品功能

1.资产管理

资产管理是平台的重要功能模块， 产品能够提供对网内资产的扫描发现、手工管理、 资产变更比对、资产信息整合展示能基本功能。 资产发现部分， 平台可以通过 IP 扫描、 SNMP 扫描、流量发现等手段对网内 IP 的存活情况进行跟踪，一旦发现超出当前管理范围的 IP，用户可以导出相关数据进行编辑再录入资产数据库。

2.拓扑管理

产品支持对企业网络拓扑进行扫描和发现， 用户可以将管理好的资产直接添加到任何一个自定义网络拓扑中，并对拓扑进行相关编辑

3.安全事件管理

告警在进行本地存储，并在需要时进行调阅查询。具备对告警的查询功能，查询条件包括告警对象、时间范围、告警级别、告警类型、告警内容关键字等。

4.告警管理

告警在进行本地存储，并在需要时进行调阅查询。具备对告警的查询功能，查询条件包括告警对象、时间范围、告警级别、告警类型、告警内容关键字等。

（1）网口状态监测:通过SNMP轮询和TRAP方式主被动监测交换机网口运行状态，当运行状态发生变更时，产生实时告警，并通过改变拓扑图中主机和相关连线颜色做实时展现。

（2）网口流量监测:监测交换机各网口实时流量，当网口流量超过既定阈值（如40%）时产生流量超限告警，并通过改变拓扑图中相应设备和相关连线颜色做实时展现。

（3）USB设备拔插:监测对象包括站控层具备USB口的主机。主机上需要安装部署绿色免安装代理软件（Agent）来监测各主机USB设备拔插情况。当发生USB设备接入与拔出时，结合USB设备白名单，产生不同告警信息。

（4）非法外联:监视主机网络连接情况，当发现主机连入互联网时，立即产生告警。

（5）Agent运行监测:网络安全监测装置通过和主机Agent之间保持心跳报文的方式，监测主机Agent是否处于开启状态，若装置在约定时间段内未收到心跳报文，判定为该主机Agent离线，产生告警信息并展示。

构建预警态势感知平台产品功能

5.知识库管理

平台提供知识库管理，主要涉及三个知识库，事件数据库、用户数据库、知识数据库。事件数据库，存储的是所有底层的探针所捕捉到的所有的事件。知识数据库，将系统的状态进行了参数化的定义，这些参数将为系统的安全管理提供详细的数据说明和定义。用户数据库，存储的是用户的行为和其他与用户相关的事件。

6.日志采集和管理

采集协议支持较为全面（很多是依赖插件完成），比如Syslog, Syslog-ng,SNMPv2, SNMPv3, OPSEC, HTTP,WMI, SQL, ODBC, FTP,SFTP, Socket UNIX, flat file, SSH, Rsync, Samba, NFS, SDEE, RDEP, CPMI多种协议

7.关联分析

支持数据关联，将多个数据源的数据进行联合、相关或组合分析，以获得高质量的信息。将不同　　空间设备的日志，不同时间序列存在的问题进过特定关联方法结合在一起。支持交叉交联，将安全事件与网络拓扑、系统开放的服务、设备存在的漏洞进行关联匹配，分析攻击成功的可能性。支持根据安全事件自动定义关联分析规则。

8.工业系统行为监测

工业安全事件管理平台够实时监测工控系统控制器下装、启动、停止等关键操作行为， 包括支持西门子 S7-300、施耐德昆腾、罗克韦尔 Control Logix 等系列工控系统，该功能需要部署监测探针。

9.响应与处理

工业安全事件管理平台具有自定义处理程序，可以发送邮件和短信响应处理功能，在发现关联告警后，安全管理员可将告警内容和响应建议通过邮件、短信等方式发送给指定的安全事件处置人员；也可以自定义处理程序，根据不同的事件进行自动的应急处理，降低对告警的处理的时间以及复杂度。具有闭环管理、统计和分析功能。

目录 / Contents

目录 CONTENTS

01 构建预警态势感知建设背景及政策支持

02 预警态势感知平台建设的总体设计

03 预警态势感知部署方案

04 预警态势感知部署的典型案例

构建预警态势感知平台产品

工控网络安全预警态势感知平台的建设通过部署工业网络安全采集探针，运用实时监视、预警告警、定位溯源、审计分析、闭环管控等先进适用功能，全面监控网络空间内计算机、网络设备、安防设施等设备上的安全行为，进一步完善智能制造监控系统安全防护体系，推动网络安全管理从“静态布防、边界监视” 向“实时管控、纵深防御”的转变，全面实现“外部侵入有效阻断、外力干扰有效隔离、内部介入有效遏制、安全风险有效管控”的防控目标。工业网络安全预警态势感知平台的建设主要包括两个部分:工业网络行为分析系统（工业网络安全采集探针）、工业网络行为管理平台（统一监管平台）两个部分。

