

智能制造新形势下的工控安全 信息安全纵深防御解决方案

浙江中控技术股份有限公司
常务副总工程师 谭彰

居高思远，
域无限



CPS信息物理系统

移动互联网

虚拟现实VR/增强现实AR

增材制造

IIoT工业物联网

大数据

工业 4.0

工业互联网

无人机

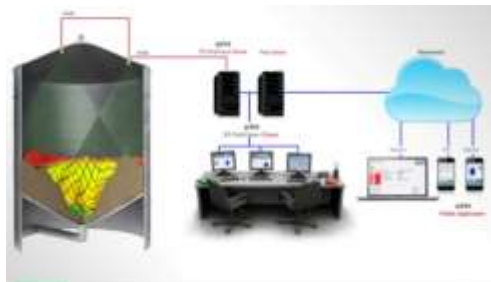
智能工厂

工业云计算

人工智能

中国制造2025

感知化



一体化



智能化



1

2

3

4

5

6

电气/机械化



自动化



数字化



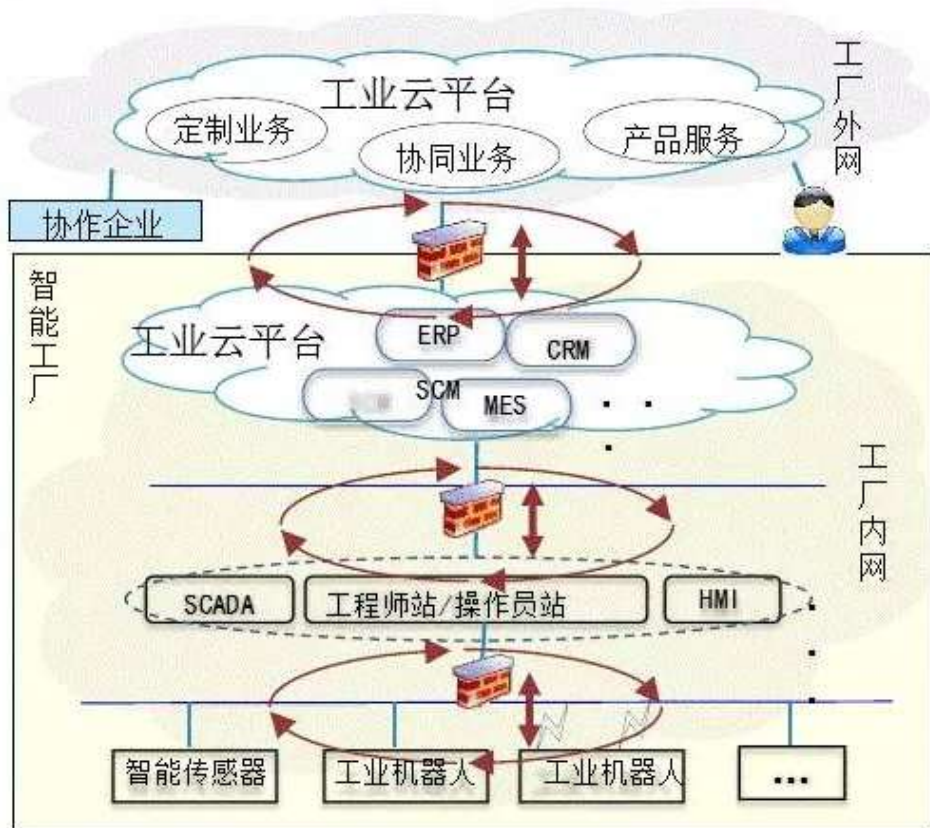
设备安全、网络安全、控制安全和数据安全组成新的安全体系

控制环境开放化使外部互联网威胁渗透到工厂控制环境

1 控制安全

网络IP化、无线化以及组网灵活化给工厂网络带来更大安全风险

3 网络安全



数据的开放、流动和共享使数据和隐私保护面临前所未有的挑战

2 网络安全

设备智能化使生产装备和产品直接暴露在网络攻击之下

4 设备安全

工信部信息化和软件服务业司副司长安筱鹏解读制造业与互联网融合国家政策：
工业信息安全形势日趋严峻

工厂物联网

产线设备更加智能化；封闭系统演变为开放式系统；各种原先孤立的智能系统相互连接起来，整个工厂构成了一个大网络，任何一个接入点可以连接到全厂任何设备和子系统；网络设备或节点故障引发全网瘫痪

