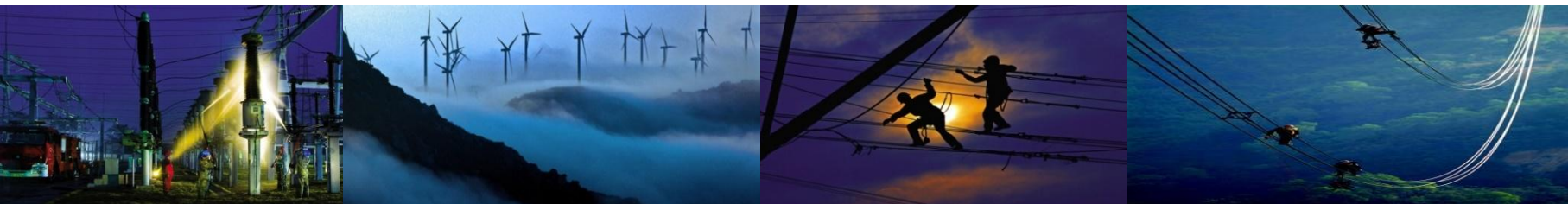


火电厂控制系统信息安全主动防御技术



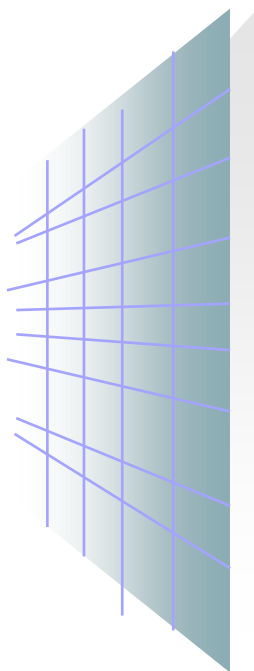
广东电网有限责任公司电力科学研究院



报告人：陈世和

2016年7月20日

报告提纲



1

火电厂安全风险点分析

2

主动防御的概念

3

主动防御的工控网络安全技术

4

研究与展望

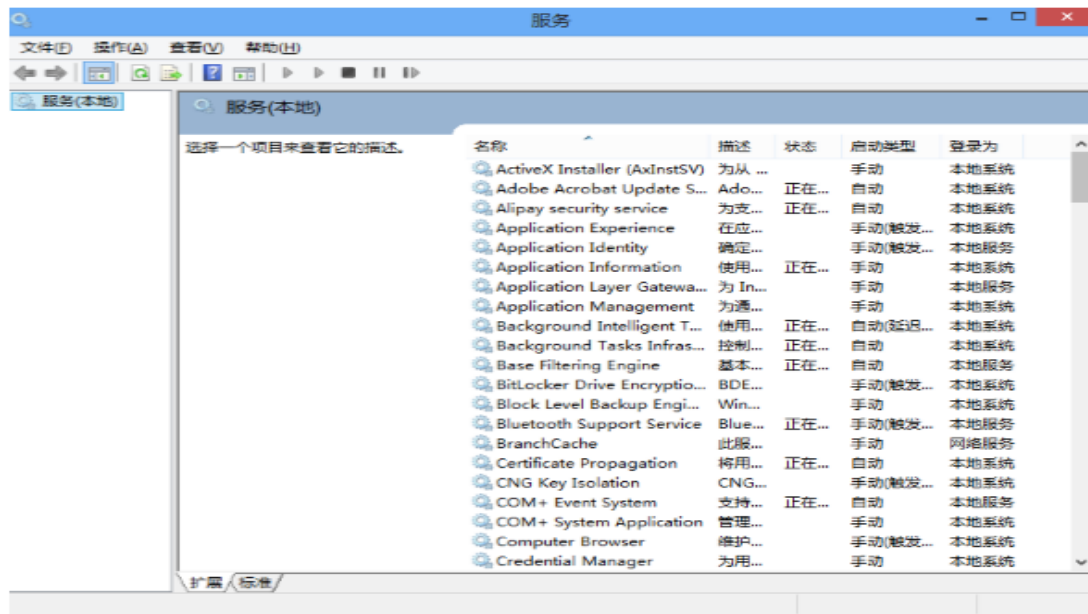


01

火电厂安全风险点分析

火电厂安全风险点分析



大量系统使用缺省配置




不必要的端口或服务没有被关闭，导致系统脆弱性上升

不安全的网络通信协议

 没有更新的补丁，对于已知的RPC / DCOM漏洞来说OPC是脆弱的

 分布式网络协议，MODBUS，PROFIBUS，以及其他协议，是公开的，
 很容易伪造数据包

 工业控制协议通常很少或根本没有内置的安全功能

 许多ICS的协议传输介质之间的明文传输的消息，使得它们很容易被对手窃听。

控制设备漏洞和后门



漏洞信息

漏洞名称: emerson 危险级别: 高 中 低 信息

漏洞其他: --请选择--

标签: Apache BIND Cisco Chrome DB2 Firefox 更多

查询 重置

收起

漏洞列表

- 漏洞列表 (0/18)
- 工业控制系统漏洞 (0/18)
- 其他工控 (0/18)
- Emerson DeltaV 信任管理漏洞 (CVE-2014-2350)
- Emerson DeltaV 权限许可和访问控制漏洞 (CVE-2012-4698)
- Emerson DeltaV 拒绝服务漏洞 (CVE-2012-4698)
- Emerson DeltaV 缓冲区溢出漏洞 (CVE-2012-4698)
- Emerson DeltaV 多个产品任意文件重写漏洞 (CVE-2012-4698)
- Emerson DeltaV 多个产品缓冲区溢出漏洞 (CVE-2012-4698)
- Emerson DeltaV 多个产品安全漏洞 (CVE-2012-4698)
- Emerson DeltaV 多个产品SQL注入漏洞 (CVE-2012-4698)
- Emerson DeltaV 多个产品任意代码执行漏洞 (CVE-2012-4698)
- Emerson DeltaV 信任管理漏洞 (CVE-2014-2350)
- Emerson DeltaV 权限许可和访问控制漏洞 (CVE-2012-4698)

漏洞信息

漏洞名称: Emerson DeltaV 信任管理漏洞 (CVE-2014-2350)

漏洞类型: ipv4 ipv6

更新时间: 2014-12-03

漏洞编号: 000330AD

影响平台: Emerson DeltaV 10.3.1, 11.3, 11.3.1, and 12.3

危险级别: 高危险

CVSS分值: 7.5

关闭

例：艾默生控制系统漏洞



危险级别: 高 中 低 信息

更多查询条件

漏洞信息

漏洞名称: Siemens RuggedCom ROS安全漏洞 (CVE-2012-4698)

漏洞类型: ipv4 ipv6

更新时间: 2014-12-04

漏洞编号: 000330EC

影响平台: Siemens RuggedCom Rugged Operating System (ROS) before 3.12, ROX I OS through 1.14.5, ROX II OS through 2.3.0, and RuggedMax OS through 4.2.1.4621.22