工业网络行为分析系统

处理器	4核 CPU处理器
内存	内存8GB DDR4；
硬盘	256GB -25～70℃,2.5寸SATA SSD；
电源	两个交流220V/50HZ，电源插座,双路交流电源独立供电
USB	两个USB2.0接口
网口	8个10M/100M/1000M自适应以太网电口
操作系统	代码可控的经过裁减定制的Linux操作系统；

工业网络行为管理平台

处理器	4核CPU处理器；主频1.8GHz
内存	8GB*4 DDR3
硬盘	3*2T监控级硬盘，RAID卡：LSI-9260-8i，PCI-E转接卡：3300-1；
电源	两个交流220V/50HZ，电源插座,双路交流电源独立供电
网口	6个10M/100M/1000M自适应以太网电口
操作系统	Debian 3.16.56-1+deb8u1

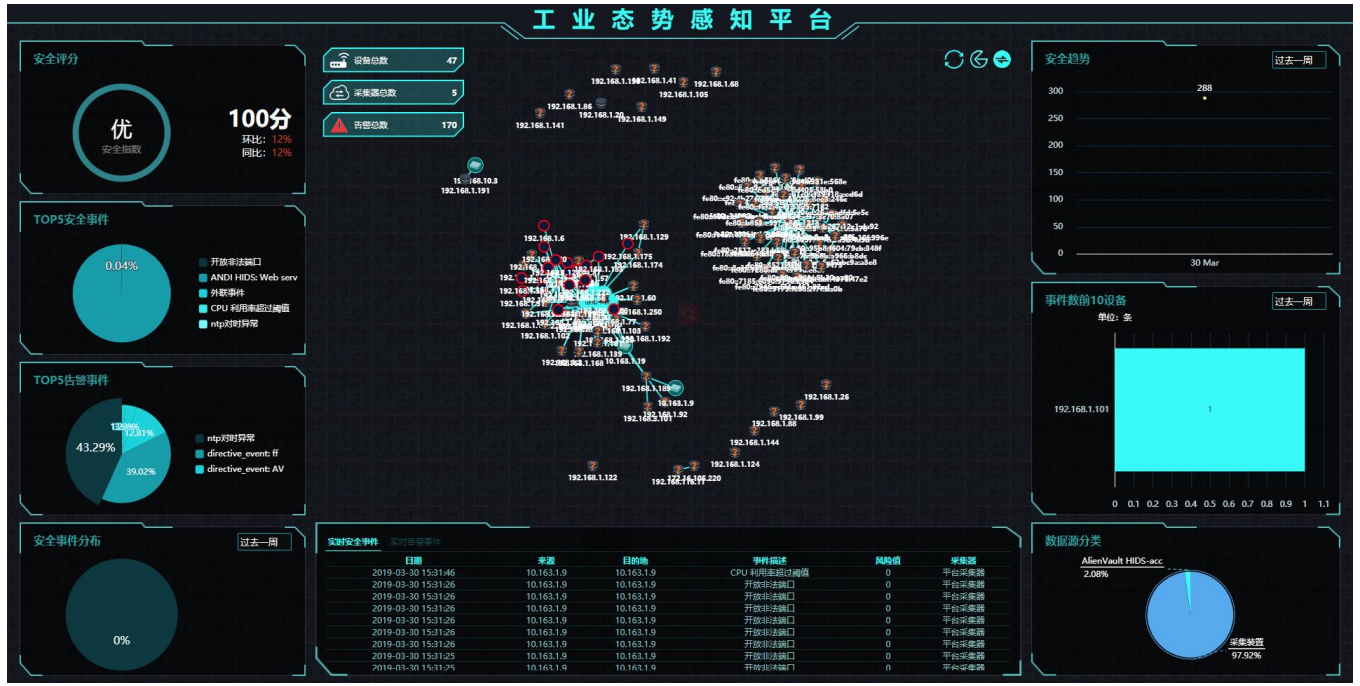
构建预警态势感知平台产品介绍

能力一：安全可视

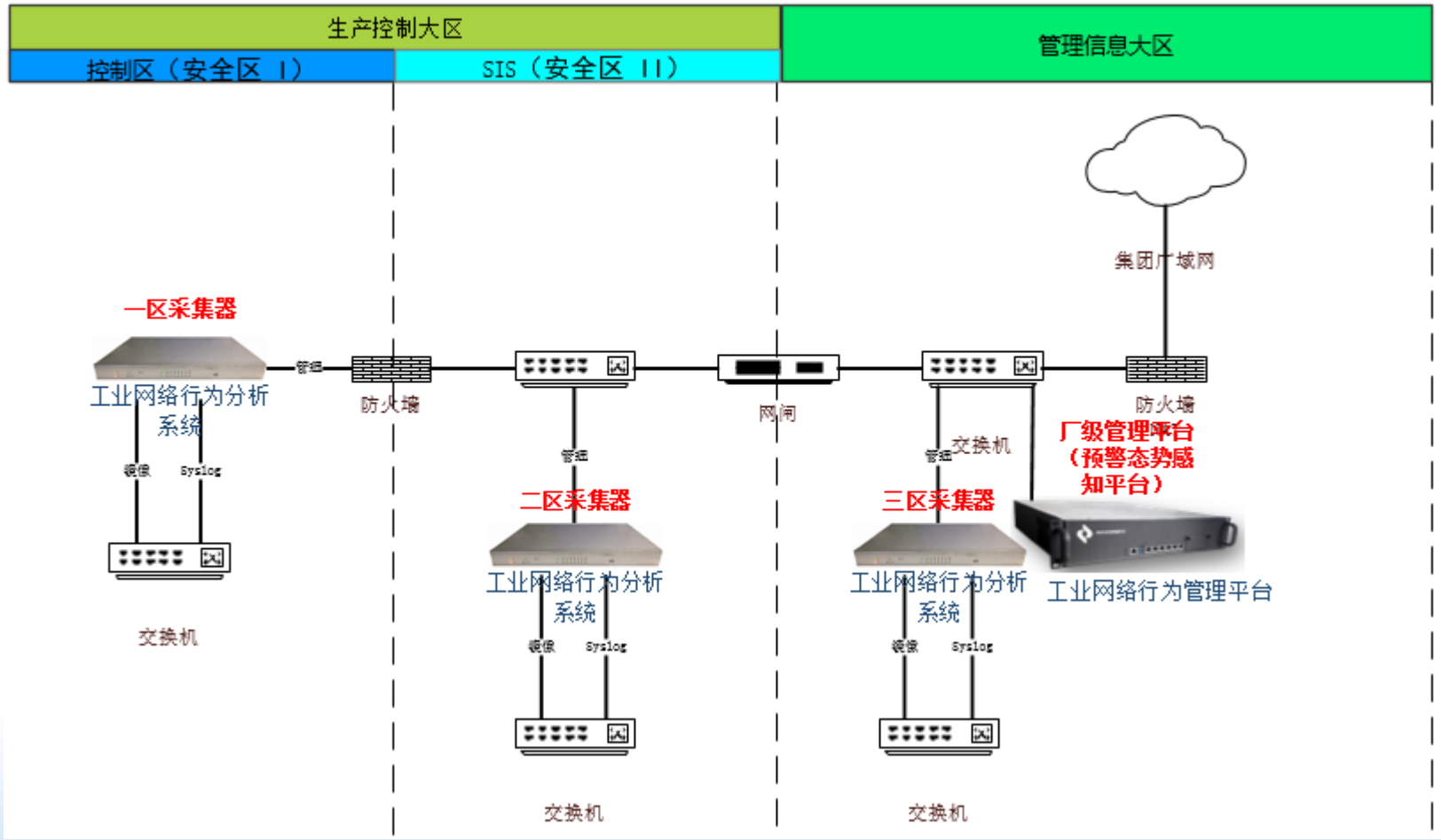
- 资产识别，包括：类型、型号、版本等；
- 业务识别，包括：身份、应用、设备等；
- 行为识别，包括：操作、内容、关系等；
- 安全识别，包括：身份、漏洞、风险等。

能力二：动态感知

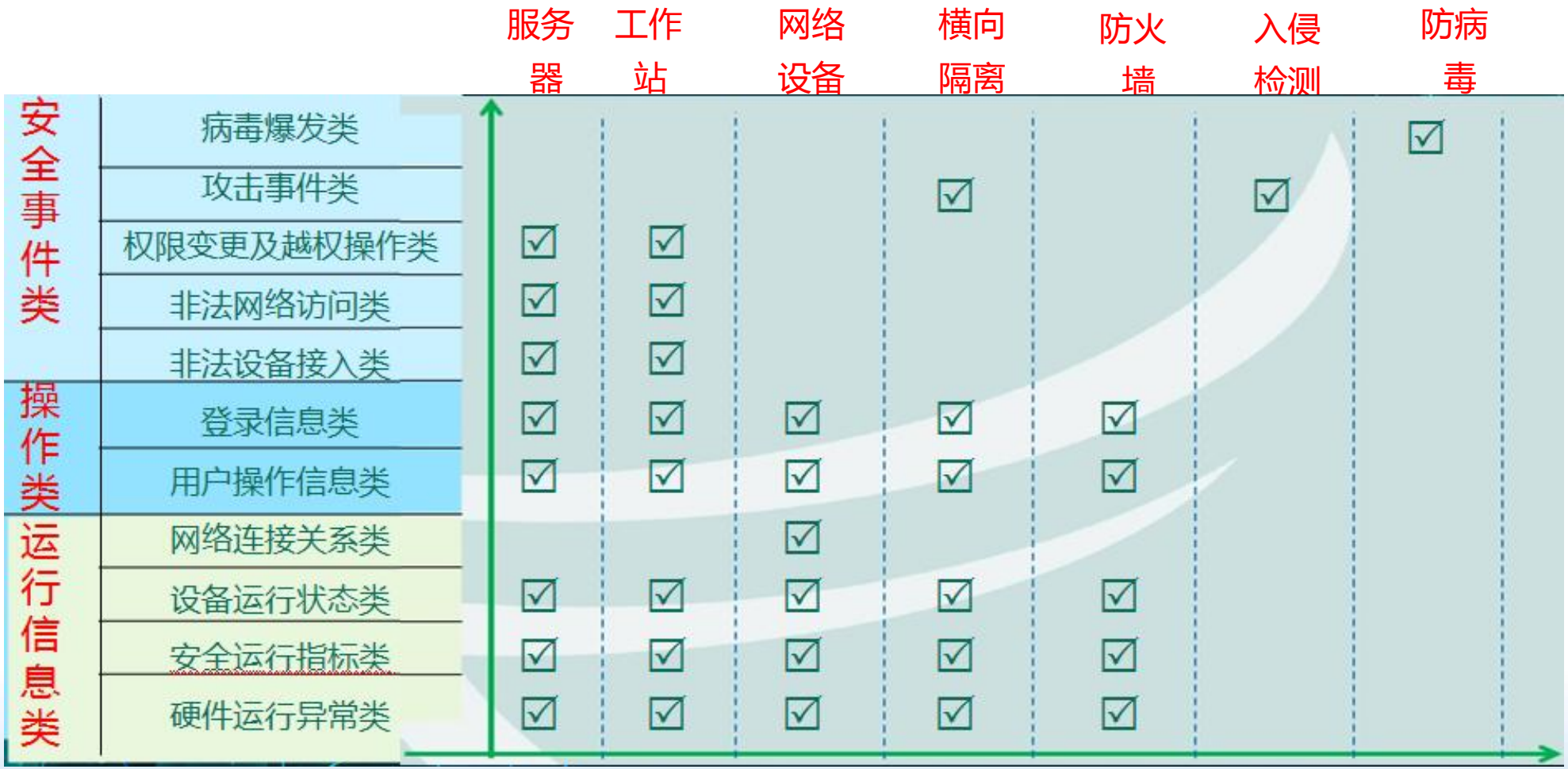
- 资产变更动态感知；
- 威胁风险动态感知；
- 安全事件持续感知；
- 异常行为持循感知。