管控一体化

信息化与工业化深度融合，更多的纵向集成，控制层与管理层交互更加频繁和双向，视频/生产控制联动、VR虚拟现实与实时生产互动

工业云和大数据应用

互联网+个性化定制生产（根据原材料和消费市场变化、用户需求变化进行柔性生产制造）；企业上云，企业电商、协同生产、云制造，基于工业云平台的产业链生态；政府云端监管（安全、环保、能源三位一体）、工业园区聚集区（物流一体化、循环经济化）

移动互联网的普及

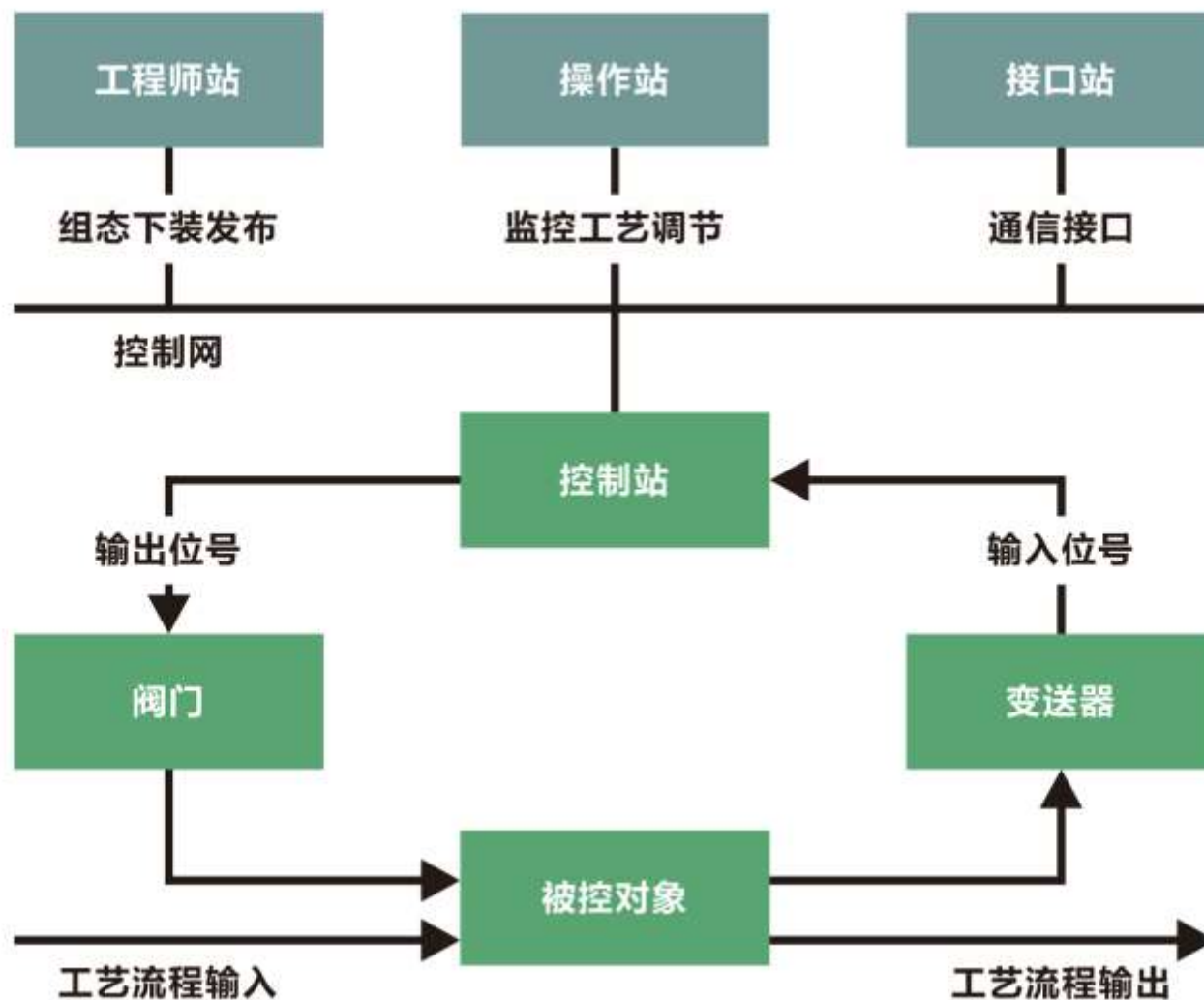
手机、Pad、便携式电脑等移动终端联网，WIFI无线接入，手持式智能巡检操作设备、智能手机充电、USB移动存储介质、云盘存储

