工业控制系统信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

井工煤矿工业控制网络安全防护体系

汇 报 人：上海三零卫士信息安全有限公司 李绪国

汇报日期： 2019年5月9日

目 录

CONTENTS

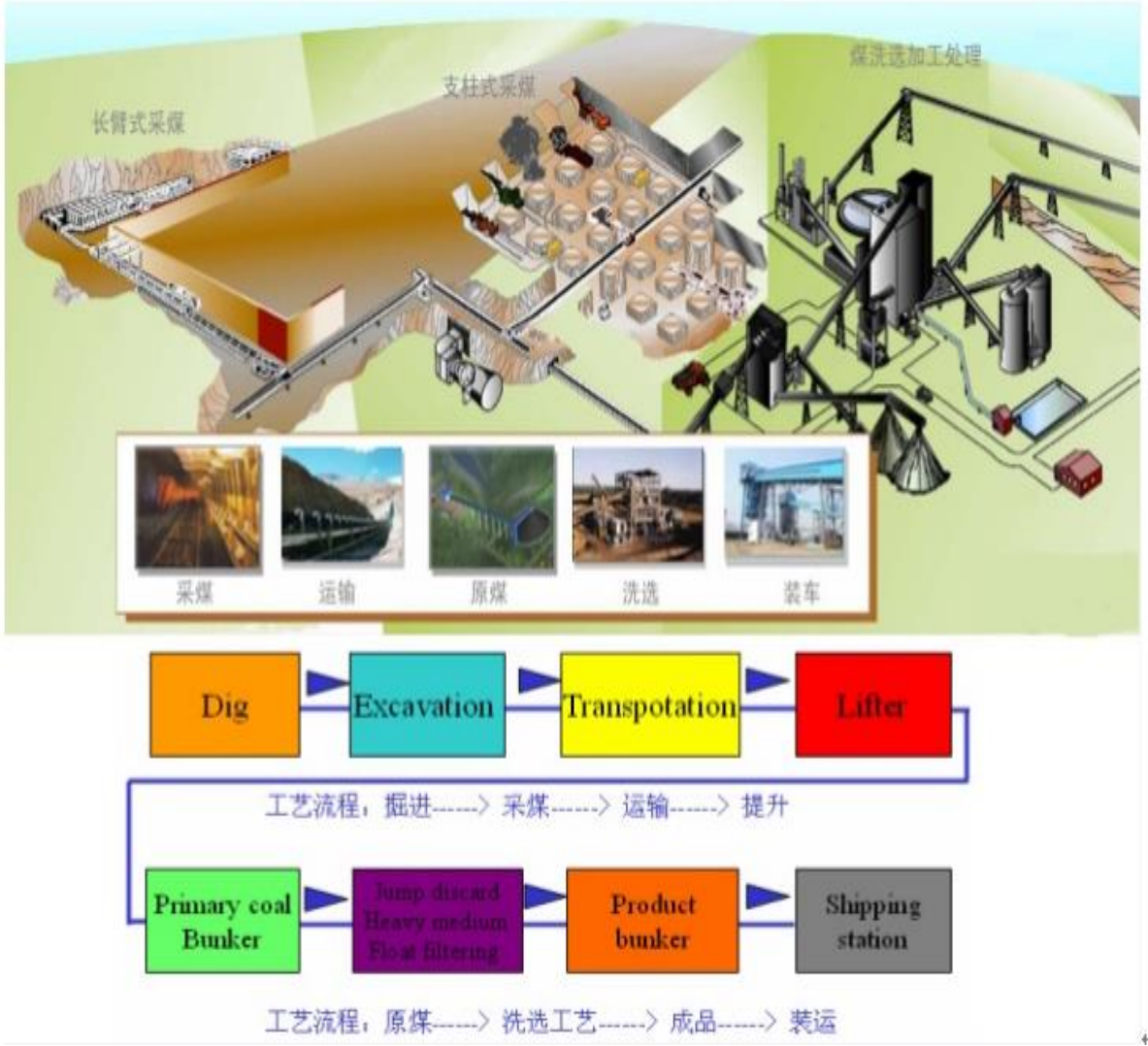
井工煤矿工业控制网络特点

兼有流程工业和离散工业特点

- ✓ 采煤和掘进两大生产系统，每个系统形成相对独立的生产流程，两大流程涉及的工控系统相对独立运行，信息相对独立；
- ✓ 开采：涉及开采、运输、洗选、排水、环境监控等工业控制系统，某个系统一旦出现运行故障，直接造成生产流程中断；
- ✓ 掘进：涉及掘进、运输、排水、环境监控等工业控制系统，某个系统一旦出现运行故障，直接造成生产流程中断。