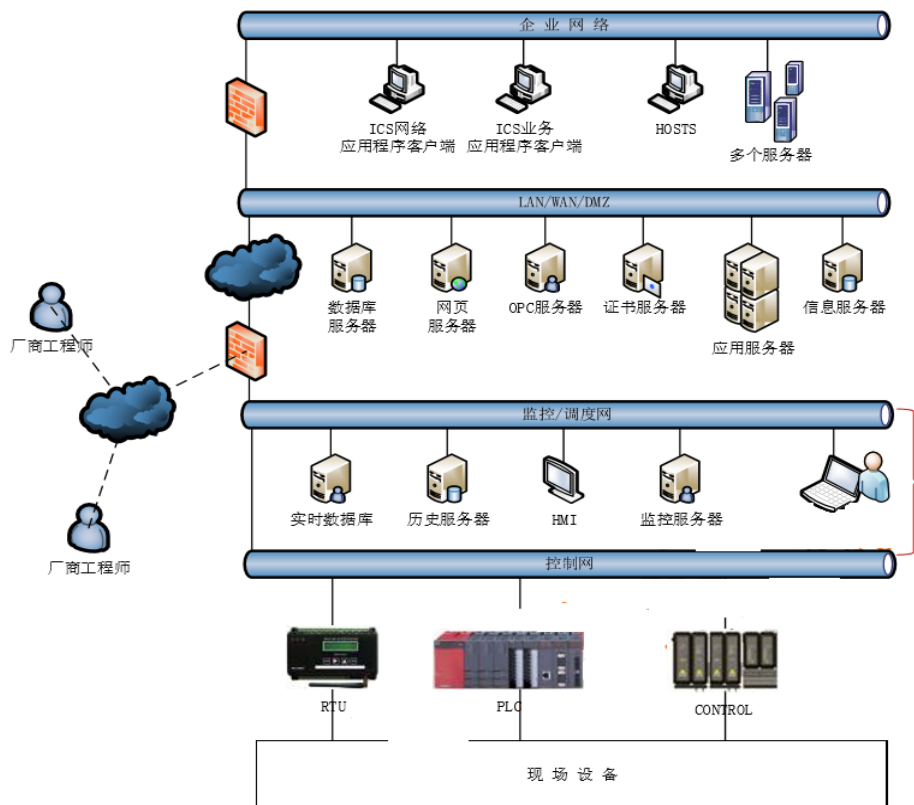
危险级别: 中危险

CVSS分值: 4.3

关闭

例：西门子PLC设备漏洞

火电厂安全风险点分析



未安装防火墙



缺少网络访问控制



弱防火墙规则



弱口令



不安全的协议



电力生产控制系统风险点分析

1

- 移动介质管理（重点是USB）只有管理制度，没有有效的技术手段进行防护，APT恶意程序极易通过移动介质传播到生产控制网络
- 操作员、工程师站操作系统多采用Windows XP、Windows 2000等，系统漏洞极多，容易被利用攻击；没有有效的系统加固技术手段和病毒防护能力

本体安全

2

- 针对电力监控系统，缺少必要的网络审计手段和针对工业级恶意代码的入侵检测系统；系统补丁未及时更新
- 针对一区、二区之间的逻辑隔离力度不够；缺乏通讯端口的管控和防护

结构安全

3

- 日志管理：未对工控系统关键设备进行信息安全策略设置；
- 安全审计：未对工控系统帐户进行定期审计，且缺乏对违规操作、越权访问行为审计能力

行为安全

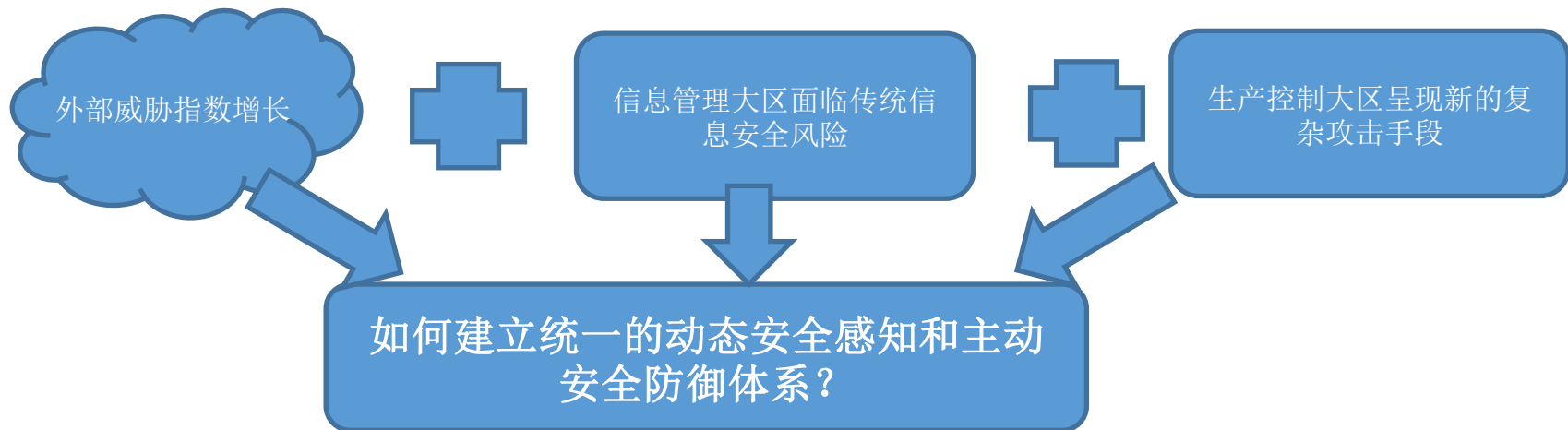
4

- 缺乏行而有效的管理制度和防护方案，缺乏有安全防护经验的现场管理和维护人员；
- 现有的安全设计方案需要加强评估，安全设备维护过分依赖第三方；
- 生产控制系统权限管理较弱，密码使用弱口令

管理和运维

电力监控系统面临的安全新风险

- 攻击者专业程度越来越高，对电力工业控制系统及规约协议了解充分
- 攻击方式更加全面，社工技巧更加高明（如远程U盘控制）
- 内部安全风险缺少资产盘点，脆弱性难以实时评估
- 外部威胁应对不足





02

主动防御的概念

主动防御的概念

控制系统网络安全技术与传统IT安全有本质的区别

工控网络的特点决定了基于办公网和互联网设计的信息安全防护手段（如防火墙、病毒查杀等）无法有效地保护工控网络的安全

网络通讯协议不同

大量的工控系统采用私有协议

对系统稳定性要求高

网络安全造成误报等同于攻击

体系结构不同

系统横向分区，多重网络

更新代价高

无法像办公网或互联网那样通过补丁来解决安全问题

实时性要求高

在不影响生产的情况下实现安全防护

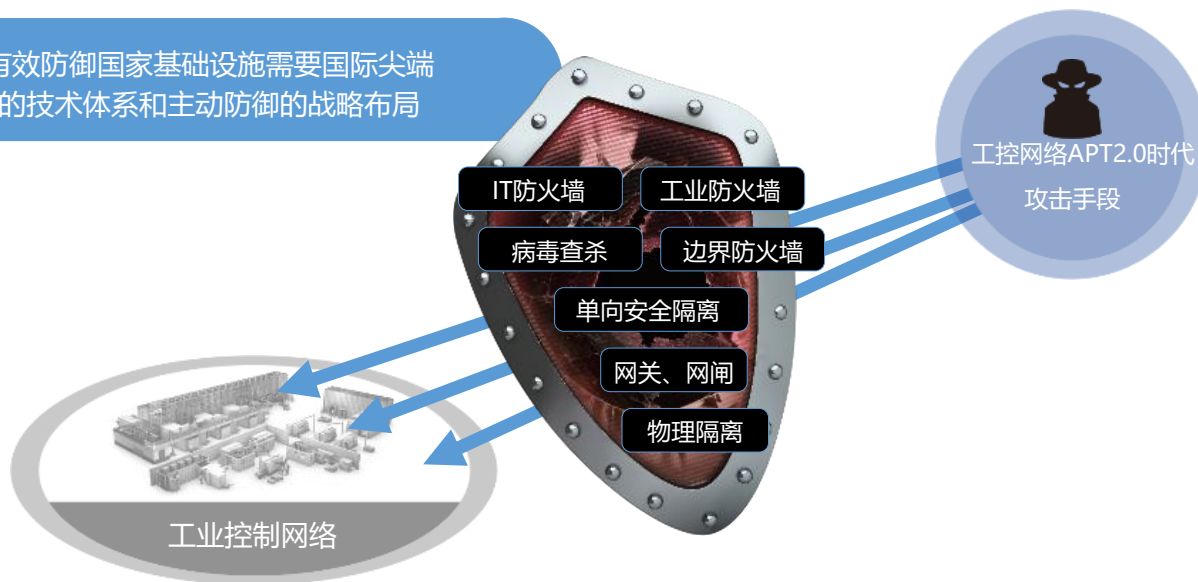


工业控制网络

主动防御的概念

基于信息网络安全防护手段以及现有的工控网络防护手段在APT2.0时代的攻击面前已经成为“皇帝的新衣”