服务外包、设备远程运维

设备和工控系统的远程维护、远程监控、应用软件升级，远程入侵途径

工控安全大环境严峻

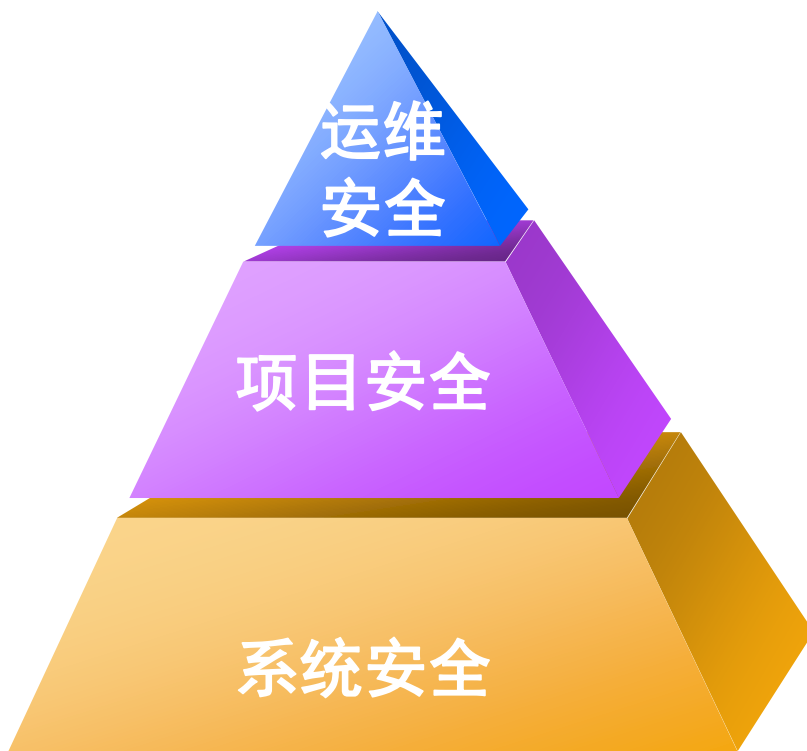
杀不完的病毒和木马，工控系统专向攻击（震网病毒等）、第三方研究机构针对工控系统进行攻击研究/公开漏洞库





植根内建安全，构筑集成综合防御

自下而上
自内而外



全生命周期
工控安全服务

纵深防御

内建安全

➤ 遵循国际标准IEC62443-3-3

通信健壮性

- 1.通过通讯健壮性认证，Codenomicon或Achilles Level 2认证

信息安全技术措施

- 1.访问控制
- 2.使用控制
- 3.数据完整性
- 4.数据保密
- 5.限制数据流
- 6.及时响应事件
- 7.网络资源可用性

嵌入式软件研发流程

- 1.安全管理流程 (SMP)
- 2.安全需求规格 (SRS)
- 3.软件架构设计 (SAD)
- 4.安全风险评估和威胁建模 (SRA)
- 5.软件详设 (DSD)
- 6.信息安全指导文档 (DSG)
- 7.模块实现和验证 (MIV)
- 8.信息安全完整性测试 (SIT)
- 9.信息安全流程检查 (SPV)
- 10.安全响应计划 (SPR)
- 11.安全验证测试 (SVT)
- 12.信息安全响应执行 (SRE)

- 控制与通信安全隔离技术
- 内核自主可控技术
- 数据安全技术
- 通信安全技术
- 多维度权限综合技术
- 全冗余与备份技术
- 全面报警与审计技术
- 安全V&V验证技术