系统的稳定运行至关重要

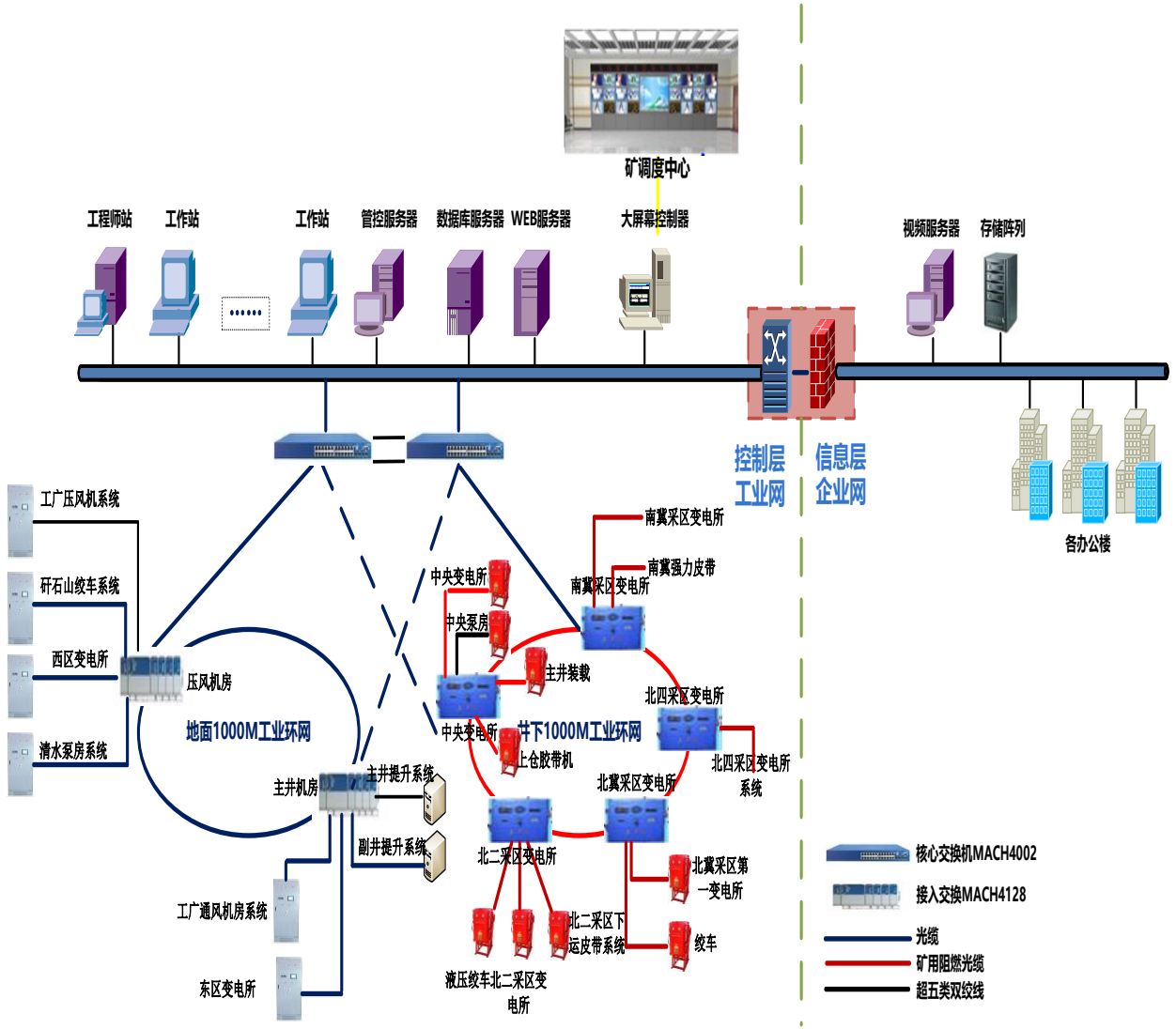
- ✓ 排水系统、供电系统、运输系统等一旦出现故障，造成生产中断，给企业带来直接经济损失；
- ✓ 安全监控系统、瓦斯抽放系统、风机运行监控系统、束管监测系统等一旦出现故障，可能引发重特大生产安全事故，应属于关键信息基础设施。



工业控制系统与信息系统深度融合

随着PC架构计算机应用和基于IEEE802.3的工业以太网普及，工业控制系统与传统信息系统深度融合，大量采用TCP（UDP）/IP网络协议和OPC、ModbusTCP等统一接口标准，工业以太网逐渐取代传统总线，不同系统间的“信息孤岛”现象正在消失。

- ✓ **信息层**：可与生产管理系统、安全监控系统、生产调度指挥系统等汇接，按信息流方式实现煤矿现代化管理。
- ✓ **控制层**：由百兆、千兆工业以太网构成井上、下冗余环网，通过工业以太网或现场总线接入网络控制器、工业视频等控制系统。
- ✓ **设备层**：设备的执行机构和网络传感器通过以太网交换机接入网络。
- ✓ **组态软件与通信协议**：使用IFix、Intouch、PSI、Wincc、Rsriew等组态软件，与子系统常采用OPC通讯，实时采集数据。