有效防御国家基础设施需要国际尖端的技术体系和主动防御的战略布局



主动防御的概念

单纯依赖隔离

物理隔离的变种，网关、网闸、单向隔离，隔离背后是脆弱的，现代高端持续性攻击都是针对隔离系统的。

纵深防御体系

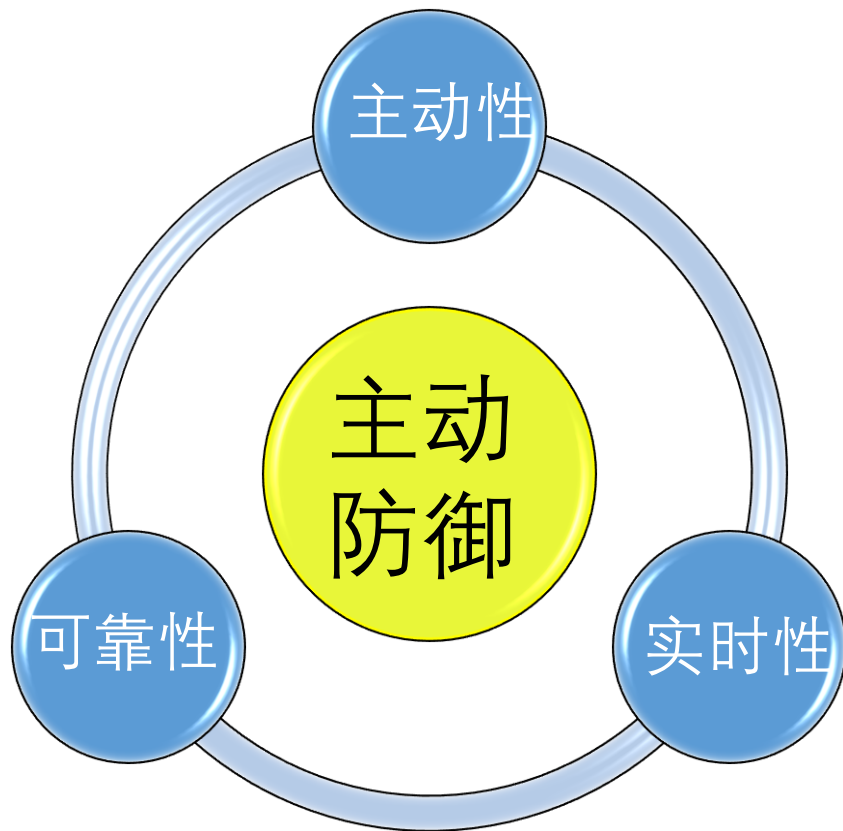
由传统信息安全厂商提出的，大多数项目演变为信息安全产品的简单堆砌，不能完全适应工业网络安全的特点