⚠️ 全系统冗余和关键数据备份设计，保证控制系统实时诊断与恢复

● 全系统冗余设计

工程师站、服务器、控制网、控制器、IO总线、IO模块

单一故障不影响工业控制系统正常运行

实时对比诊断，可快速检测并定位安全问题

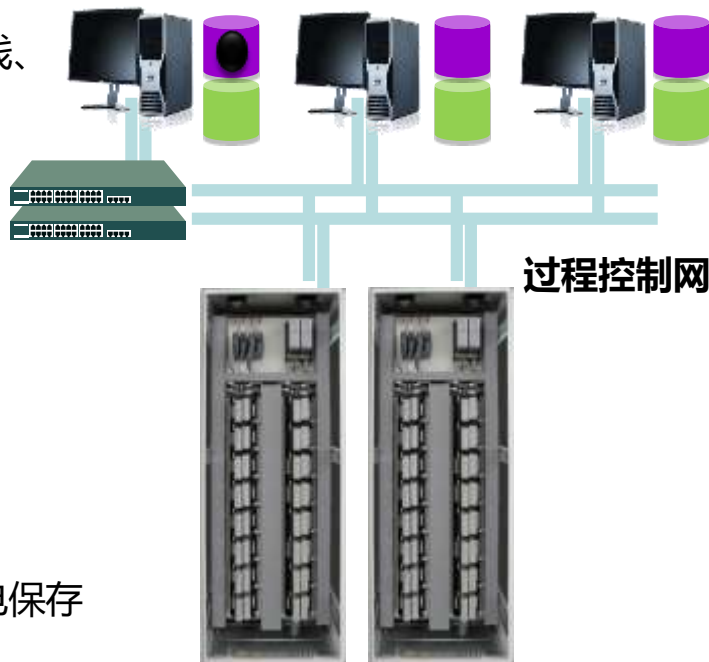
● 关键数据备份设计


工程师站/操作站：组态文件、历史数据

控制站：硬件组态、位号组态、控制算法

控制站组态数据、功能块参数、事件记录掉电保存

实时对比诊断，可快速检测并定位安全问题



 通过多层次数据加密和防护技术，保证数据的完整性和机密性

• 操作层

- 用户组态加密与防篡改技术
- 历史/实时数据库加密与防篡改技术
- 组态软件/监控软件关键EXE、DLL防篡改技术

• 网络层

- 实时通信数据加密与签名技术

• 控制层

- 控制站组态数据实时校验技术
- 用户程序实时检测技术
- 支持硬件清除组态设计

• 现场总线/无线层

- 通信加密与数据隔离转换技术

SCnet

控制网络

DO=1

&@*%^&*( &@*%^&*(

非明码传输，防止窃听和篡改

通讯错误	安全措施			
	报文序列号	时间监视器 (带应答机制)	身份认证	一致性校验
数据损坏				✓
报文损坏	✓			
报文重放	✓			
报文乱序	✓			
报文丢失		✓		
报文超时		✓		
报文插入		✓	✓	
报文伪造		✓	✓	✓
错误选址			✓	
交换机FIFO错误	✓			