井工煤矿工业控制网络安全问题

➢ 网络边界防护不力

✓ **生产控制网与办公网边界防护薄弱**

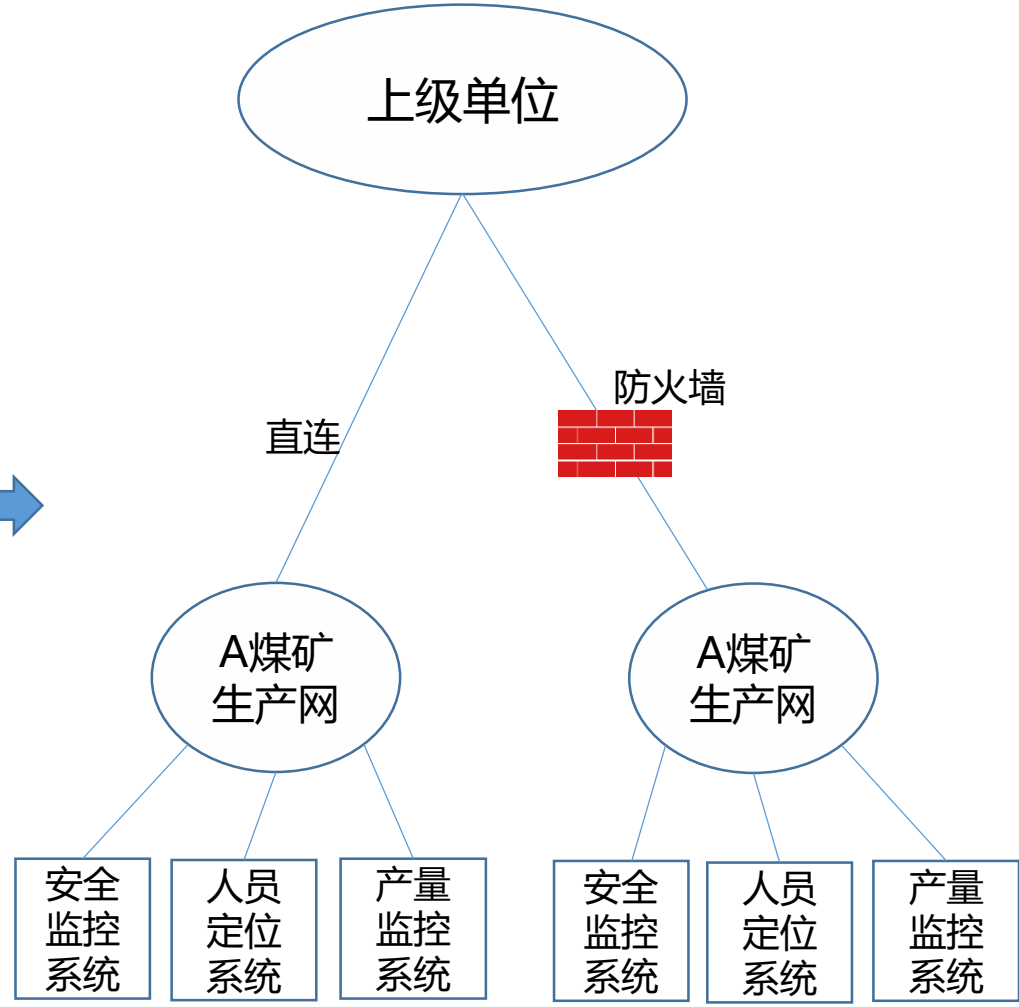
两网间防护措施不到位，仅通过防火墙连接，但防火墙发挥作用有限；或无防护措施，内网计算机可直接控制生产设备，存在巨大安全隐患。

✓ **工业控制网络与专网间的安全防护措施不到位**

人员定位、安全监控、产量监控等系统联网，直接暴漏在专网中，病毒传播和网络攻击风险大。

✓ **工控网络内部缺乏区域隔离防护手段**

网络结构缺少安全考虑，各工控系统全部接入环网，系统间无法分区分域防护，只要入侵生产网，便可攻击环网内的所有工控系统。



● 工控设备防护效果不理想

- ✓ 大型设备控制器和监控软件多采用主流国内外知名PLC和组态软件，成功利用设备漏洞进行网络攻击的可能性高；
- ✓ 设备维护完全依赖厂商或第三方，无法实现自主安全可控；
- ✓ 主机、服务器漏洞补丁更新严重滞后，恶意攻击成本低，数据被窃取或系统被破坏可能性大。

● 网络监测和审计手段缺乏

- ✓ 缺乏主机、服务器以及交换机等网络节点等监测审计手段，无法及时发现病毒木马和恶意入侵行为，缺乏对违规操作、越权访问行为审计能力，不利于事件发生后的故障定位和追踪溯源；
- ✓ 系统主机及系统服务器USB端口随意使用现象普遍，无访问控制措施；
- ✓ 第三方设备维护管理松懈，缺乏对维修操作行为的审计。

● 管理体制机制不健全

- ✓ 网络安全管理机构、规章制度不完善，措施执行不到位；
- ✓ 安全管理职责不明确，机电管理部门只负责工控设备功能安全，信息管理部门人员无力介入；
- ✓ 工控网络安全应急预案缺失，难以与生产安全融合，存在无法及时处理事件和恢复生产的风险。

● 井下适用网络安全设备开发缓慢

- ✓ 井下工控网络安全保护处于空白状态；
- ✓ 开发取得煤安标志和井下设备许可证的网络安全设备迫在眉睫。

井工煤矿工业控制网络安全防护体系

合规性安全防护

- 2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》,2017年6月1日正式实施

- 《信息安全技术 网络安全等级保护基本要求》

- 2016年10月17日，工业和信息化部《工业控制系统信息安全防护指南》
- 2017年5月31日，工业和信息化部《工业控制系统信息安全事件应急管理工作指南》

- 2015年12月22日，国家安全生产监管总局令《煤矿安全规程（2016版）》

全国人民代表大会
The National People's Congress of the People's Republic of China

中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China

中国国家标准化管理委员会
STANDARDIZATION ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA

中华人民共和国工业和信息化部
Ministry of Industry and Technology of the People's Republic of China

中华人民共和国应急管理部
Ministry of Emergency Management of the People's Republic of China

分阶段逐步深入安全防护

中长期目标：

- 工控网络安全融入生产安全：安全质量标准化体系、作业规程、安全技术措施；
- 矿用许可安全防护产品研发与推广：煤安标志与防爆合格证；
- 安全自主可控：核心控制设备内生安全。