由工业控制系统内部生长的主动防御体系

适应工业控制网络的特点，通过基础硬件创新来实现，低延时，高可靠，可定制化，持续更新，简单化的实施和操作等

工控网络安全防护理念的演变

主动防御理念



能够抵御针对工控系统的攻击，不影响工控系统运行

——可靠、透明、主动、实时的Bypass系统

主动防御理念

建立主动防御系统过程



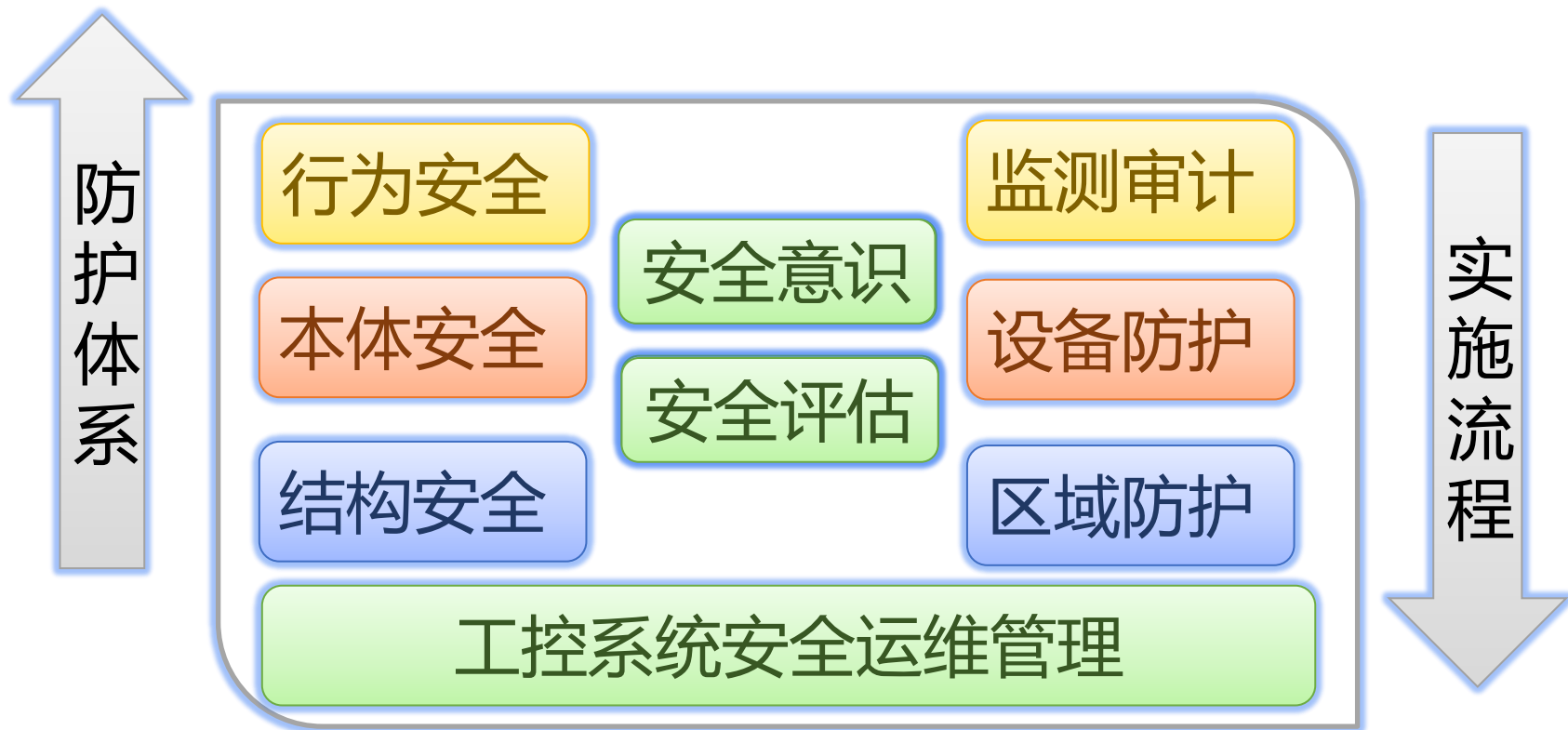
持续改进



03

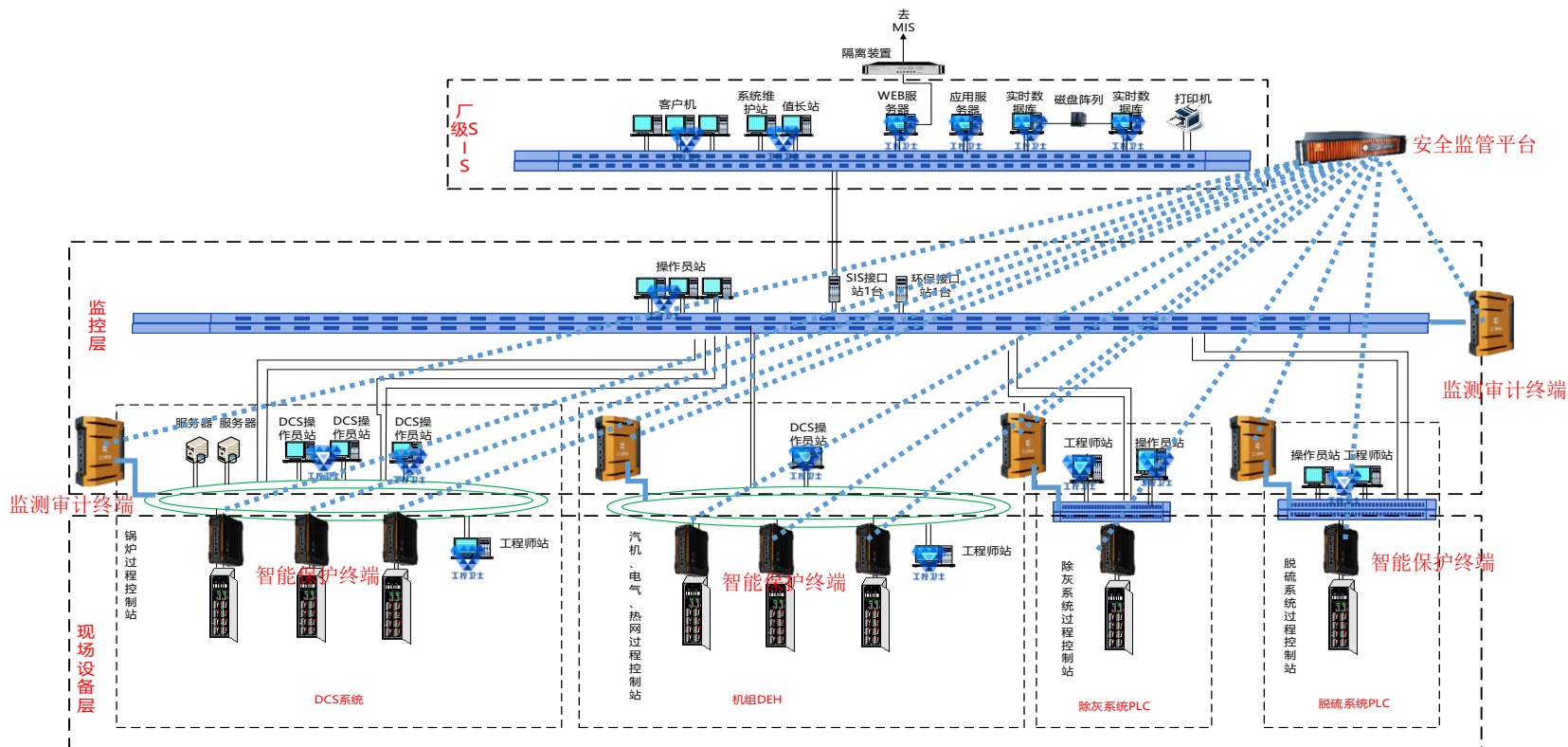
主动防御的安全防护技术

主动防御的安全防护技术



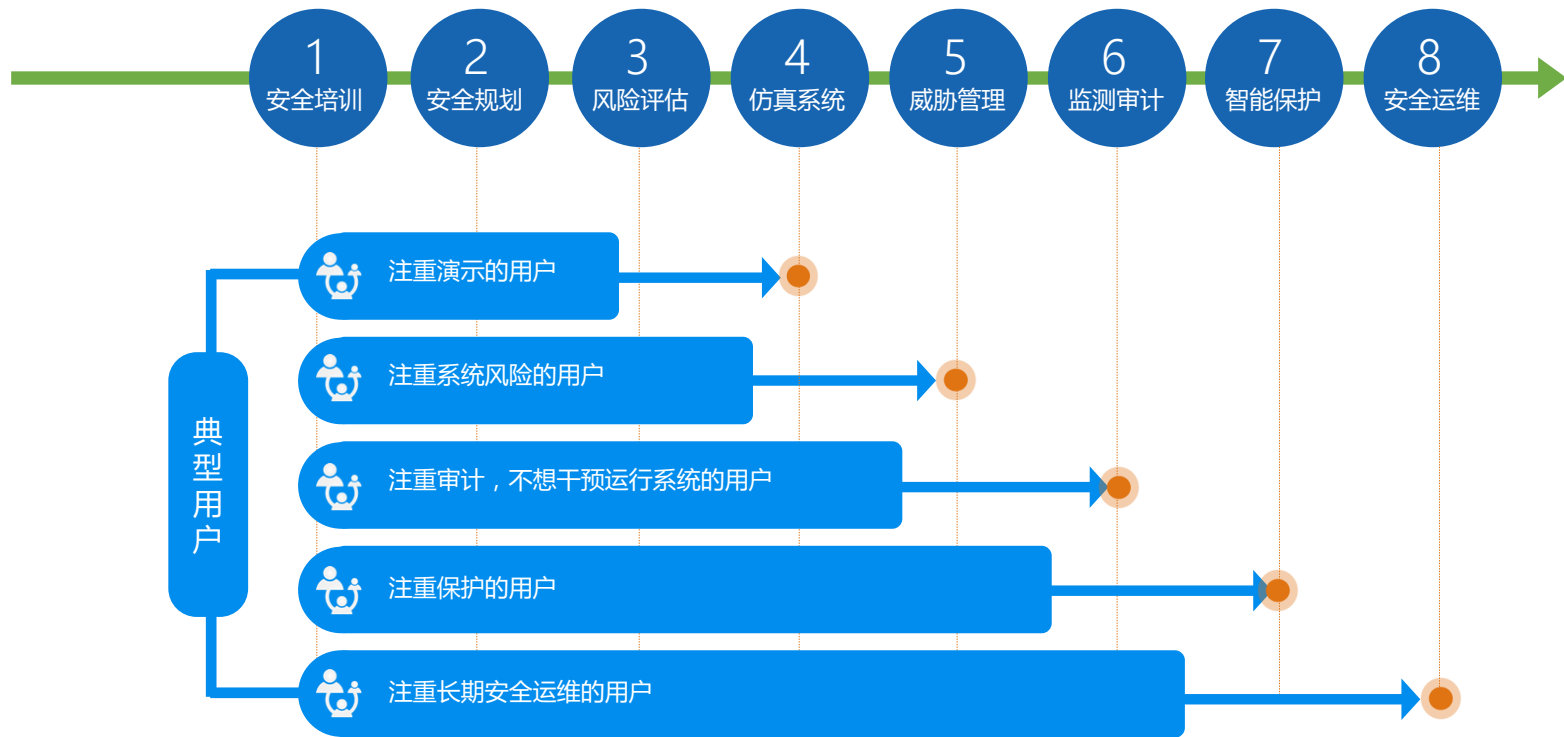
火电厂工控安全防护体系建设思路

主动防御的安全防护技术



火电厂工控网络安全解决方案

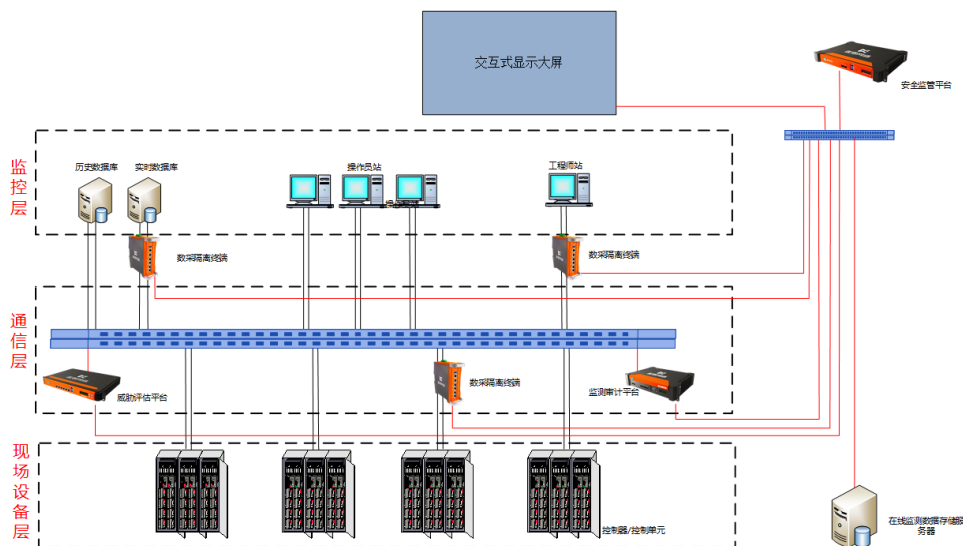