 全面的权限管理，**让合适的人看到合适的内容**



用户权限+软件狗授权



控制器访问密钥+工作模式



最小授权原则




控制节点ID+应用程序ID

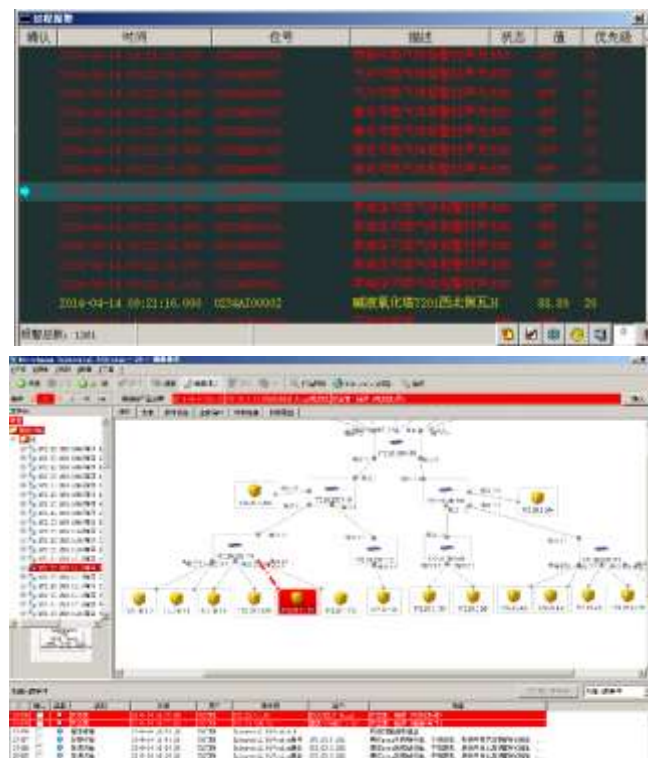


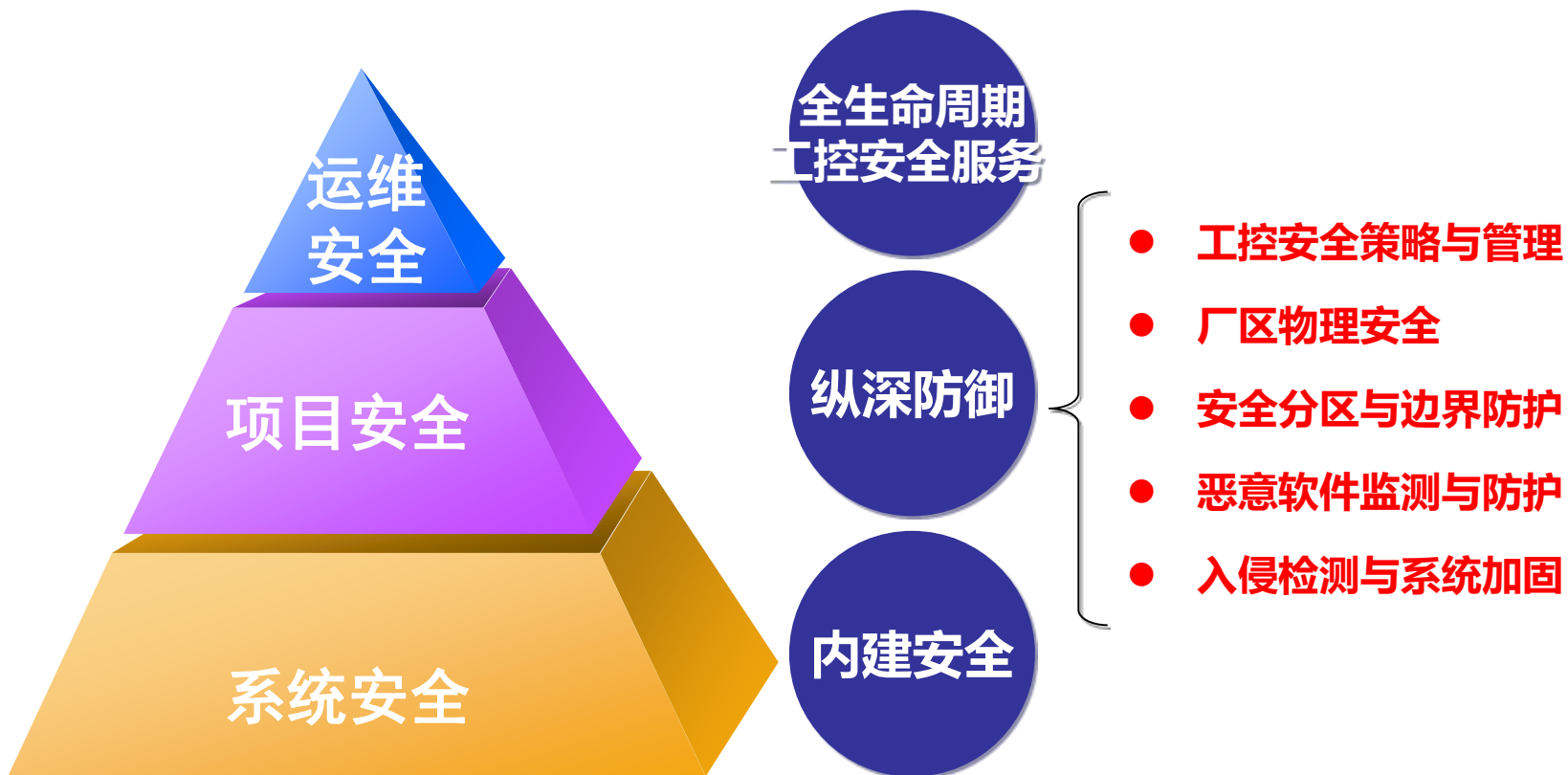
用户功能块查看、导出权限



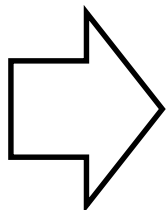
 完善的报警功能和审计功能，**让行为不可抵赖，故障不被隐藏**

- 过程报警（工艺报警）
- 系统报警
- 详细诊断
- 全网诊断
- 设备管理与智能诊断
- 操作记录与安全事件记录
- 工艺建模/行为建模/预测管理



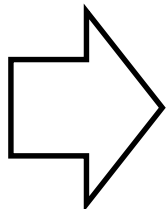


工控安全策略和管理



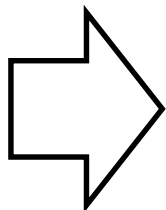
帮忙用户建立正确的安全政策和管理措施，
防止管理漏洞导致纵深防御形同虚设

安全分区与边界防护



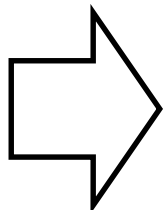
阻止外部攻击，防止黑客或病毒长驱直入

恶意软件监测与防护



让病毒无处遁形，无用武之地

入侵检测与系统加固



阻止病毒利用操作系统漏洞、TCP/IP漏洞、
协议漏洞，链路连接漏洞等攻击计算机

- 最常见安全手段
- 安装灵活易于操作
- 对操作系统依赖强
- 病毒库不更新不能很好达到防护的目的
- 每次病毒库或软件更新均需兼容性验证
- 操作系统补丁不及时升级也影响防护效果

黑名单技术

- 占用资源极少
- 无需更新病毒库
- 可动态更新白名单
- 保证软件运行的绝对安全
- 对操作系统无依赖，无需操作系统升级
- 无杀毒功能，病毒可通过其他途径传播

白名单技术

- 工作站优化大师
- 可信工作站卫士
 - 系统加固：操作系统、驱动、协议栈
 - 白名单控制：端口、服务、协议
 - 管控进程，杜绝未知恶意程序启动
 - 对可疑进程生成报警信息



纵深防御：入侵检测与审计

The screenshot displays a network management application. The main window shows a network topology diagram with various nodes and connections. A red box highlights a specific node in the diagram. Below the diagram, there is a table of events. The table has columns for ID, Confirmation, Type, Category, Time, User, Event Name, Description, and Message. The first two rows are highlighted in red, indicating critical events.

ID	确认	类型	类别	时间	用户	事件名	描述	消息
27420	<input checked="" type="checkbox"/>	报警	状态差	12-8-14 16:25:09	SYSTEM	172.20.1.131	向公网请求 RARP...	状态差: 错误 (可发现=否)
27425	<input checked="" type="checkbox"/>	报警	状态差	12-8-14 16:25:09	SYSTEM	172.20.100.111	要求 2/端口 3/37	状态差: 错误 (连接=否下)
27428	<input type="checkbox"/>	提示	设备异常	12-8-14 16:54:30	SYSTEM	Industrial HiView 服务	网络扫描请求地址	
27427	<input type="checkbox"/>	提示	发现设备	12-8-14 16:54:25	SYSTEM	Industrial HiView 服务	172.20.0.201	发现 ping 发现新设备, 不能添加, 系统中已有发现的 MAC 地址 ...
27426	<input type="checkbox"/>	提示	发现设备	12-8-14 16:54:23	SYSTEM	Industrial HiView 服务	172.20.0.201	通过 ping 发现新设备, 不能添加, 系统中已有发现的 MAC 地址 ...
27425	<input type="checkbox"/>	提示	发现设备	12-8-14 16:54:25	SYSTEM	Industrial HiView 服务	172.20.0.201	通过 ping 发现新设备, 不能添加, 系统中已有发现的 MAC 地址 ...

设备扫描 拓扑选择 拓扑生成 节点报警

确定 取消 帮助

全网诊断、网络监控

访问控制、实时监测、安全审计

控制网立体防护，保证通信的实时性和确定性

- **接入设备认证**

 - 兼容性、安全特征

 - 交换机、防火墙、GPS服务器等

- **安全交换机**

 - 协议检测，只允许工控协议通信

 - 一体化诊断

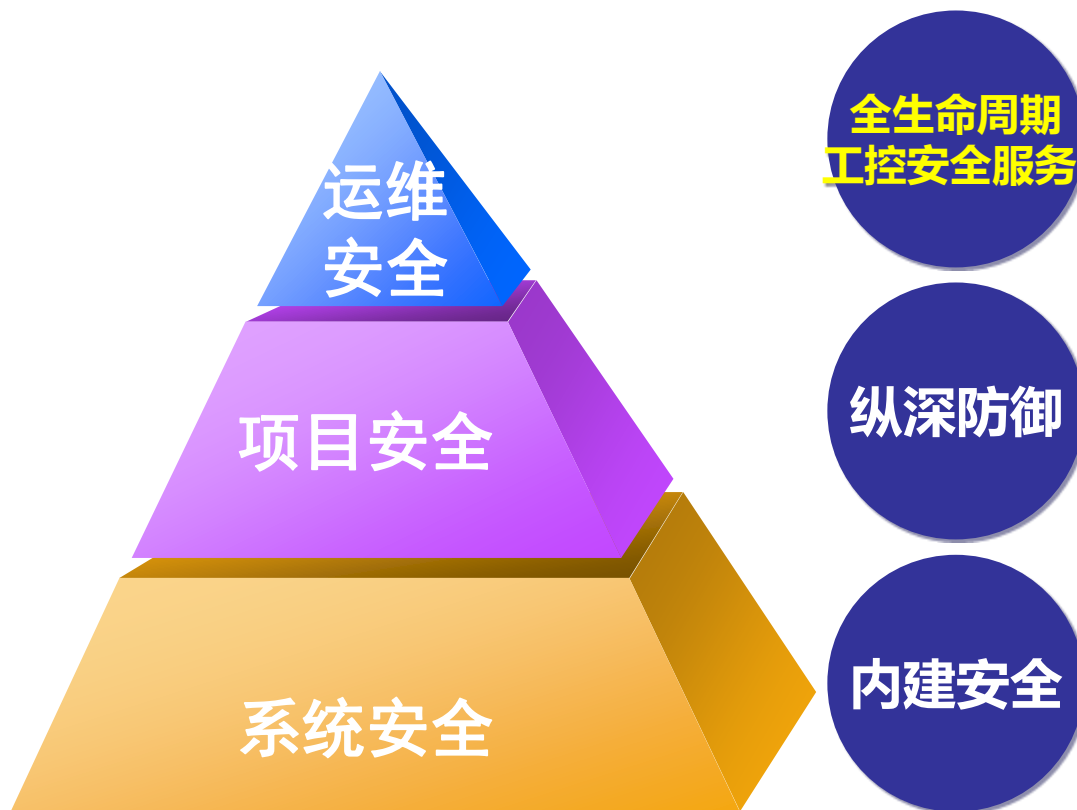
- **工业协议安全网关**

 - 隔离标准工业协议（Modbus等）

 - 深度检测，防止错误指令、数据空间越界、未授权操作



逐步提升服务器、路由器、交换机等核心硬件设备国产品牌覆盖率



评估内容

● 网络运行状况评估

- 网络拓扑结构统计
- 主机设备分布和基本配置
- 网络负荷分析
- 节点响应时间统计
- 网络通信状况分析
- 网络设备配置分析

● 网络架构评估

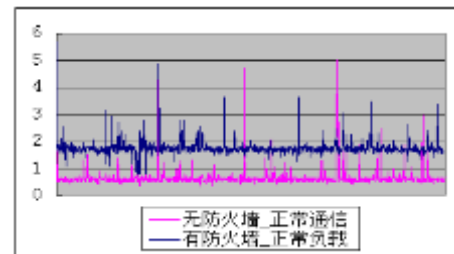
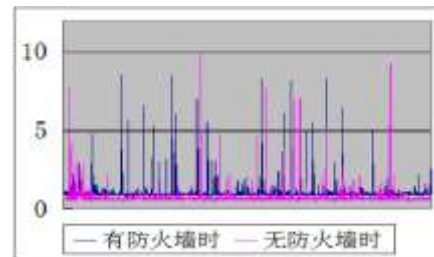
- 网络区域划分评估
- 边界防火墙评估
- 网络接口漏洞评估

● 控制系统主站安全漏洞评估

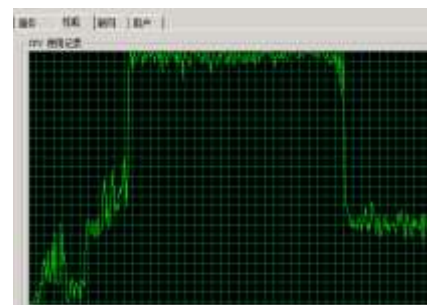
- 网络服务开放端口扫描
- 网络、操作系统漏洞扫描

● 已知工控系统产品漏洞防护审计

- 统计现有相关安全策略
- 审计已部署的安全控制措施（产品）



工控网络通讯性能测试



主机负荷测试

改造内容

● 安全策略与流程

- 风险评估
- 安全规划
- 安全操作指南
- 安全运维
- 安全监控

● 网络分区与边界防护

- 过程网和信息网的隔离解决方案
- 信息网和企业网的隔离解决方案
- 过程网VLAN分区隔离解决方案

● 系统加固

- 漏洞扫描系统
- 工作站优化

● 恶意软件检测与防护

- 网络审计与诊断
- 管理层黑名单防病毒解决方案
- 过程信息网白名单防病毒解决方案

● 访问控制与账号管理

- 加强对操作站及工控应用帐号的管理
- 采用最小权限的原则
- 为不同（权限）的操作员分配不同的帐号/口令，并进行备份
- 定期检查、更新帐号、口令
- 为关键控制程序的读写提供基本的访问控制功能
- 严格控制手提、移动设备的使用等

● 日志与审计

- 操作日志（登录成功、失败）日志
- 病毒查杀日志
- 白名单异常日志
- 其他安全事件等

- 参与工控安全国标制订
- 国内首家通过Achilles Level2工控信息安全认证
- 获得信息安全服务资质（安全工程类一级）
- 工业控制系统信息安全产业联盟成员
- 建立纵深防御技术体系，并在大型项目中应用
- 建立工控安全实验室
- 承担科技部“网络空间安全专项”、工信部智能制造专项-工控安全标准化项目



风险分析->安全需求-> 安全设计-> 安全实施-> 安全验收

类型	产品	型号
工控安全 防护产品	工业防火墙	GW731
	电力装置单向网闸	GW732
	工业协议安全网关	GW713
	工业互联网安全网关	GW715
	安全交换机	SUP3000
	可信工作站卫士	VxDefender
	操作站优化大师	OSGenius
	网络在线监测平台	VxNetSight
	防病毒软件（黑名单）	Kaspersky
	系统备份与灾难恢复工具	VxRecover
检查工具	工业漏洞扫描工具	-
	基线扫描工具	-
	合规性检查工具	-

安全方案设计

中控·SUPCON

咨询和服务

中石化川维30万吨醋酸乙烯项目
网络安全

中石化北海炼油异地改造1000万吨炼油项目
网络、防病毒安全解决方案

舟山国家储备油基地大型SCADA
安保和系统安全方案

中石化安庆项目
防病毒和信息安全方案

中天合创大型煤化工项目
信息网安全方案

中石化海南大炼油FOXBORO MESH网络频繁故障
导致全厂网络瘫痪重大网络事件网络安全分析

中石化青岛石化西门子系统
数据服务瘫痪事件安全分析

冀东水泥44分厂
网络安全改造

浙江龙盛集团鸿盛公司
信息安全改造

智能工厂，安全为先

工控信息安全不是常规意义的信息安全，可用性远重于完整性和机密性，不仅应加强外部防护，更应关注内建安全、本体防御

从内建安全，到纵深防御，再到运维安全，打造综合安全防护体系

TECHONLOGY WINS DREAMS

TECHONLOGY WINS DREAMS

感谢支持!



TECHONLOGY WINS DREAMS

TECHONLOGY WINS DREAMS

中控 · SUPCON