近期工作重点：

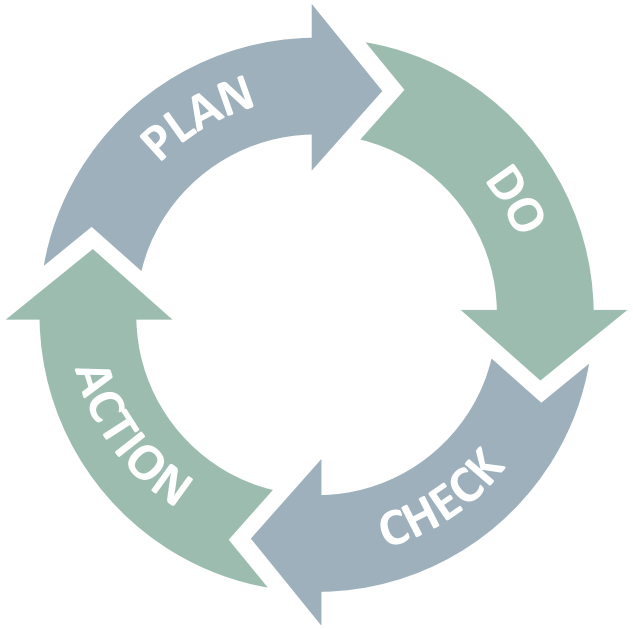
- 网络安全分等级保护；
- 纵深立体网络安全防护；
- 现有网络架构下的安全补偿加固：边界防护、监测审计、主机防护、应急响应；
- 管理体制机制与人才队伍建设。

全生命周期安全防护

包括计划准备、方案实施、结果评估和优化提升，四个步骤环环相扣形成PDCA安全环，它是爬楼上升式循环，每转动一周，工控网络安全防护水平上升一个台阶。

- P (PLAN)：计划准备
  - ✓ 安全技术培训
  - ✓ 系统风险评估
  - ✓ 安全方案咨询

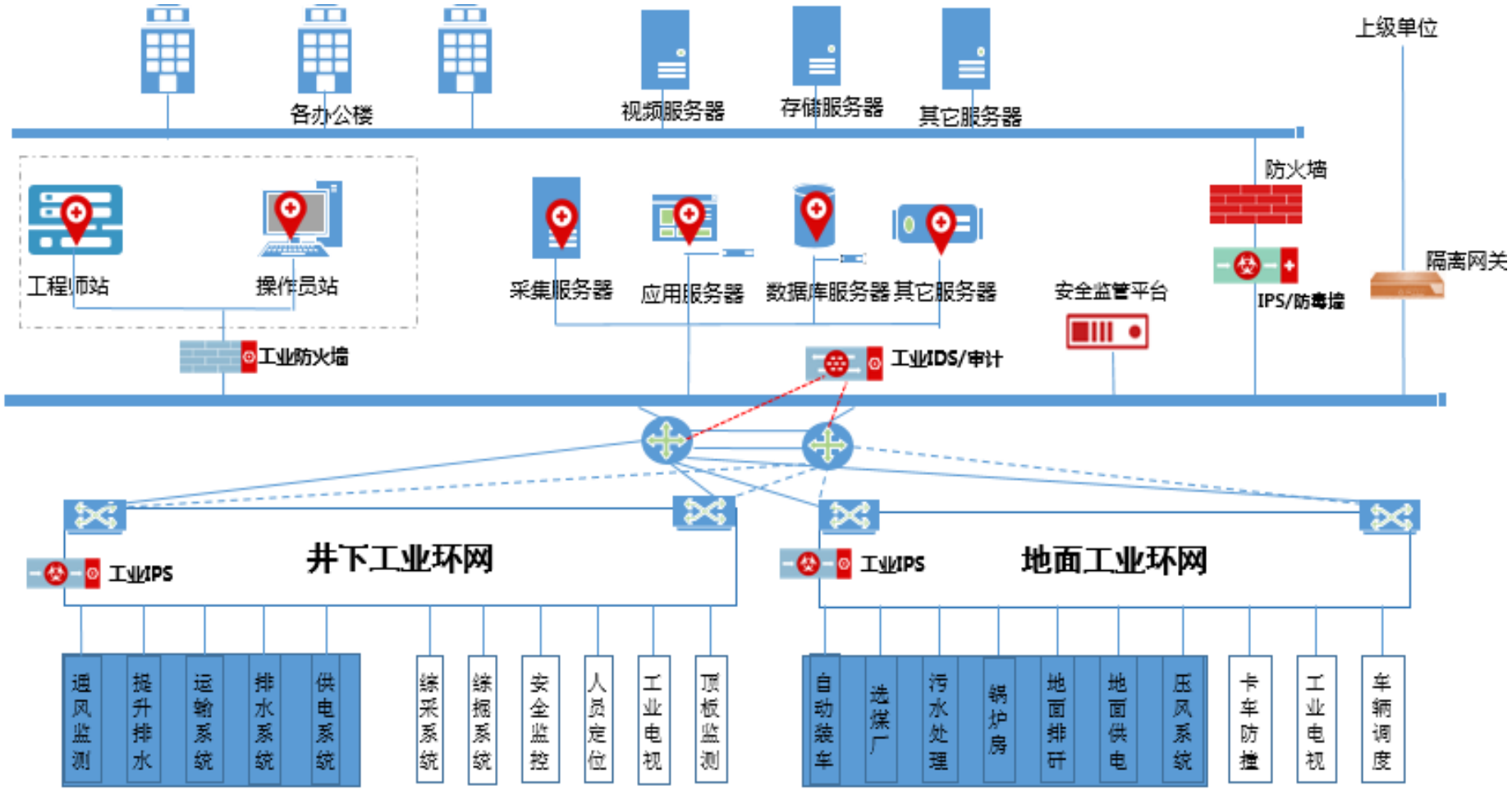
- A (Action & Acceleration)：优化提升
  - ✓ 系统安全防护工程改造
  - ✓ 安全管理制度完善
  - ✓ 人员队伍能力提升