主动防御的安全防护技术



火电厂工控网络安全解决方案分步实施

主动防御的安全防护技术

- 工控网络流量采集系统
- 网络流量收集及实时分析系统
- 在线监测数据挖掘系统



基于安全监管平台的仿真部署

主动防御的安全防护技术

通过USB病毒对终端进行攻击方式

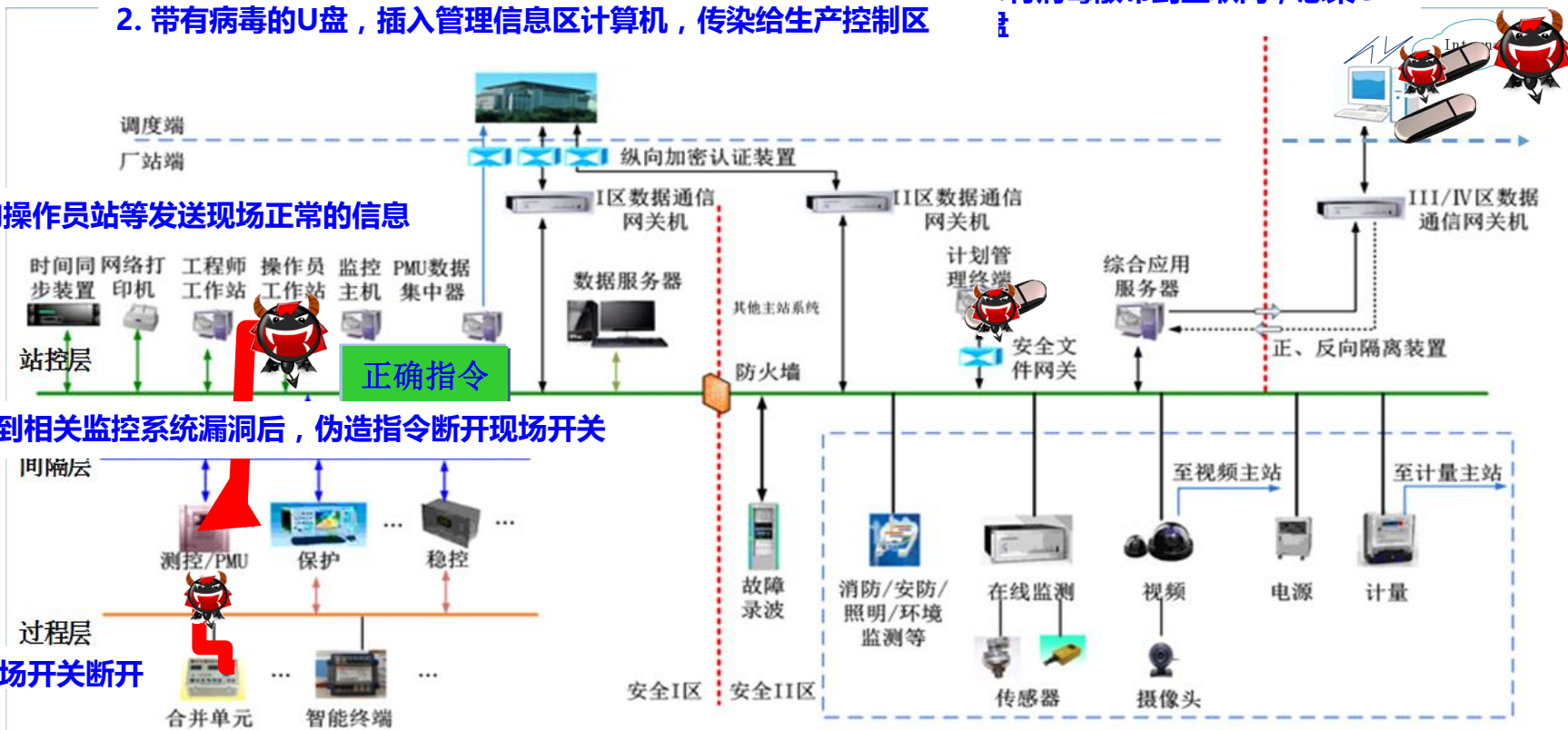
2. 带有病毒的U盘，插入管理信息区计算机，传染给生产控制区

1. 将病毒散布到互联网，感染U盘

5. 向操作员站等发送现场正常的信息

3. 找到相关监控系统漏洞后，伪造指令断开现场开关

4. 现场开关断开



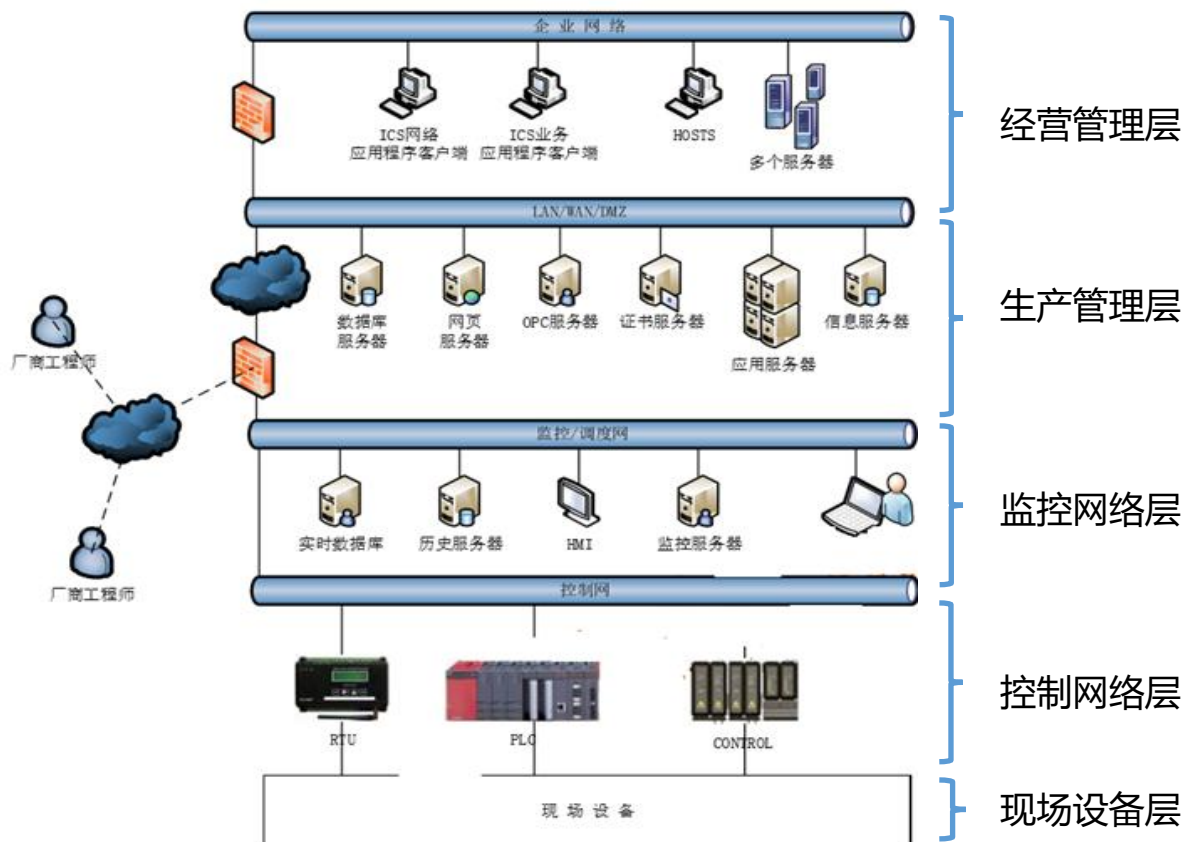
主动防御的安全防护技术

主动防御技术



主动防御的安全防护技术

主动防御的网络安全技术



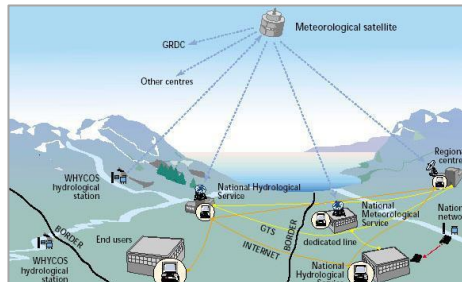


04

研究与展望