构建预警态势感知平台产品部署



构建预警态势感知平台产品采集内容



同时，作为工控网络安全预警态势感知平台，还能针对工业控制系统够实时监测工控系统控制器下装、启动、停止等关键操作行为， 包括支持西门子 S7-300、施耐德昆腾、罗克韦尔 Control Logix 等系列工控系统，该功能需要部署监测探针。并能支持更多的协议比如Syslog, Syslog-ng,SNMPv2, SNMPv3, OPSEC, HTTP,WMI, SQL, ODBC, FTP,SFTP, Socket UNIX, flat file, SSH, Rsync, Samba, NFS, SDEE, RDEP, CPMI等多种协议。

构建预警态势感知平台产品数据上传

设备类型	上传分类	详细信息
装置自身上传事件	1）装置行为监视事件上传	登录成功
		退出登录
		装置USB设备拔出
		本地管理界面登录成功事件上传
		本地管理界面退出登录事件上传
		配置变更事件上传
	2）装置自身安全事件上传	USB设备（非无线网卡类）插入事件上传
		USB设备（无线网卡类）插入事件上传
		外联事件上传
		系统登录失败超过阈值事件上传
		危险操作事件上传
		开放非法端口事件上传
		网口up事件上传
		网口down事件上传
		CPU利用率超过阈值事件上传
		内存使用率超过阈值事件上传
		磁盘空间使用率超过阈值事件上传
		本地管理界面登录失败被锁定事件上传
		装置异常告警事件上传
		对时异常告警事件上传
		验签错误事件上传