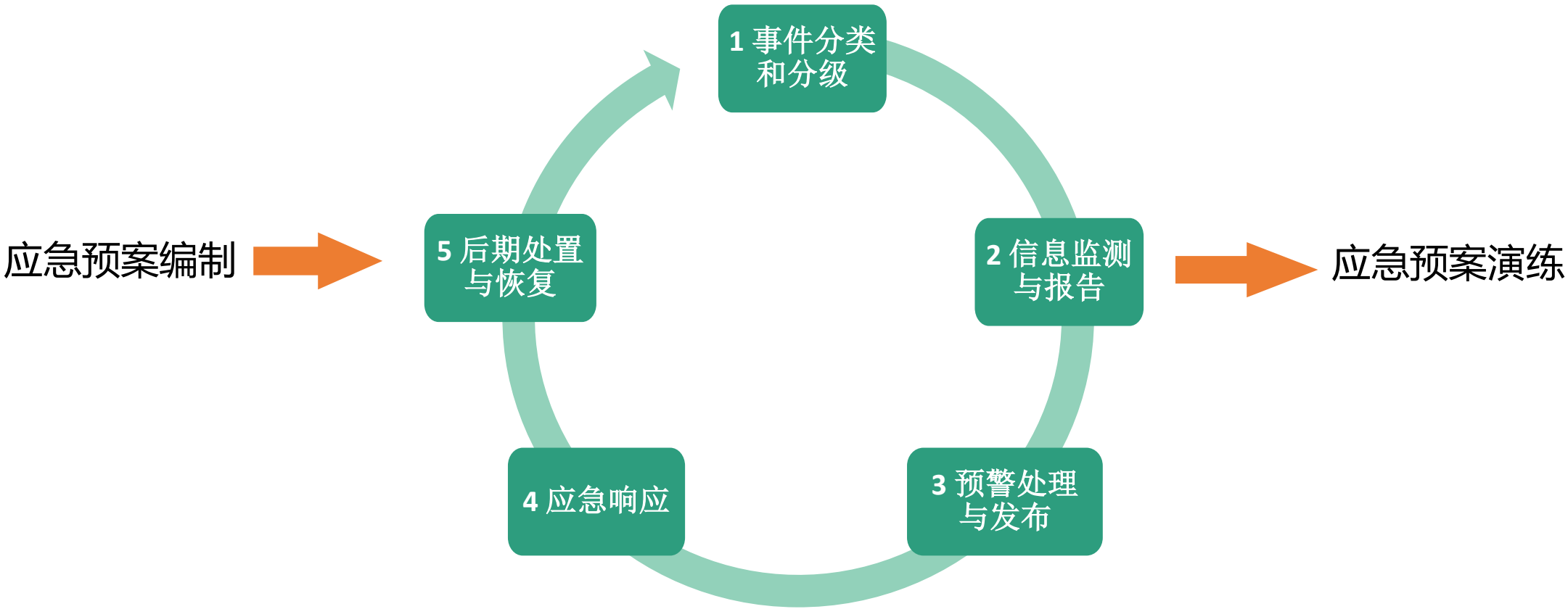
- D (DO)：方案实施
  - ✓ 系统定级与备案
  - ✓ 系统安全建设
  - ✓ 系统等保测评
  - ✓ 系统安全改造
  - ✓ 系统动态运维
  - ✓ 安全监督管理

- C (CHECK)：效果评估
  - ✓ 安全态势感知与监测预警
  - ✓ 动态安全风险自查
  - ✓ 第三方安全风险评估
  - ✓ 周期性系统等保测评

纵深立体网络安全防护


各办公楼
视频服务器
存储服务器
其它服务器
上级单位
防火墙
工程师站
操作员站
采集服务器
应用服务器
数据库服务器
其它服务器
安全监管平台
IPS/防毒墙
隔离网关
工业防火墙
工业IDS/审计
工业IPS
井下工业环网
工业IPS
地面工业环网
通风监测
提升排水
运输系统
排水系统
供电系统
综采系统
综掘系统
安全监控
人员定位
工业电视
顶板监测
自动装车
选煤厂
污水处理
锅炉房
地面排矸
地面供电
压风系统
卡车防撞
工业电视
车辆调度

事件应急响应与处置



《工业控制系统信息安全事件应急管理工作指南》（工信部信软[2017]122号）

三零卫士工控网络安全业务介绍

公司概况

上海三零卫士信息安全有限公司成立于2001年7月，是中国网安旗下专业从事信息安全服务、产品的高新技术企业。是“信息安全特色明显、IT服务能力卓越”的综合性安全服务企业。公司总部位于上海，在杭州、广州、南京、武汉、北京、成都等地设立了分支机构。客户覆盖政府、大型国企、涵盖及其他行业，全国累积约1500家，其中长期服务约500家。

业务覆盖：

- 安全服务业务
- 工控信息安全业务
- 信用与大数据业务
- 互联网情报业务

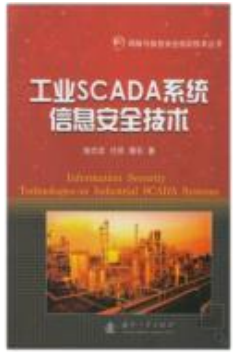
发明专利

工控发明专利				
序号	发明名称	申请号	专利号	备注
1	一种保护工业设备串口接头的方法及其装置	201310242574.5	ZL01310242574.5	授权日：2016.04.27
2	一种基于分区分域的工控系统信息安全资产识别方法	201510459623.X		等待实审提案
3	一种基于漏斗式白名单的工控网络信息安全监控方法	201510569030.9		一通回案实审
4	一种基于白名单矩阵的智能工控网络信息安全监控方法	201610953811.2		等待实审提案
5	一种基于 SCADA 系统的周期性异常检测的方法	201610953812.7		等待实审提案