研究与展望

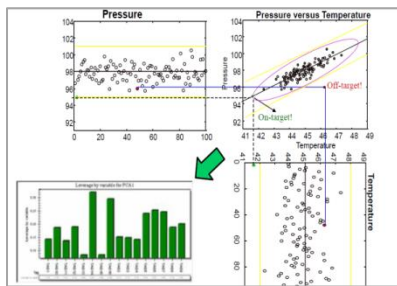
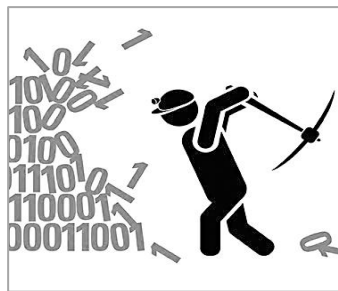
主要研发内容



软硬件异构冗余控制器研究与开发

控制网络多协议并行通信技术研究开发与

操作站主动防御技术研究开发与



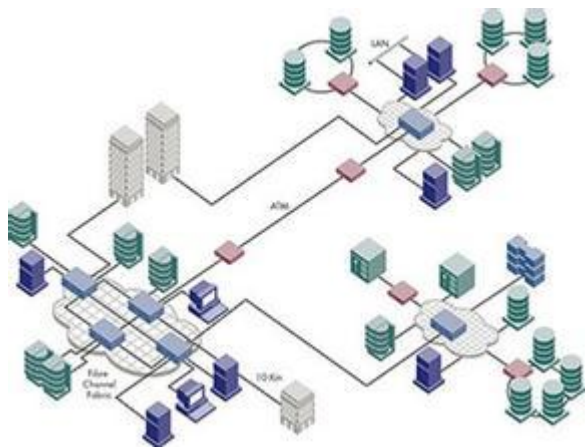
控制软件及应用软件安全技术

具备主动防御功能工控系统的示范应用

电厂安全数据在线监测平台

研究与展望

软硬件异构冗余控制器研究与开发



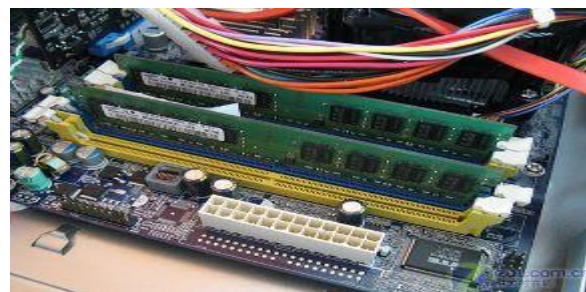
异构冗余



控制与通信控制器分离



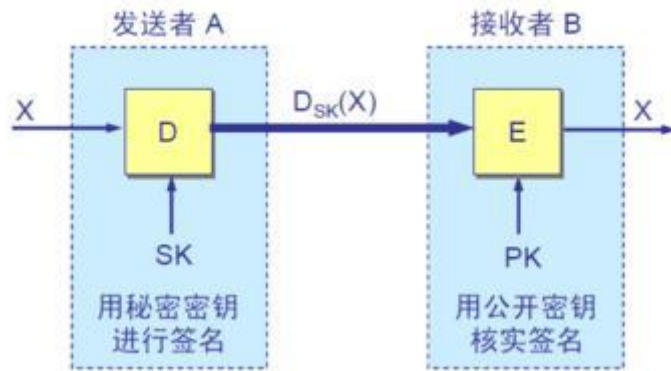
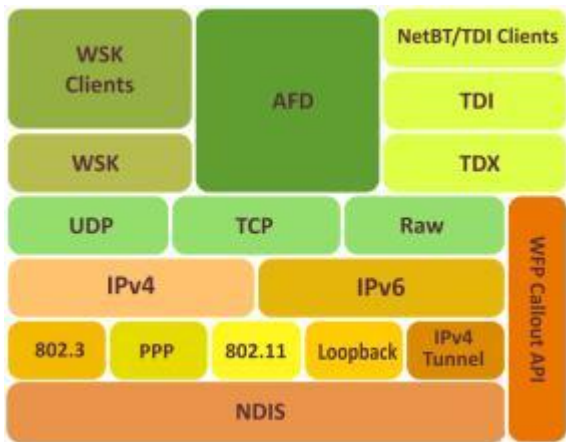
网络接口软硬件加固