构建预警态势感知平台产品数据上传

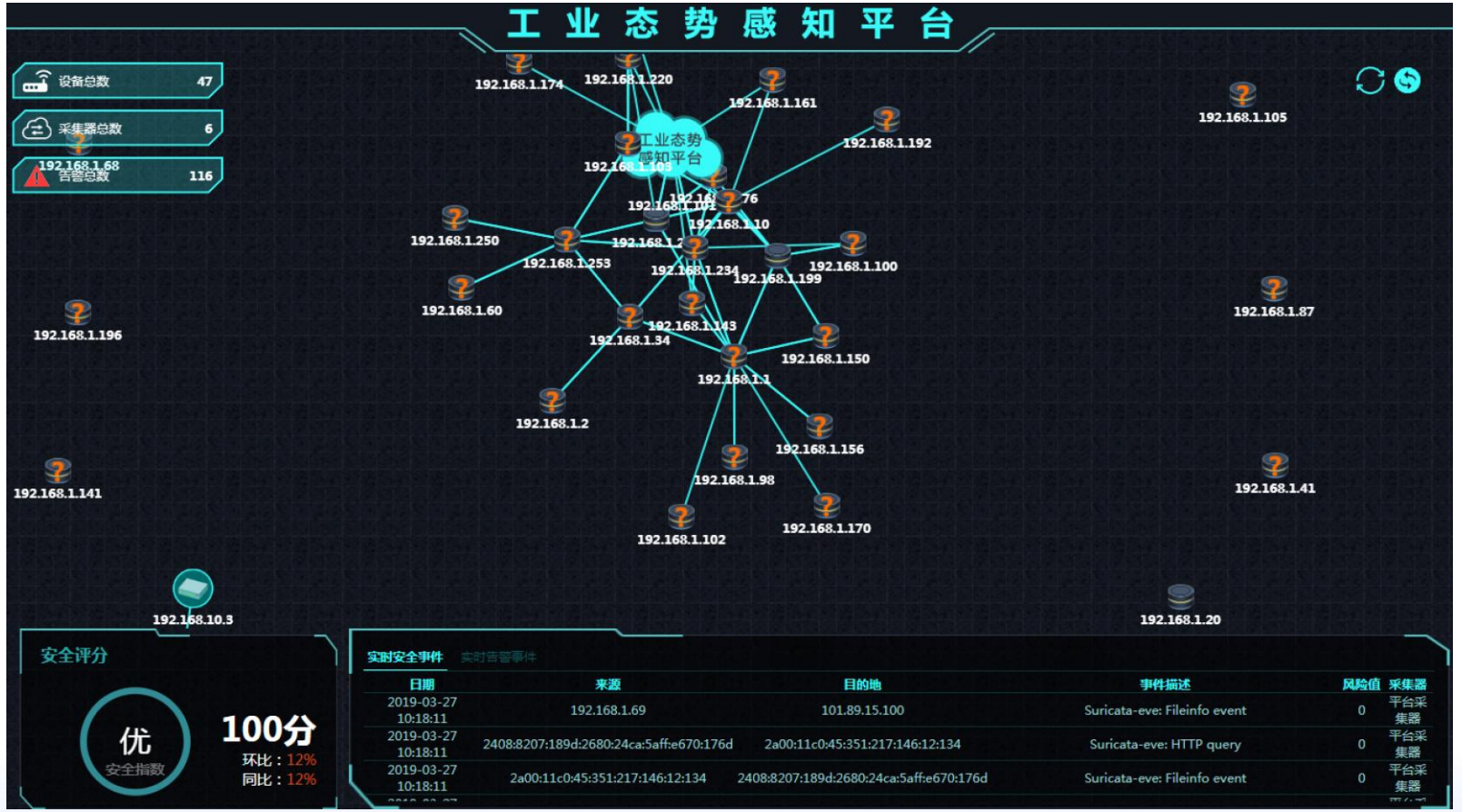
设备类型	上传分类	详细信息
主机上传事件	1）主机行为监视事件上传	登录成功事件上传
		退出登录事件上传
		USB设备拔出
		串口释放事件上传
		并口释放
		光驱卸载事件上传
		设备上线事件上传
	2）主机安全事件上传	USB设备（非无线网卡类）插入
		串口占用
		并口占用
		光驱挂载事件
		外联事件上传
		登录失败超过阈值事件上传
		关键文件变更事件上传
		用户权限变更事件上传
		开放非法端口事件上传
		网口up事件上传
		网口down事件上传
		危险操作事件上传

构建预警态势感知平台产品数据上传

设备类型	上传分类	详细信息
交换机上传事件	交换机告警上传	配置变更上传
		网口up事件上传
		网口down事件上传
		网口流量超过阈值
		交换机离线
		端口未绑定MAC地址

构建预警态势感知平台产品数据上传

设备类型	上传分类	详细信息
防火墙设备上传事件	1）防火墙设备行为监视事件上传	登录成功事件上传
		退出登录事件上传
		录失败事件上传
		上线事件上传
		修改策略事件上传
	2）防火墙设备安全事件上传	不符合安全策略访问事件上传
		攻击告警事件上传*
		离线事件上传
		CPU利用率超过阈值事件上传
		内存使用率超过阈值事件上传
隔离设备上传事件	1）正向隔离装置行为监视事件上传	隔离装置上线事件上传
	2）正向隔离装置安全事件上传	不符合安全策略访问
		隔离装置离线
		CPU利用率超过阈值
		内存使用率超过阈值
	3）反向隔离装置行为监视事件上传	隔离装置上线事件上传
	4）反向隔离装置安全事件上传	不符合安全策略访问
		隔离装置离线
		CPU利用率超过阈值
		内存使用率超过阈值


工业态势感知平台
设备总数 47
采集器总数 6
告警总数 116
192.168.1.174
192.168.1.220
192.168.1.161
192.168.1.105
192.168.1.192
工业态势感知平台
192.168.1.103
192.168.1.68
192.168.1.250
192.168.1.253
192.168.1.234
192.168.1.199
192.168.1.100
192.168.1.60
192.168.1.87
192.168.1.196
192.168.1.143
192.168.1.34
192.168.1.150
192.168.1.1
192.168.1.2
192.168.1.156
192.168.1.141
192.168.1.98
192.168.1.41
192.168.1.170
192.168.1.102
192.168.10.3
192.168.1.20
安全评分
优
安全指数
100分
环比：12%
同比：12%
实时安全事件
实时告警事件
日期 来源 目的地 事件描述 风险值 采集器
2019-03-27 10:18:11 192.168.1.69 101.89.15.100 Suricata-eve: Fileinfo event 0 平台采集器
2019-03-27 10:18:11 2408:8207:189d:2680:24ca:5aff:e670:176d 2a00:11c0:45:351:217:146:12:134 Suricata-eve: HTTP query 0 平台采集器
2019-03-27 10:18:11 2a00:11c0:45:351:217:146:12:134 2408:8207:189d:2680:24ca:5aff:e670:176d Suricata-eve: Fileinfo event 0 平台采集器

目录 / Contents

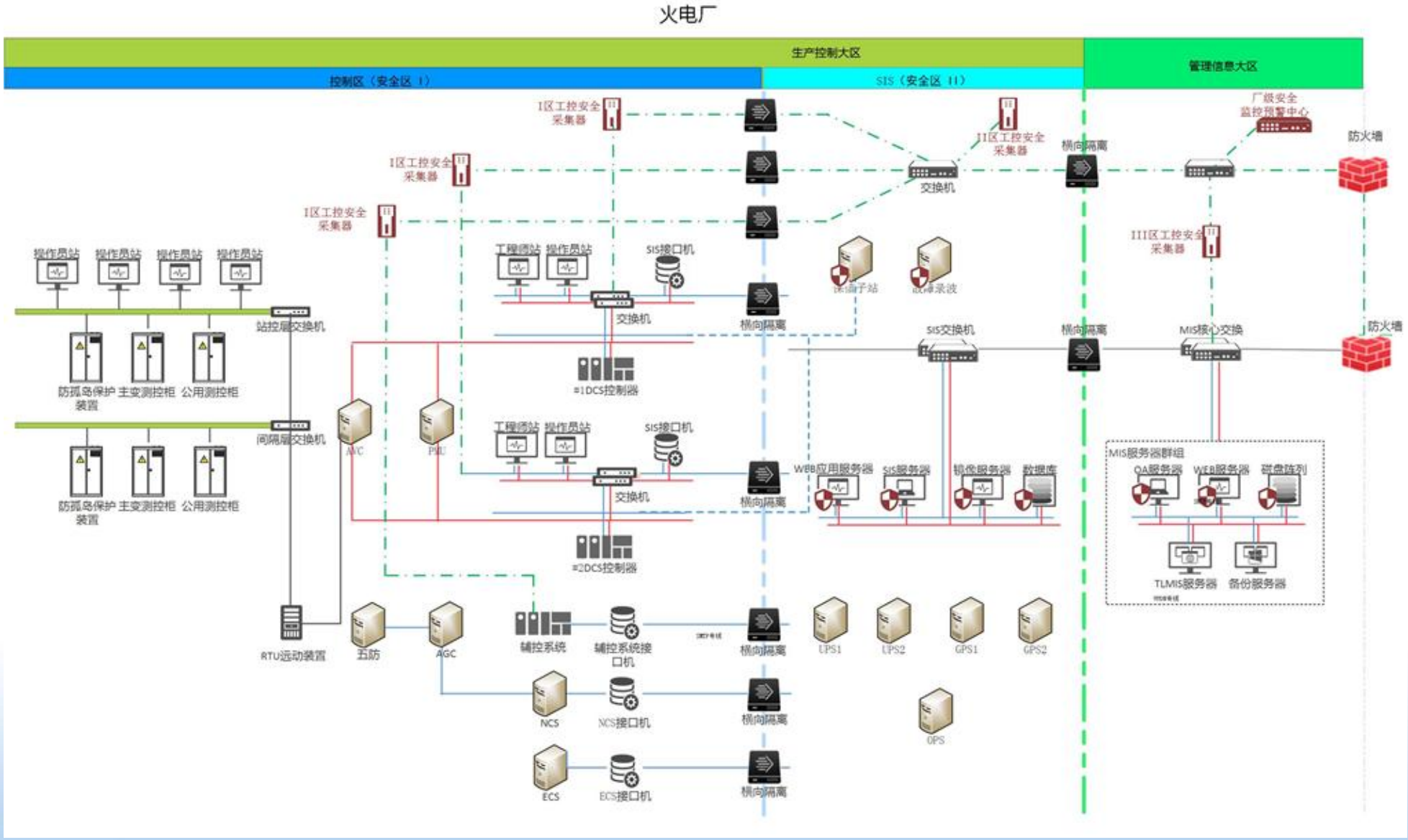
目录 CONTENTS

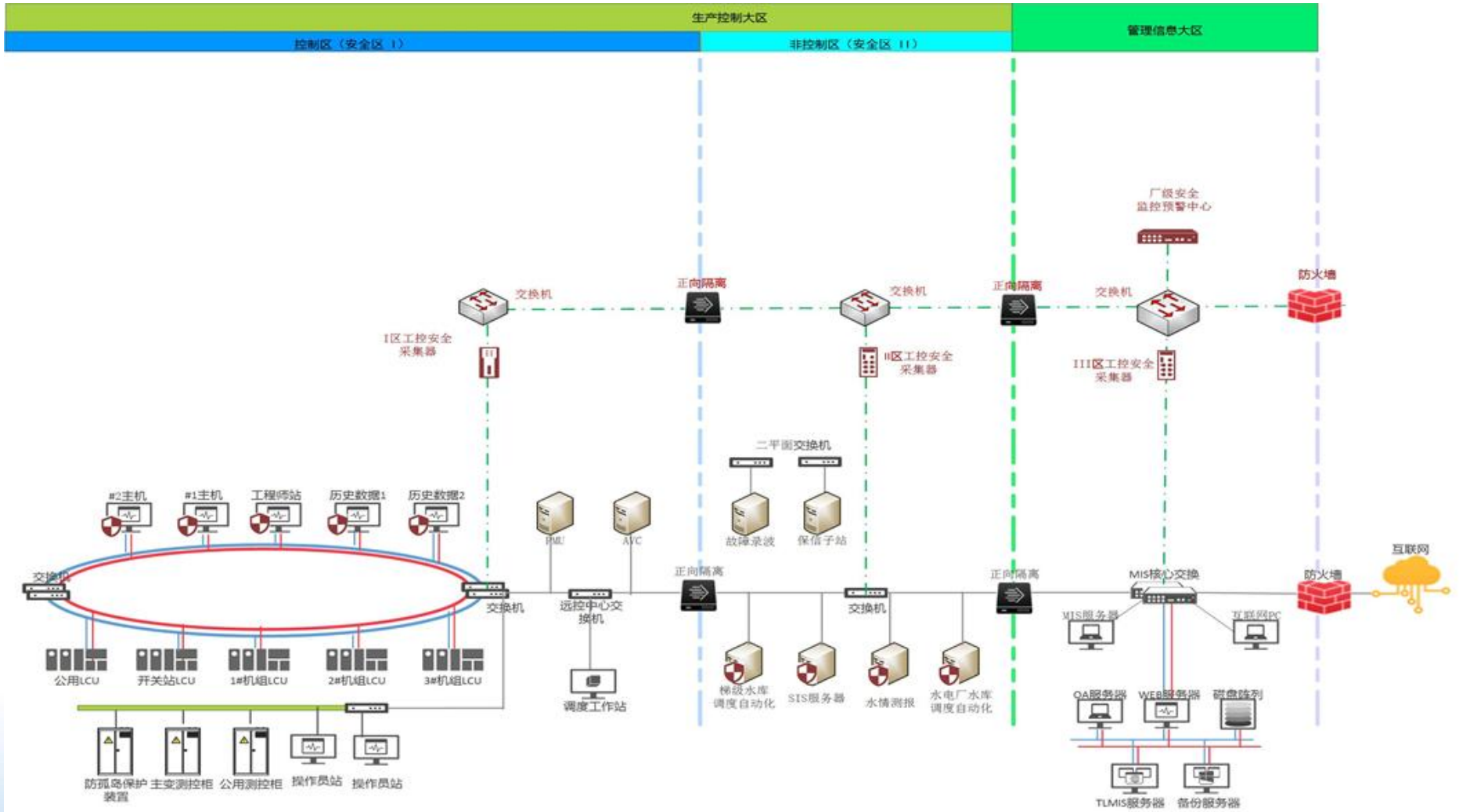
01 构建预警态势感知建设背景及政策支持

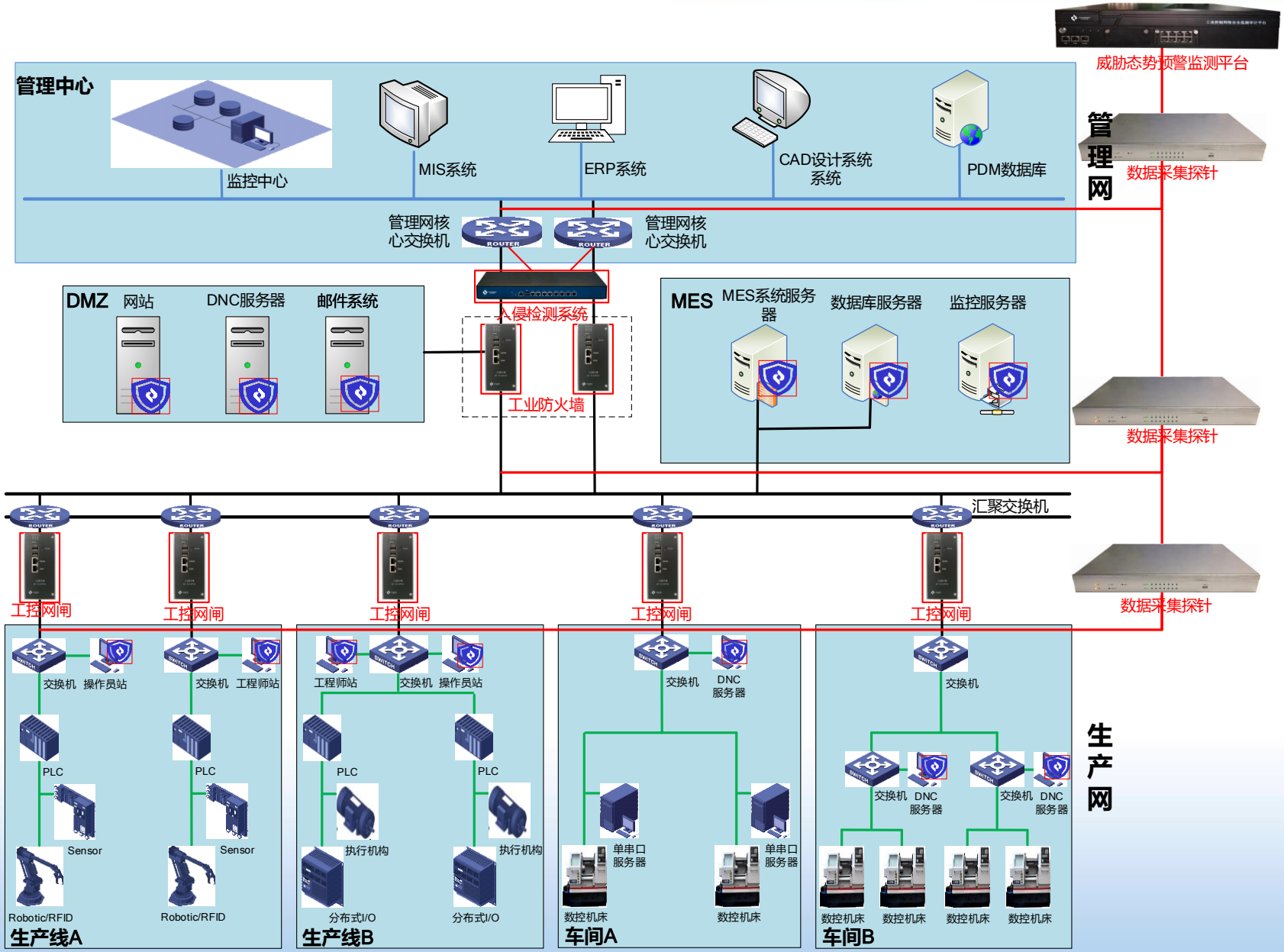
02 预警态势感知平台建设的总体设计

03 预警态势感知部署方案

04 预警态势感知部署的典型案例


火电厂
生产控制大区
管理信息大区
控制区（安全区 I）
SIS（安全区 II）
I区工控安全采集器
II区工控安全采集器
III区工控安全采集器
横向隔离
交换机
厂级安全监控预警中心
防火墙
操作员站
站控层交换机
间隔层交换机
防孤岛保护装置
主变测控柜
公用测控柜
工程师站
SIS接口机
=1DCS控制器
=2DCS控制器
AVC
PSL
SIS交换机
MIS核心交换
WEB应用服务器
SIS服务器
镜像服务器
数据库
MIS服务器群组
OA服务器
WEB服务器
磁盘阵列
TLMIS服务器
备份服务器
RTU远动装置
五防
AGC
辅控系统
辅控系统接口机
NCS
NCS接口机
ECS
ECS接口机
UPS1
UPS2
GPS1
GPS2
OPS


生产控制大区
管理信息大区
控制区（安全区 I）
非控制区（安全区 II）
厂级安全
监控预警中心
防火墙
交换机
正向隔离
交换机
正向隔离
交换机
I区工控安全
采集器
II区工控安全
采集器
III区工控安全
采集器
二平面交换机
#2主机
#1主机
工程师站
历史数据1
历史数据2
PMU
AVC
故障录波
保信子站
交换机
远控中心交换机
正向隔离
交换机
正向隔离
MIS核心交换
防火墙
互联网
WIS服务器
互联网PC
公用LCU
开关站LCU
1#机组LCU
2#机组LCU
3#机组LCU
调度工作站
梯级水库
调度自动化
SIS服务器
水情测报
水电厂水库
调度自动化
OA服务器
WEB服务器
磁盘阵列
防孤网保护
装置
主变测控柜
公用测控柜
操作员站
操作员站
TLMIS服务器
备份服务器


威胁态势预警监测平台
管理网
数据采集探针
管理中心
监控中心
MIS系统
ERP系统
CAD设计系统
系统
PDM数据库
管理网核心交换机
管理网核心交换机
DMZ
网站
DNC服务器
邮件系统
入侵检测系统
工业防火墙
MES
MES系统服务器
数据库服务器
监控服务器
数据采集探针
汇聚交换机
数据采集探针
工控网闸
工控网闸
工控网闸
工控网闸
工控网闸
交换机
操作员站
交换机
工程师站
工程师站
交换机
操作员站
交换机
DNC服务器
交换机
PLC
PLC
PLC
PLC
Sensor
Sensor
执行机构
执行机构
Robotic/RFID
Robotic/RFID
分布式I/O
分布式I/O
单串口服务器
单串口服务器
数控机床
数控机床
交换机
交换机
DNC服务器
交换机
DNC服务器
数控机床
数控机床
数控机床
数控机床
生产线A
生产线B
车间A
车间B
生产网

Thank you for your attention!

水利部机电所工控安全测评中心