自主漏洞

5.IEC-61850-8-1 (MMS)协议发现工具
6.KingView 6.53 SCADA HMI堆溢出漏洞
7.KingView 6.6 组态DOS漏洞
8.Misubishi FX3G DOS漏洞
9.Mitshbishi Q系列PLC远程关闭CPU模块
10.Mitsubishi GB-50a认证绕过漏洞，成功的攻击会允许未经授权的攻击者获得访问管理功能权限。
11.Moxa MXview V2.8存在私钥文件远程读取漏洞
12.Moxa MXview v2.8 web界面Dos拒绝服务漏洞
13.Moxa SoftCMS 1.5 AspWebServer拒绝服务漏洞
14.Omron plc信息泄漏漏洞，通过脚本攻击可以获取plc的内部详细信息
15.Phoenix Contact ILC 150 ETH PLC远程开启控制漏洞
16.Phoenix Contact ILC 150 ETH PLC远程关闭控制漏洞
17.Siemens SIMATIC S7-300 CPU中存在安全漏洞。
18.Siemens SIMATIC S7-300远程开启PLC CPU漏洞。
19.Siemens SIMATIC S7-300远程关闭PLC CPU漏洞。
20.Siemens SIMATIC S7-300远程开启CPU通信模块漏洞。
21.Siemens SIMATIC S7-300远程关闭CPU通信模块漏洞。