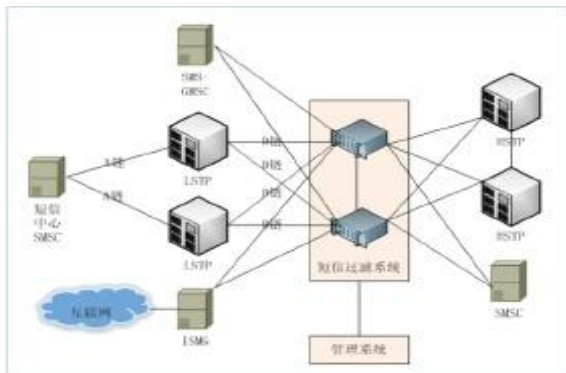
内存保护与动态重构

研究与展望

控制网络多协议并行通信技术研究开发

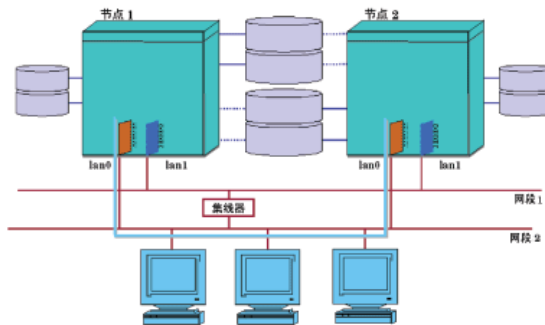


多通信协议并行



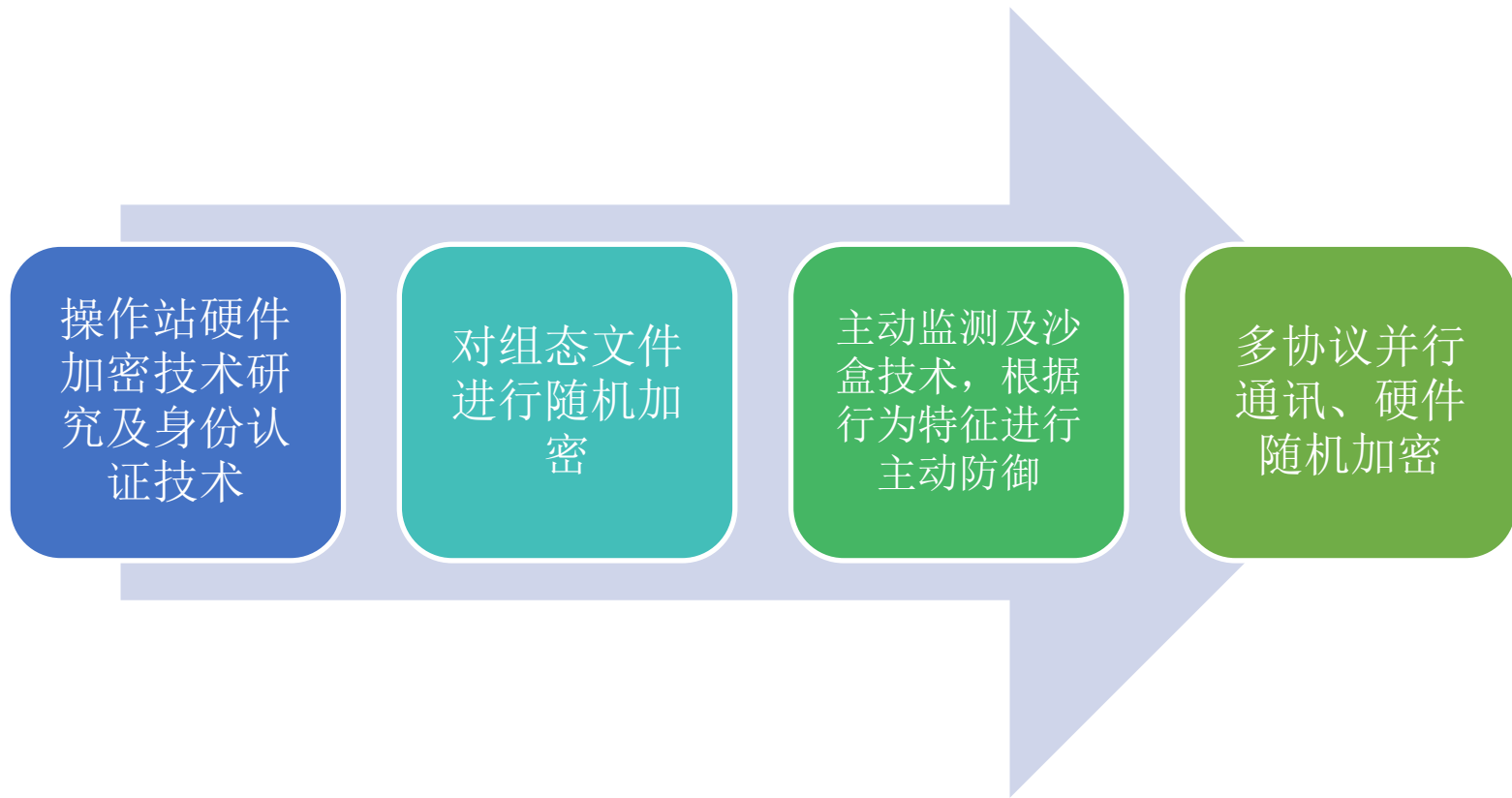
网络报文过滤

随机加密



端口封闭

研究与展望



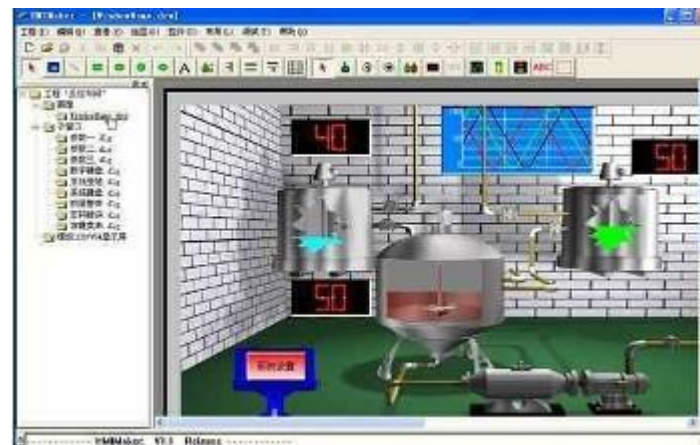
操作站主动防御技术研究与开发

研究与展望

控制软件及应用软件安全技术



应用软件白名单机制



组态软件身份认证及随机加密



控制指令加密与交互验证

研究与展望

具备主动防御功能的工控系统在电力行业的示范应用

开发一套具备主动防御功能的工业控制DCS

01

“安全分区、网络专用、横向隔离、纵向认证、综合防护”

02

具备整体安全防护体系架构

03

具备组件级的动态安全防护技术

04

05

应用在600MW或以上并网发电机组

06

满足电厂生产的控制要求，同时具备通信健壮、数据加密、系统冗余等安全特征

07

不影响控制系统实时性能，能够抵御典型漏洞攻击，防御成功率达到80%以上

研究与展望



建立电力安全大数据平台

网络数据



设备数据

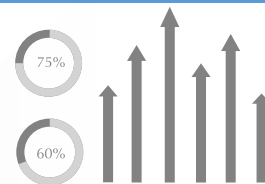


电力安全大数据平台

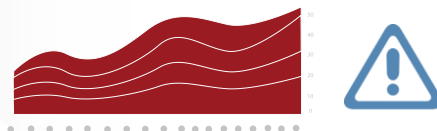
持续获取机器学习实时处理

- ✓ 兼容广泛数据源和设备类型
- ✓ 各种模板方便行业应用的定制
- ✓ 数据处理引擎提供强大的处理能力
- ✓ 智能分析引擎精确定位问题风险

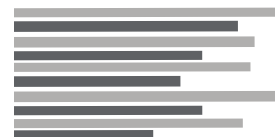
综合监控分析



安全检测防范

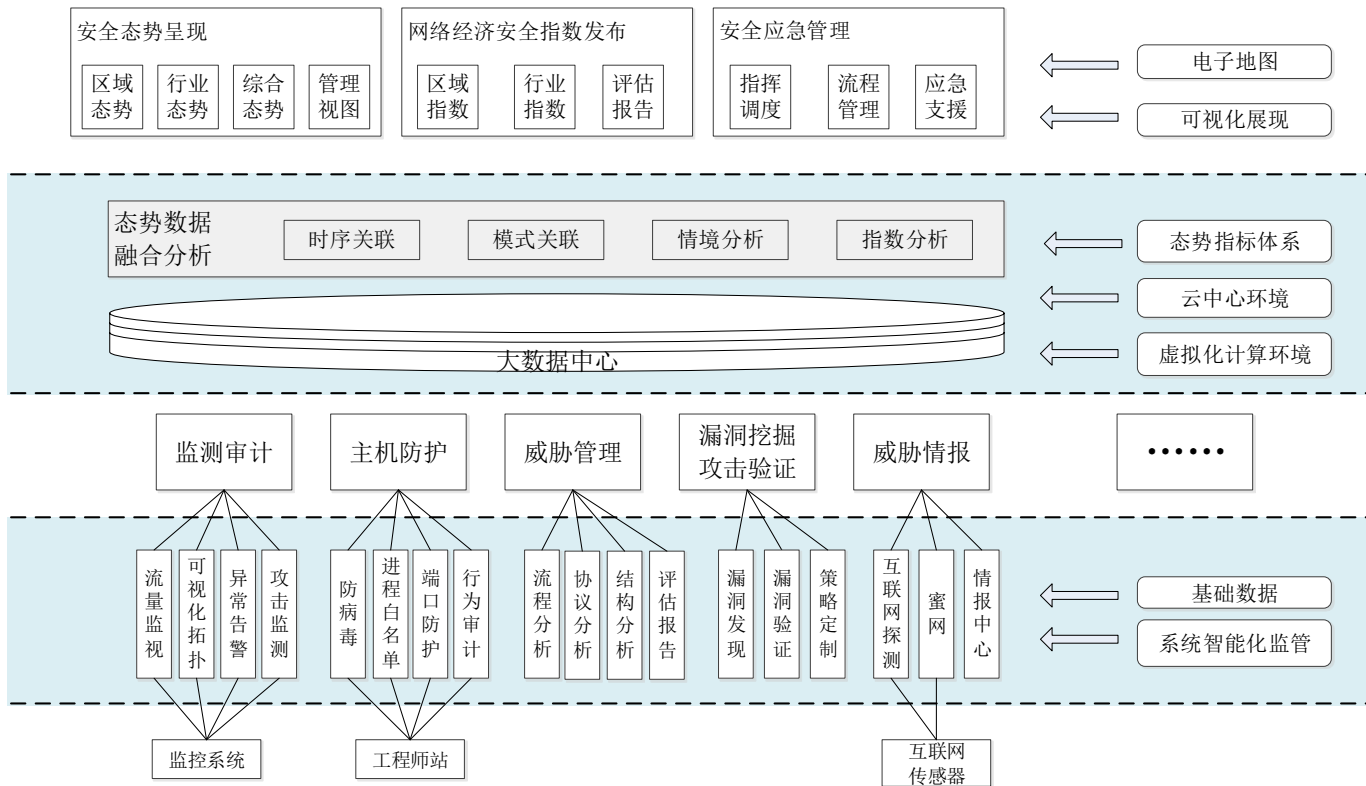


实时洞察预警



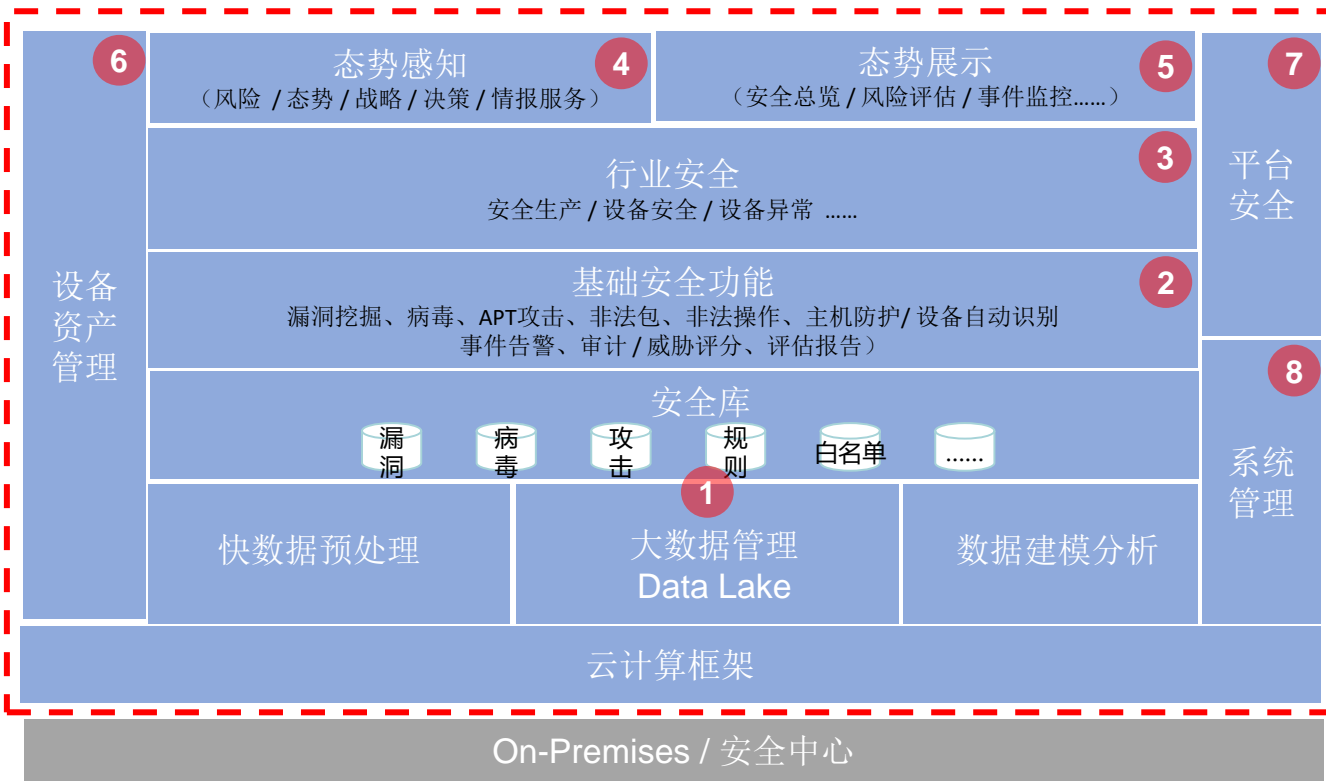
研究与展望

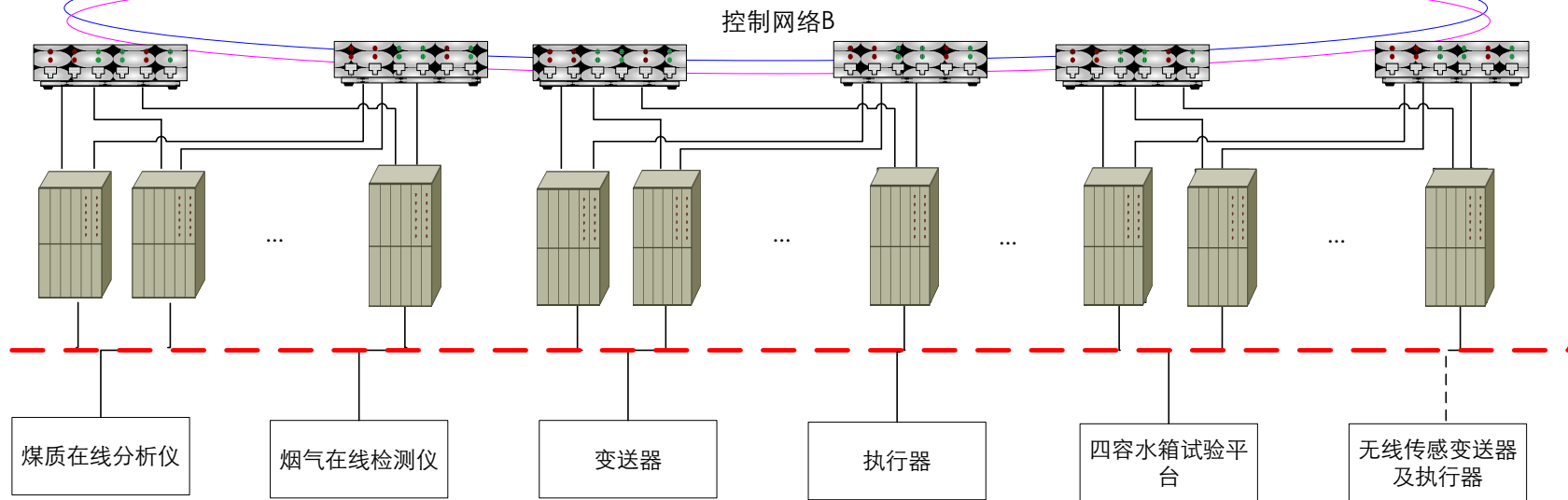
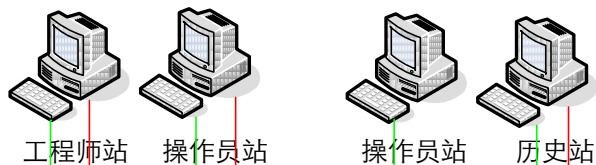
安全大数据平台技术架构



研究与展望

安全大数据平台功能





DCS最小化系统控制平台

DCS最小化系统：艾默生、GE新华(XDPS400+, OC6000e)、和利时、国电智深、ABB、西门子、浙大中控

展 望

- 电厂工控系统信息安全问题严峻
- 亟需开发具备主动防御的工控系统
- 建立电厂安全数据在线监测平台
- 形成电厂控制系统网络安全技术标准

汇报完毕

谢谢各位领导与专家！