国内第一本
工控信息安全专著



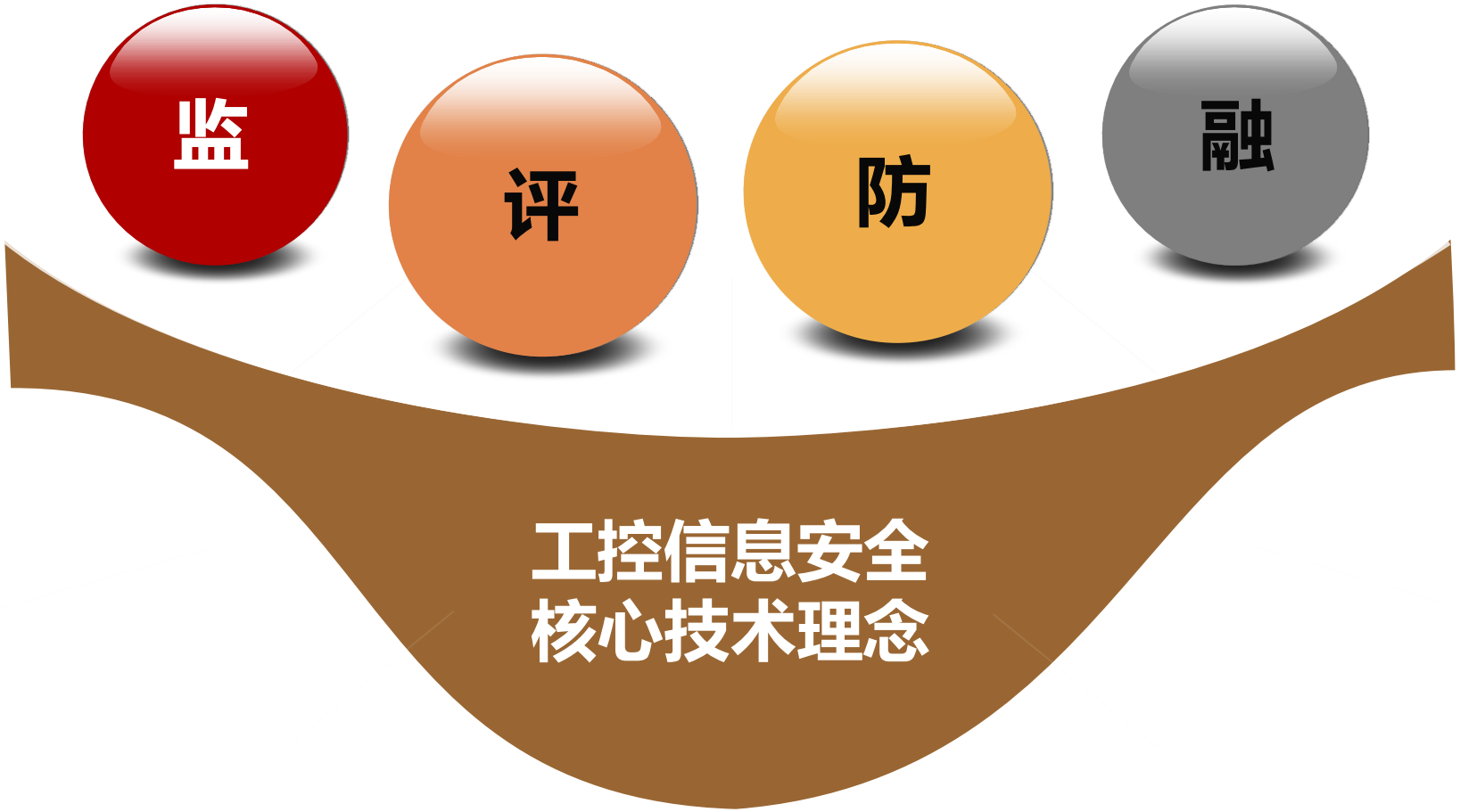
研究项目

财政部国有资本金、工信部、发改委工控信息安全专项、国家242信息安全计划、国防科工局、上海市科委、经信委信息安全专项近30项。

标准制定

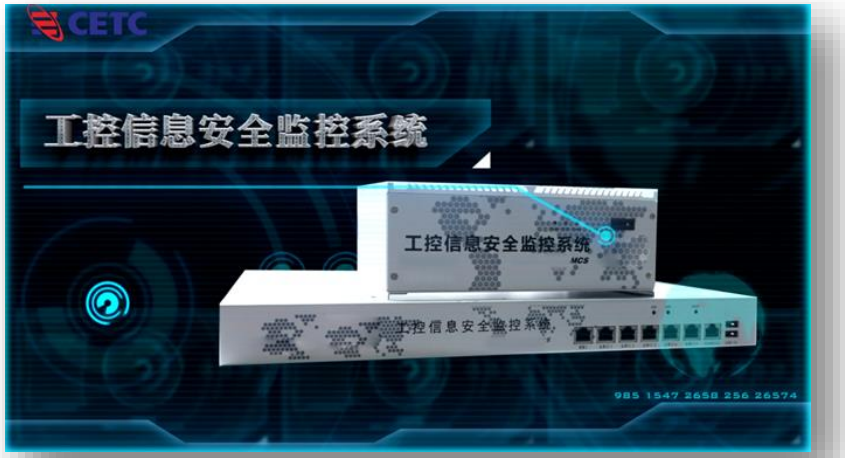
《集散控制系统（DCS）安全防护要求》
《集散控制系统（DCS）安全管理要求》
《集散控制系统（DCS）安全评估指南》
《集散控制系统（DCS）风险与脆弱性检测要求》
《可编程逻辑控制器（PLC）系统信息安全要求》
《工业控制系统信息安全分级规范》
《工业控制系统安全管理基本要求》
《工业控制系统网络审计产品安全技术要求》
《工业控制系统专用防火墙技术要求》（在研）
《工业控制系统安全管理平台技术要求》（在研）
《工业控制系统工业隔离网关技术要求》（在研）
《工业控制系统产品信息安全通用评估准则》（在研）
《工业控制系统安全防护技术要求和测试评价方法》（在研）
《xx行业网络安全等级保护基本要求》（在研）
《xx行业工业控制系统网络监测审计产品技术要求》（在研）
《xx行业工业控制系统网络边界防护产品技术要求》（在研）

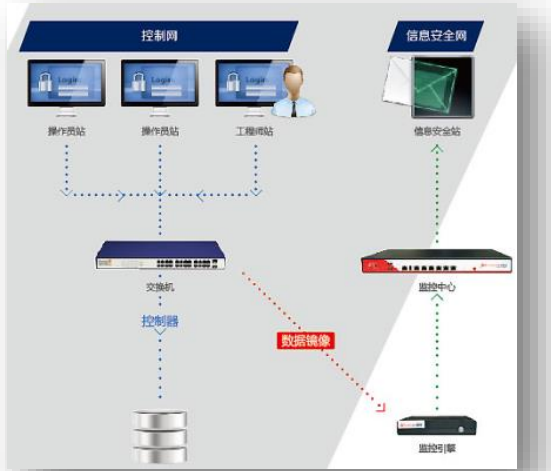
技术与产品



以“监评防融”为核心理念引领技术发展

技术与产品





旁路部署
单向获取数据，对控制系统“零”影响。

威胁精准定位
监测工业控制系统网内恶意软件，根据规划策略，及时定位报警。

实时监测异常
监控DCS工程师站组态变更、DCS操作站数据与操作指令变更，负载变更、通信行为、异常流量等，具备过程状态参数、控制信号的阀值检查与报警功能。

工控信息安全监控系统旁路部署在工业控制网中，连续不间断的监控工业以太网中传输的所有网络通讯信息，实现网络结构风险和活动的即时可见；并基于对工业控制协议（如Modbus/TCP、OPC、S7、IEC104等）的深度解析，根据用户指定的保护目标及检测策略对网络中的可疑行为或攻击行为产生报警，通知用户进行人为干预；同时，对网络通讯行为进行详实的审计记录，定期生成统计报表，全面掌控工业控制网的“过去、现在和未来”。

技术与产品

多媒体采集
能帮助用户现场评估人员真实采集评估现场的信息安全现状。

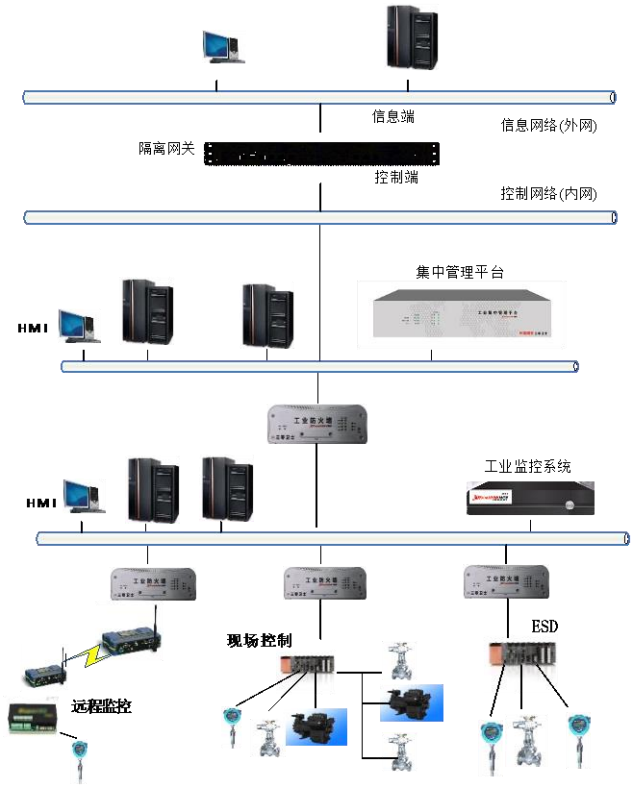
评估标准定制化
使用户可以完全按需进行安全评估工作。

统计分析功能
帮助用户多维度地了解现有系统信息安全现状，对未来的信息安全工作作出正确决策。

工控安全评估套件是国内首套主要用于工业控制系统的信息安全风险评估和现场工作管理的工具。该套件包含任务服务器，现场评估工作站及方便现场工作人员使用的现场评估PAD。通过使用该套件，能实现并规范工控信息安全风险评估和评估过程，将部分工作自动化，提高现场工作效率，降低人员工作量。

技术与产品

防



物理隔离

采用双独立主机系统，分别接入控制网和信息网，中间通过专用硬件装置隔离连接，采用私有协议数据摆渡。

支持工业数据交换

支持OPC、MODBUS等工业协议的数据交换控制，同时可扩展支持自定义应用通信。

支持数据库等数据同步

支持SQL Server、Mysql、Oracle等常用数据库的自动数据同步。还可支持其他类型的文件同步功能

工业隔离网关是专为用于解决工业控制网络如何安全接入信息网络的问题。通过内部的双独立主机系统，分别接入到控制网络和信息网络，双主机之间通过专用硬件装置连接，从物理层上断开了控制网络和信息网络的直接网络连接。同时工业隔离网关通过内嵌的高性能工业通信软件，支持各种主流工业通信标准，如：OPC、 Modbus等以及常用数据库间的数据同步功能。

技术与产品

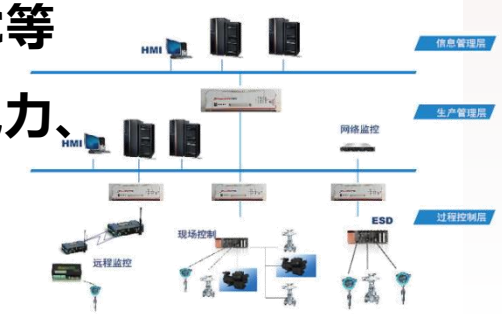
防

DIN导轨式

1U机架式

2U机架式

工业防火墙是一款专门为工业控制系统开发的全系列、立体防护式信息安全产品。适用于SCADA、DCS、PCS、PLC等工业控制系统，受益用户为核电、能源、钢铁、化工、电力、城市供水供气供热等行业用户。



防护病毒

深度解析控制多达10多种工控协议和数据，阻挡针对工业系统的病毒和恶意代码的传播和攻击（如“震网”病毒）

防护攻击

阻挡对于TCP、UDP、ICMP等协议对保护网络的攻击

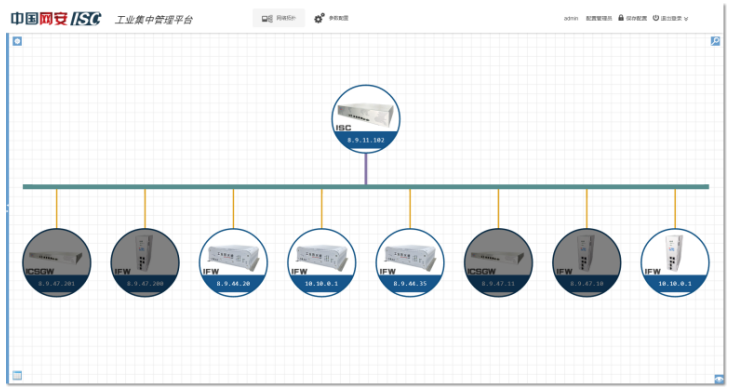
智能学习快速部署

针对工业环境提供**测试和学习模式**，能够在不影响工控网络的情况尽快部署白名单策略

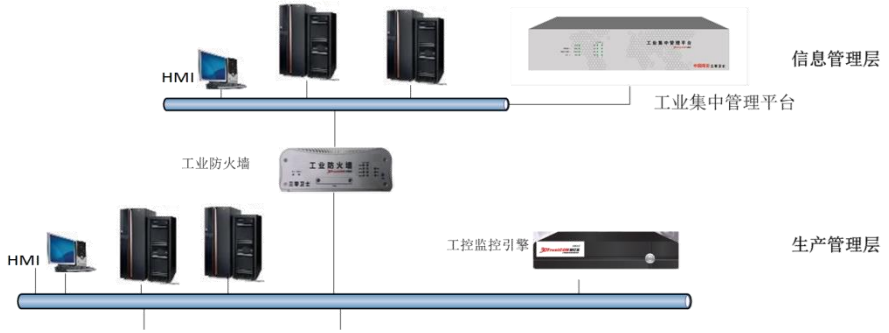
系统加固

禁止非法程序对防火墙进行配置或篡改，防止木马、口令嗅探和解密等攻击

技术与产品



工业集中管理平台是一种工控网络中的旁路设备，通过网络与工业防火墙、工控信息安全监控系统、工业交换机以及其他工控设备实现集中管理和监控。实现工控网络环境下的资产、通信和协议的可视化。



融

部署方便

无需IP地址配置即可通过私有安全协议自动发现工业防火墙和工业监控系统设备，建立安全的长连接，自动形成整个网络的拓扑结构，实时监控设备的工作状态

策略配置

通过拖拽式的组态配置方式快速配置工业防火墙和工业监控系统的策略配置，结合基本策略和安全策略的抽象实现批量下发和部署

报警和分析

海量日志的丰富的分析报告和统计报表展示，动态展现工控网络的事件状态和趋势；根据工控环境的用户需求指定的事件分析策略提供及时的报警和提醒功能

项目统计

- 成功实施了石化、核电、钢铁、烟草、水利以及轨道交通等行业企业（单位）的工业控制系统信息安全风险评估和安全加固等网络安全保障项目；
- 作为技术支持单位，配合北京网信办、江苏省经信委等政府有关部门开展所辖区域基层单位工业控制系统信息安全状况检查和评估工作；
- 截止2018年底，累计承担项目80余项，合同额5000余万元。

Thanks

工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance