海天煒業

MOSES

—— 服务提升价值

全生命周期工业控制系统
信息安全解决方案

李　涛

2014.5

目录

1.工业信息安全现状及用户需求分析

2.全生命周期工业控制系统信息安全解决方案

3. 案例分享

工业信息安全现状分析

2003年，美国俄亥俄州Davis-Besse的核电厂控制网络内的一台计算机被微软的SQL Server蠕虫所感染，导致其安全监控系统停机将近5小时

2008年，黑客劫持了南美洲某国的电网控制系统，敲诈该政府，在遭到拒绝后，攻击并导致电力中断几分钟

2007年，攻击者侵入加拿大的一个水利SCADA控制系统，通过安装恶意软件破坏了用于控制从Sacrmento河调水的控制计算机

2008年，波兰Lodz的城铁系统遭到攻击，轨道扳道器被改变，导致4节车厢出轨

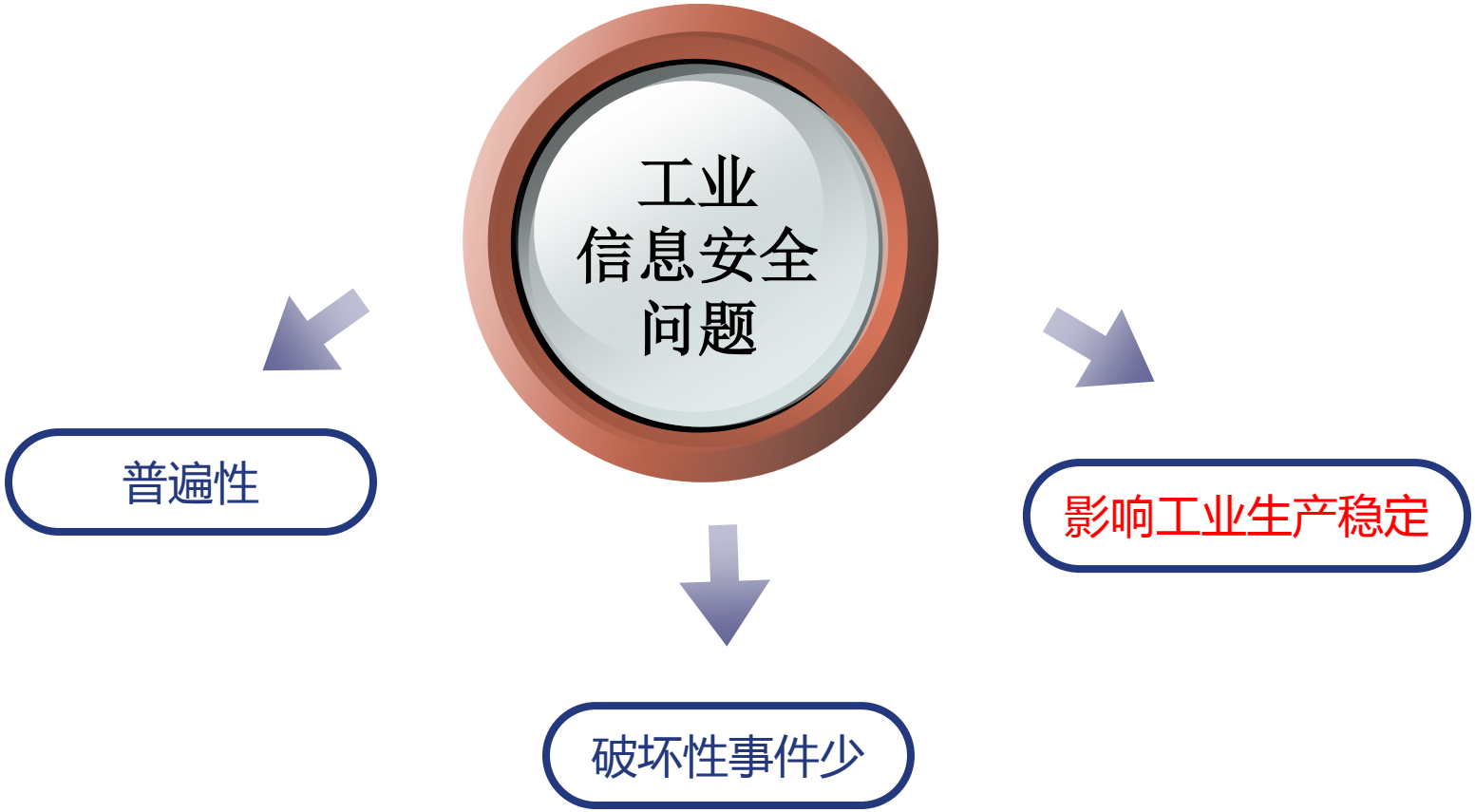
2010年10月，Stuxnet震网病毒事件

2011年9月，Duqu病毒事件

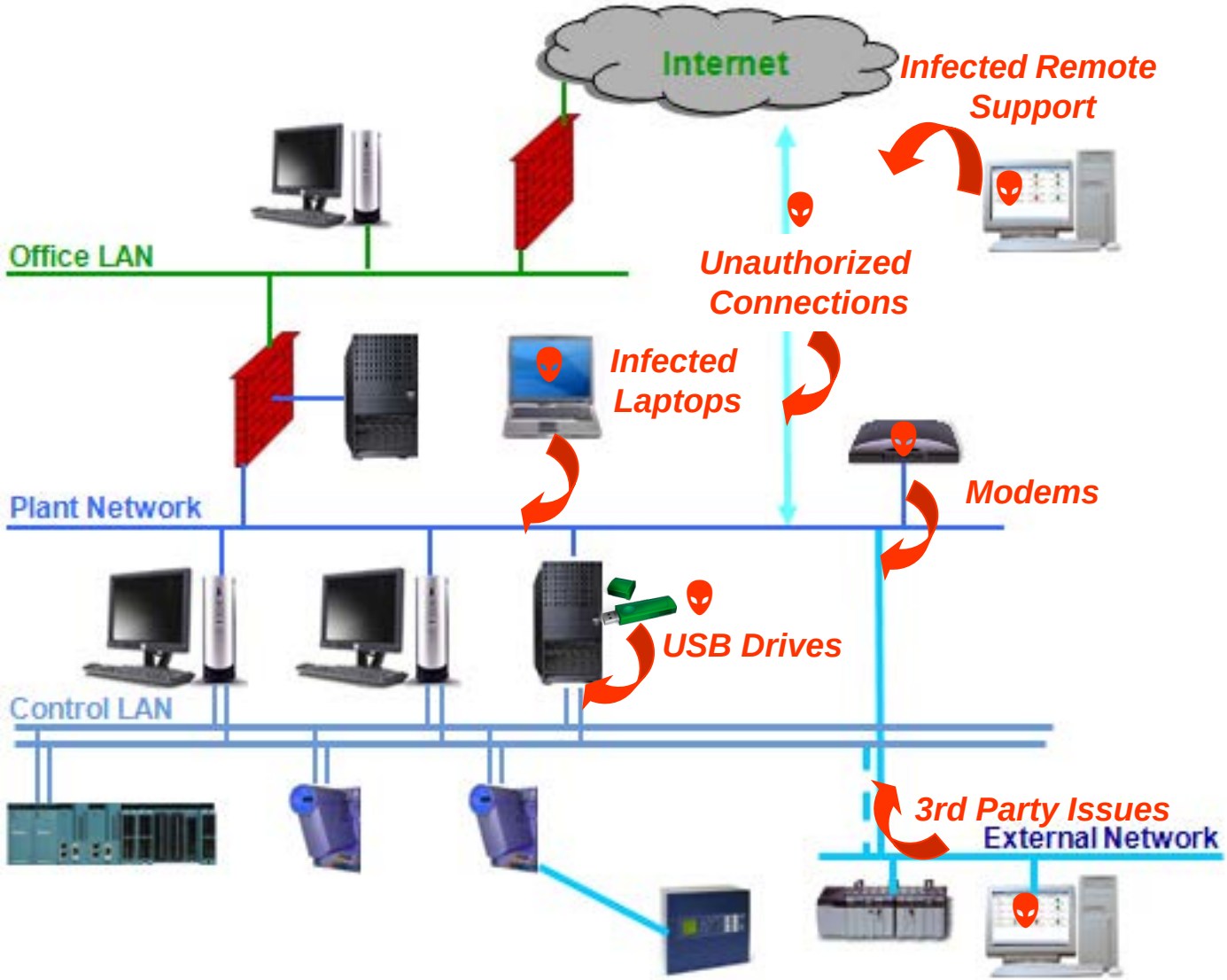
2012年5月，Flame病毒事件

……

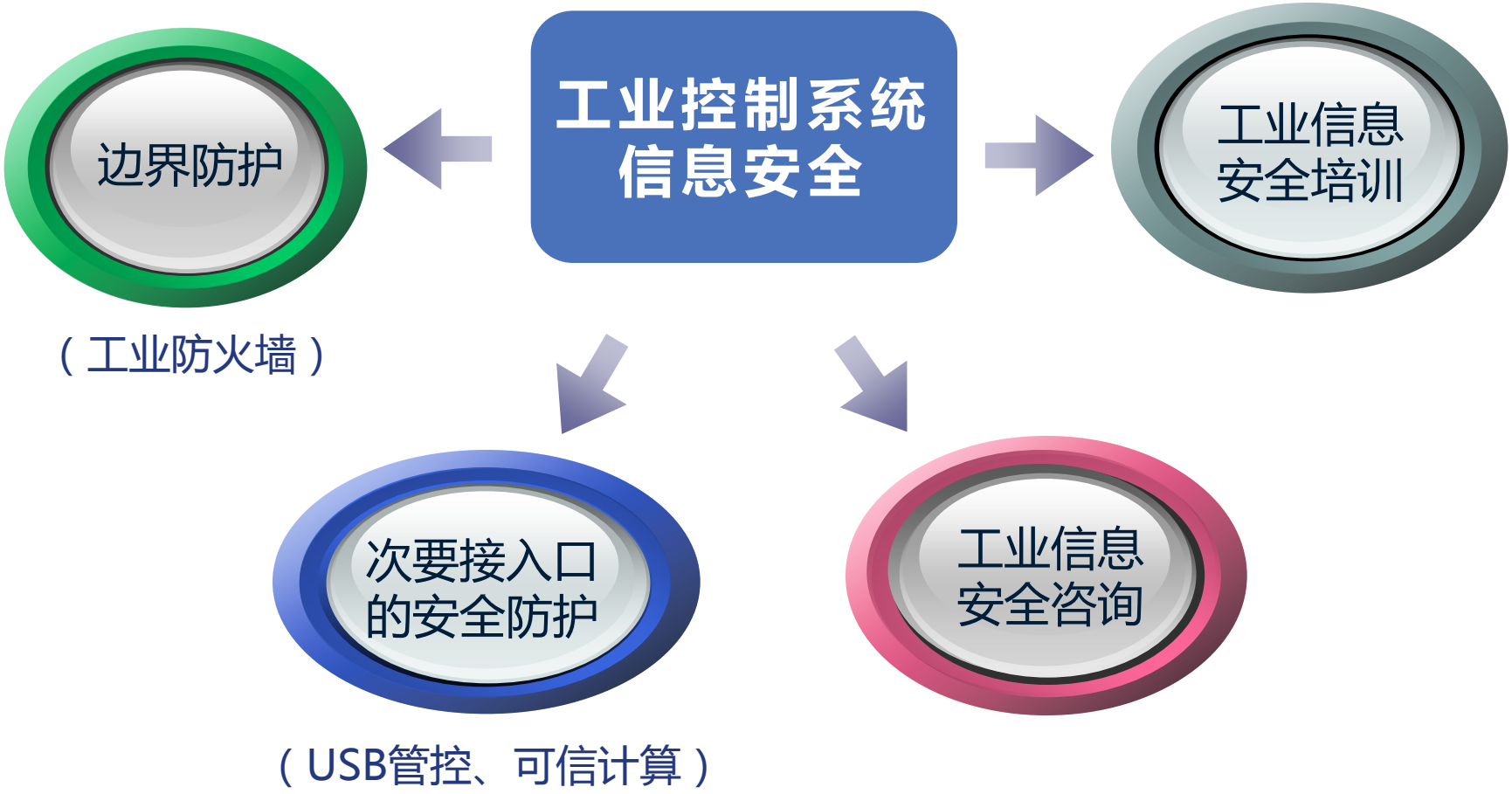
工业信息安全现状分析



病毒/黑客渗透到工业控制系统的方式



用户需求分析


工业控制系统
信息安全
边界防护
（工业防火墙）
工业信息
安全培训
次要接入口
的安全防护
（USB管控、可信计算）
工业信息
安全咨询

目录

1.工业信息安全现状及用户需求分析

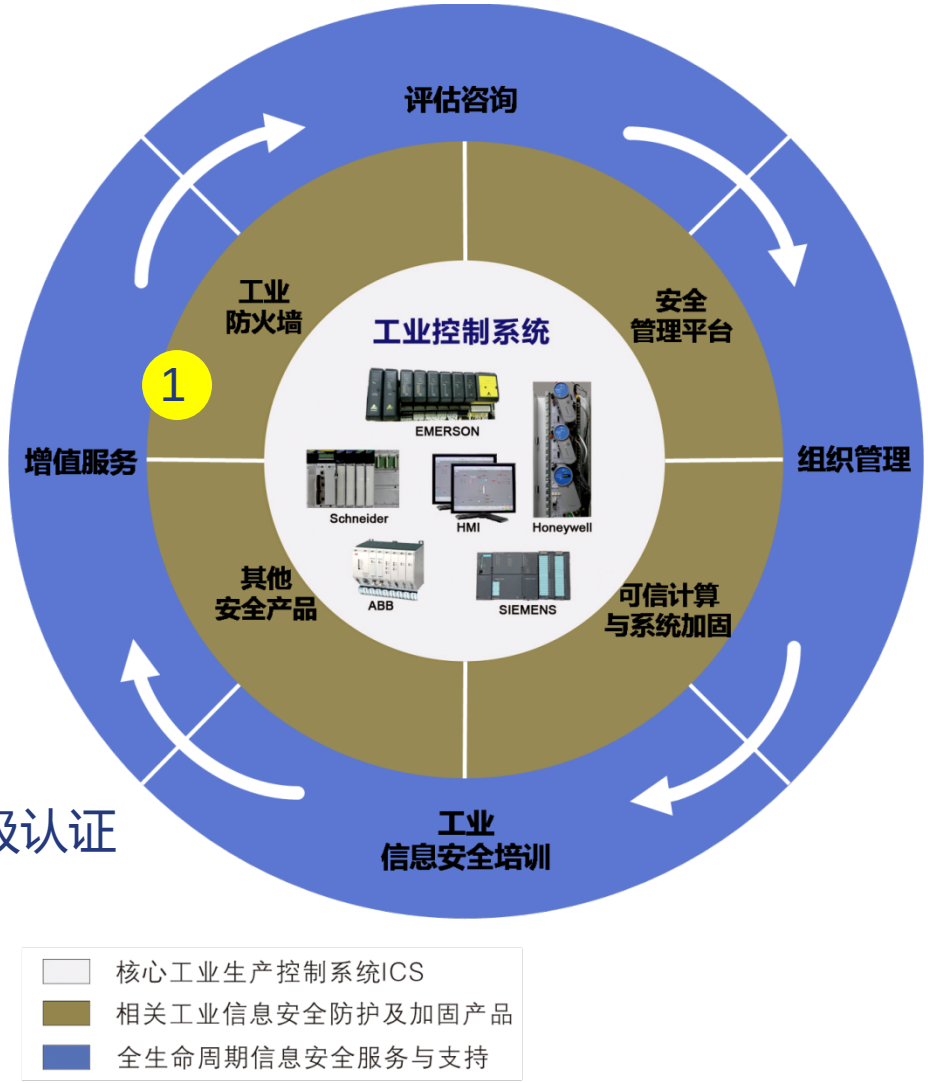
2.全生命周期工业控制系统信息安全解决方案

3. 案例分享

全生命周期工业控制系统信息安全解决方案

Guard工业防火墙

- 内置50多种工业通讯协议
- 对OPC、Modbus等进行深层防护
- 二层协议防护
- 工业型设计，可在线安装调试
- 无IP设计，CMP统一配置管理
- 自身强大的安全性，通过了EAL3等级认证
- 友好的界面，拖放式配置



全生命周期工业控制系统信息安全解决方案

Guard工业防火墙

- 海天炜业联合中科院软件研究所共同研发、推出
- 国家发改委首批重点资金支持的工业信息安全专项产品
- 通过公安部独立性产品测试
- 取得EAL3证书、ISCCC安全认证和工控防火墙销售许可证

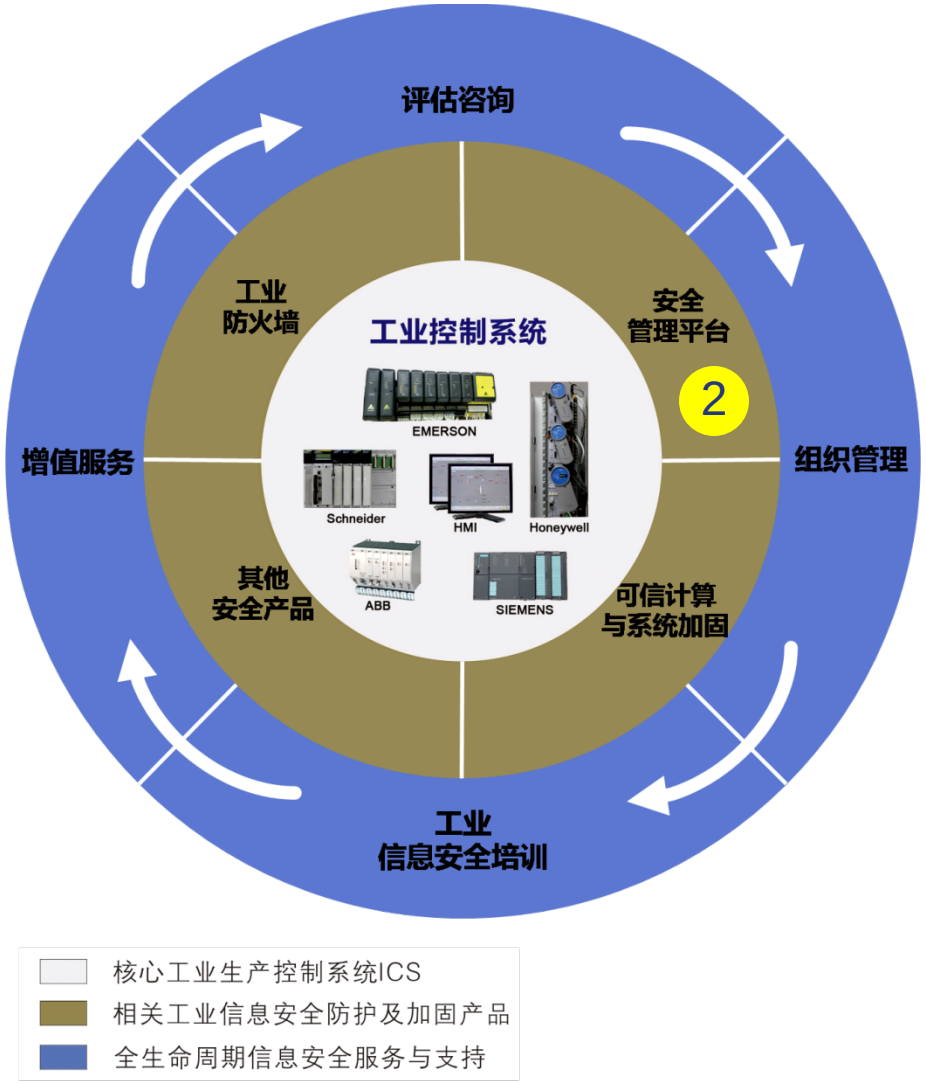
Tofino工业防火墙

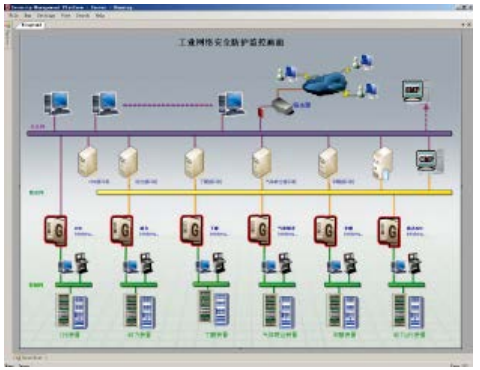
- 知名DCS/PLC厂商推荐
- 市场占有率领先

全生命周期工业控制系统信息安全解决方案

Guard工业防火墙荣誉资质

全生命周期工业控制系统信息安全解决方案

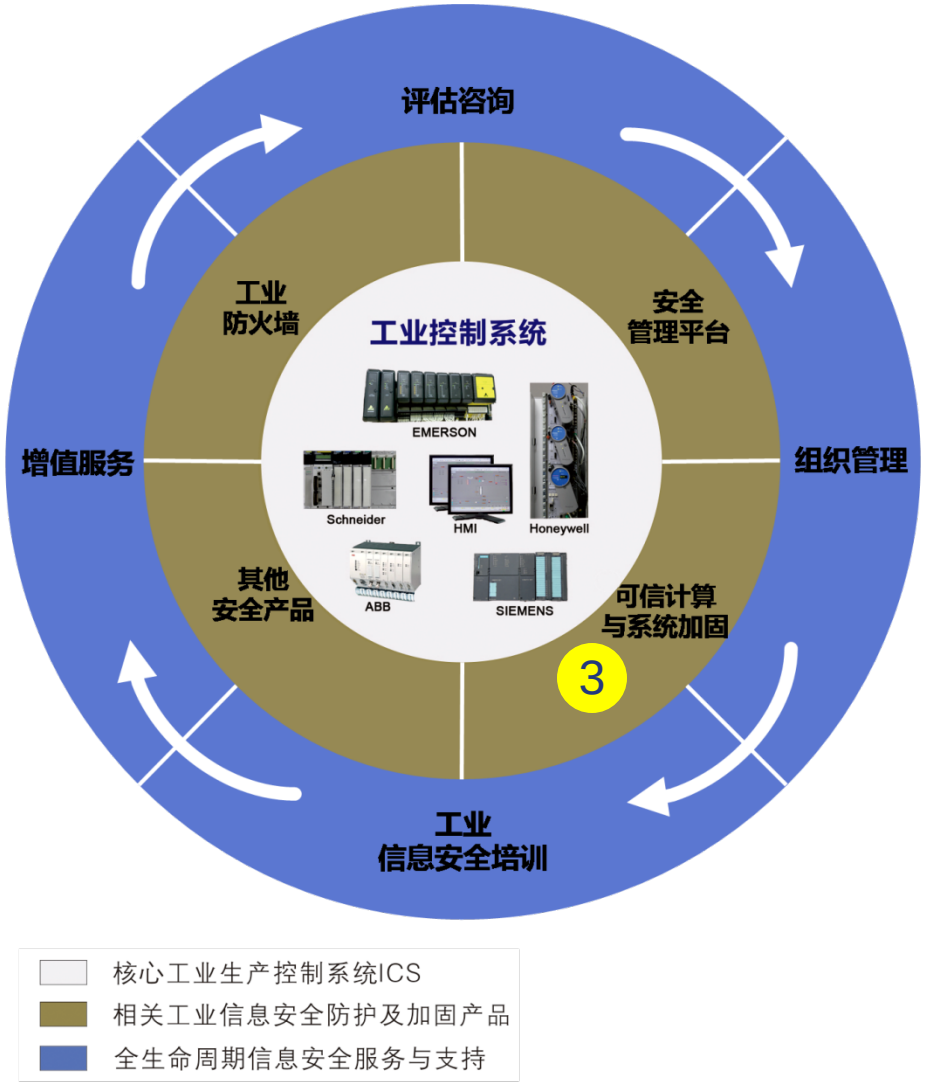


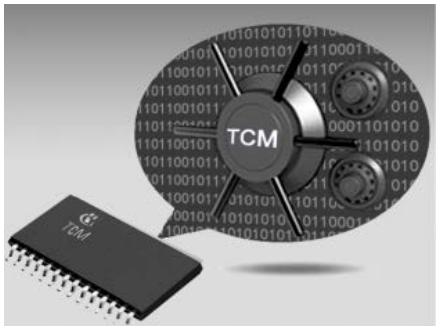


安全管理平台

网络状态实时监控、智能分析，以总揽大局的方式为工厂网络故障的及时排查、分析提供可靠依据

全生命周期工业控制系统信息安全解决方案





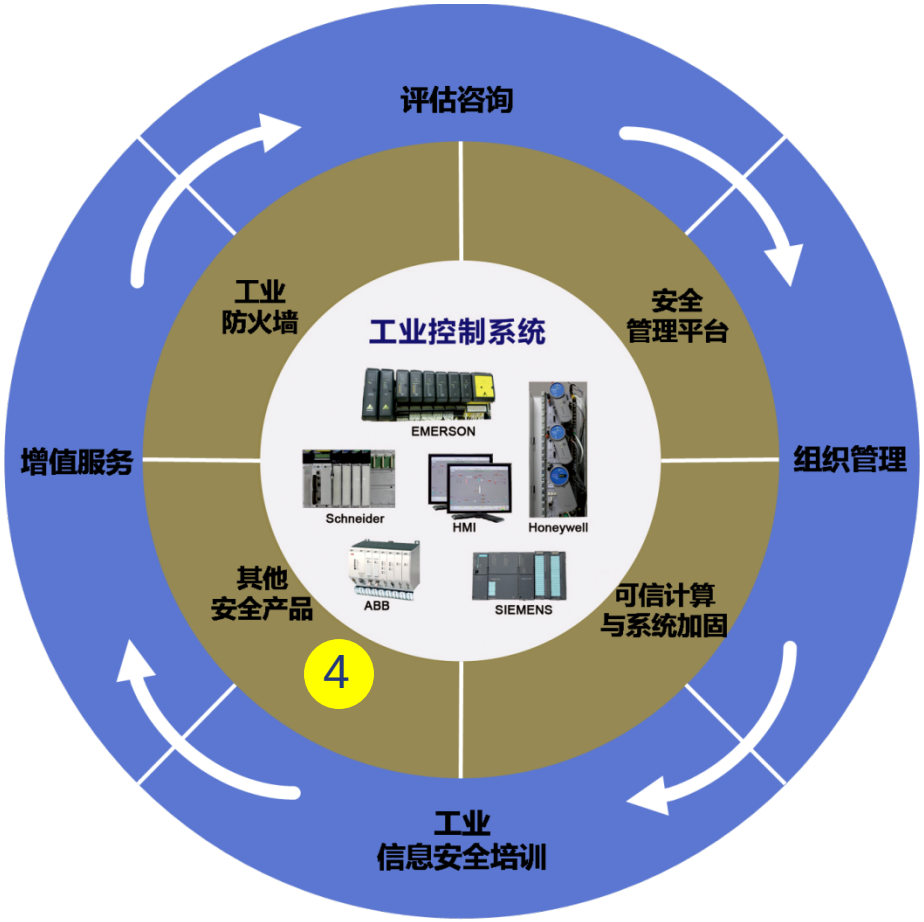
可信计算与系统加固

- 可信计算技术在工控安全领域的创新应用
- 中国自主的可信计算模块及加密算法
- 智能的可信度量与管控白名单，提高系统免疫力
- 阻止一切非可信进程运行，抗病毒，抗恶意攻击

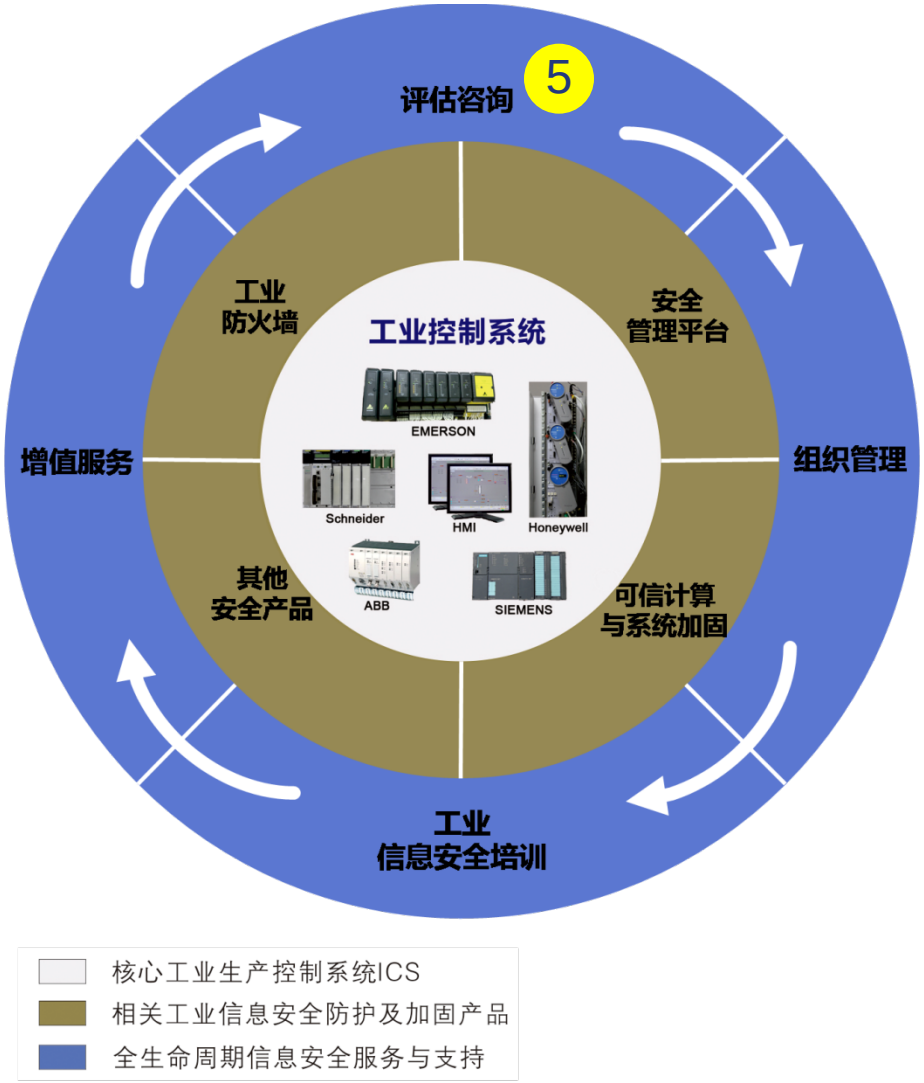
全生命周期工业控制系统信息安全解决方案

其他安全产品

以适用于工业环境为核心，拓展杀毒软件、IDS、IPS等产品在工控信息安全领域的应用，创建“纵深防御”的工业信息安全架构



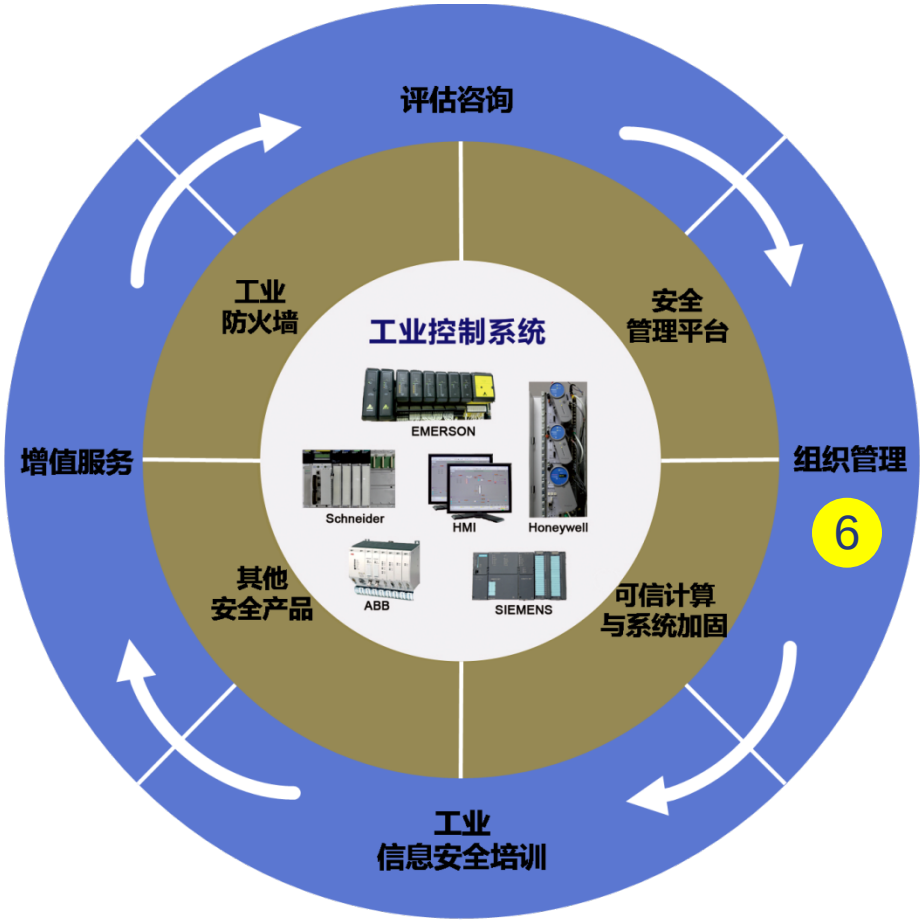
全生命周期工业控制系统信息安全解决方案

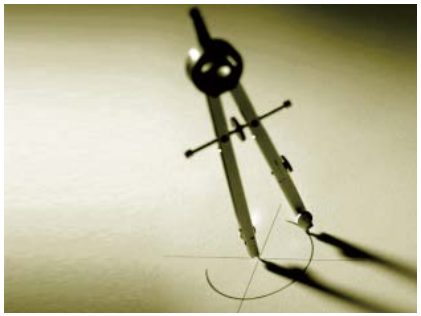


评估咨询

- 组织机构管理
- 工控系统架构
- 风险与脆弱性

全生命周期工业控制系统信息安全解决方案





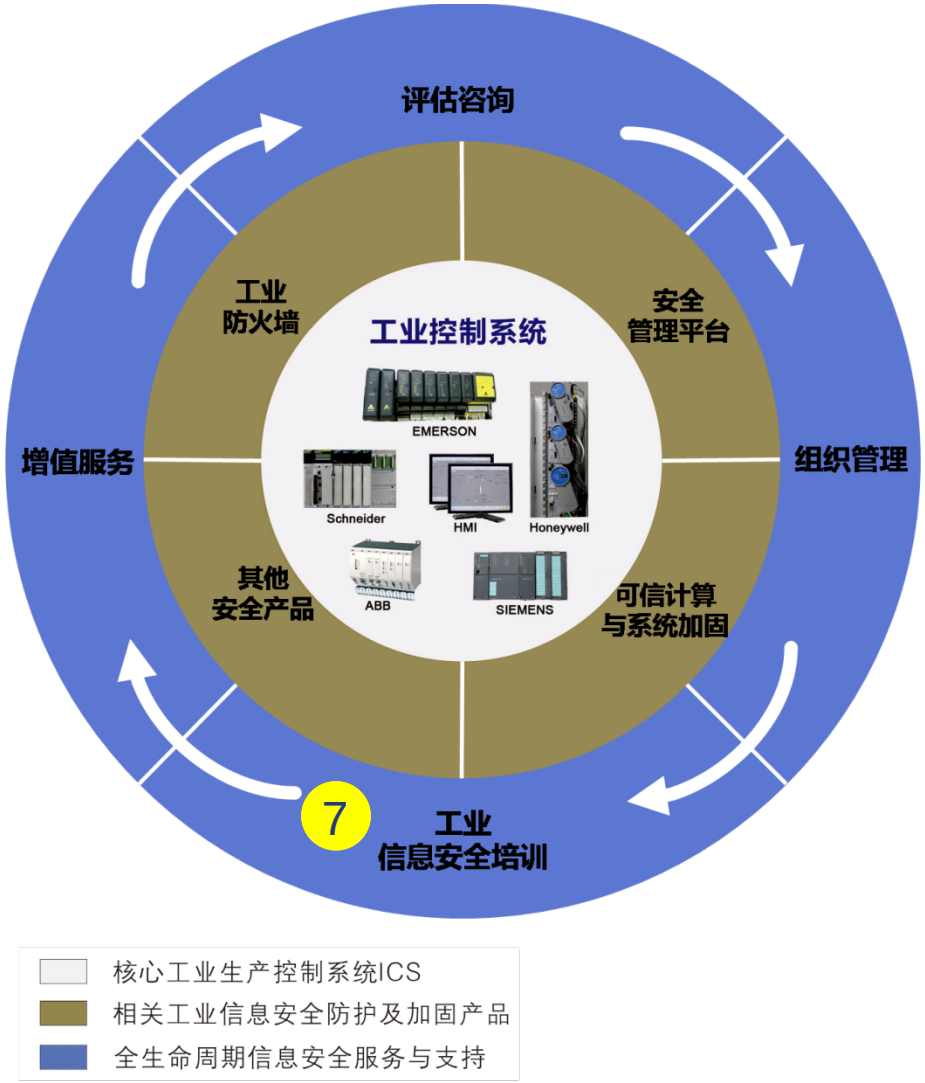
组织管理

- 安全策略及程序文件
- 工业信息安全培训
- 变更、备份与恢复管理
- 安全事件应急响应与审计

全生命周期工业控制系统信息安全解决方案

工业信息安全培训

- 工厂网络结构
- 工业网络设备及应用
- 工业网络通讯协议
- 工厂安全事件与漏洞分析
- 工控安全关键技术
- 工控信息安全标准
- 工控系统风险评估

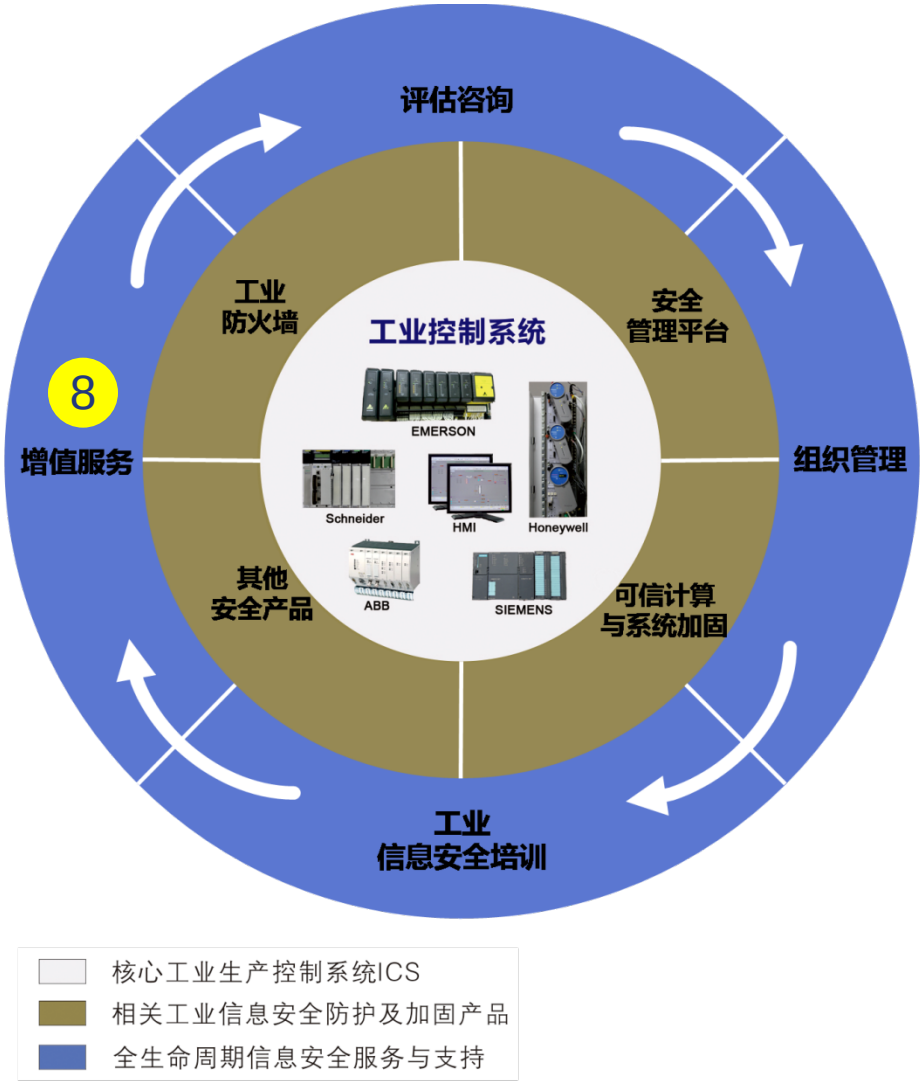


全生命周期工业控制系统信息安全解决方案

增值服务

- 工业安全日志定期分析
- 工业网络安全预警
- 工业信息安全咨询与培训
- 定期巡检及策略优化
- 系统一般及紧急故障处理

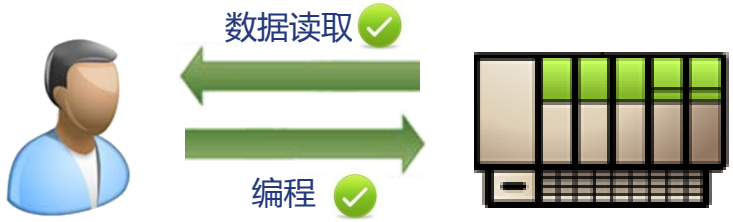
工业控制系统检维修



已建及新建控制系统的
工业信息安全解决方案思路

已建工业系统安全现状

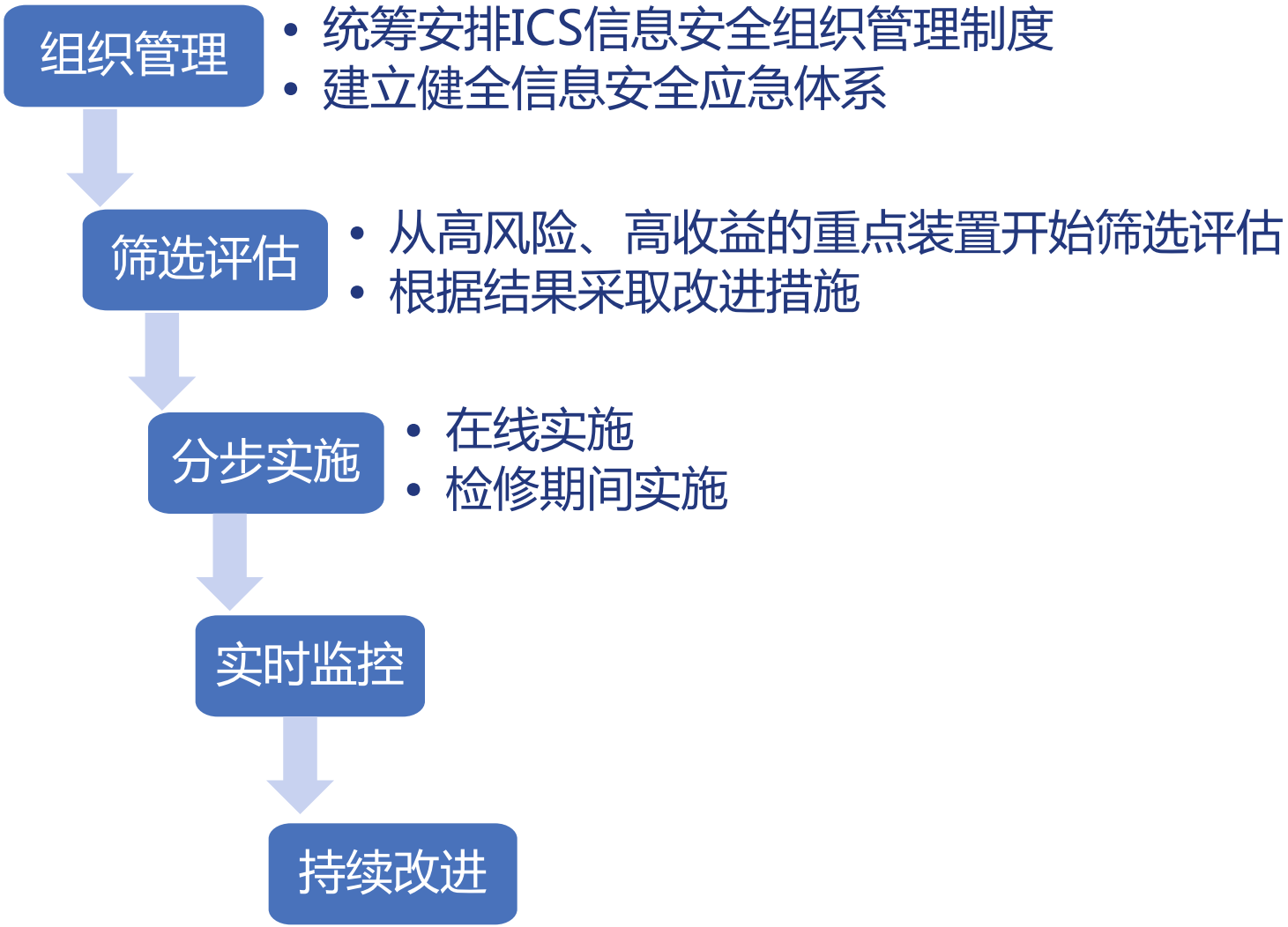
传统的ICS产品和协议，设计上未考虑信息安全因素。



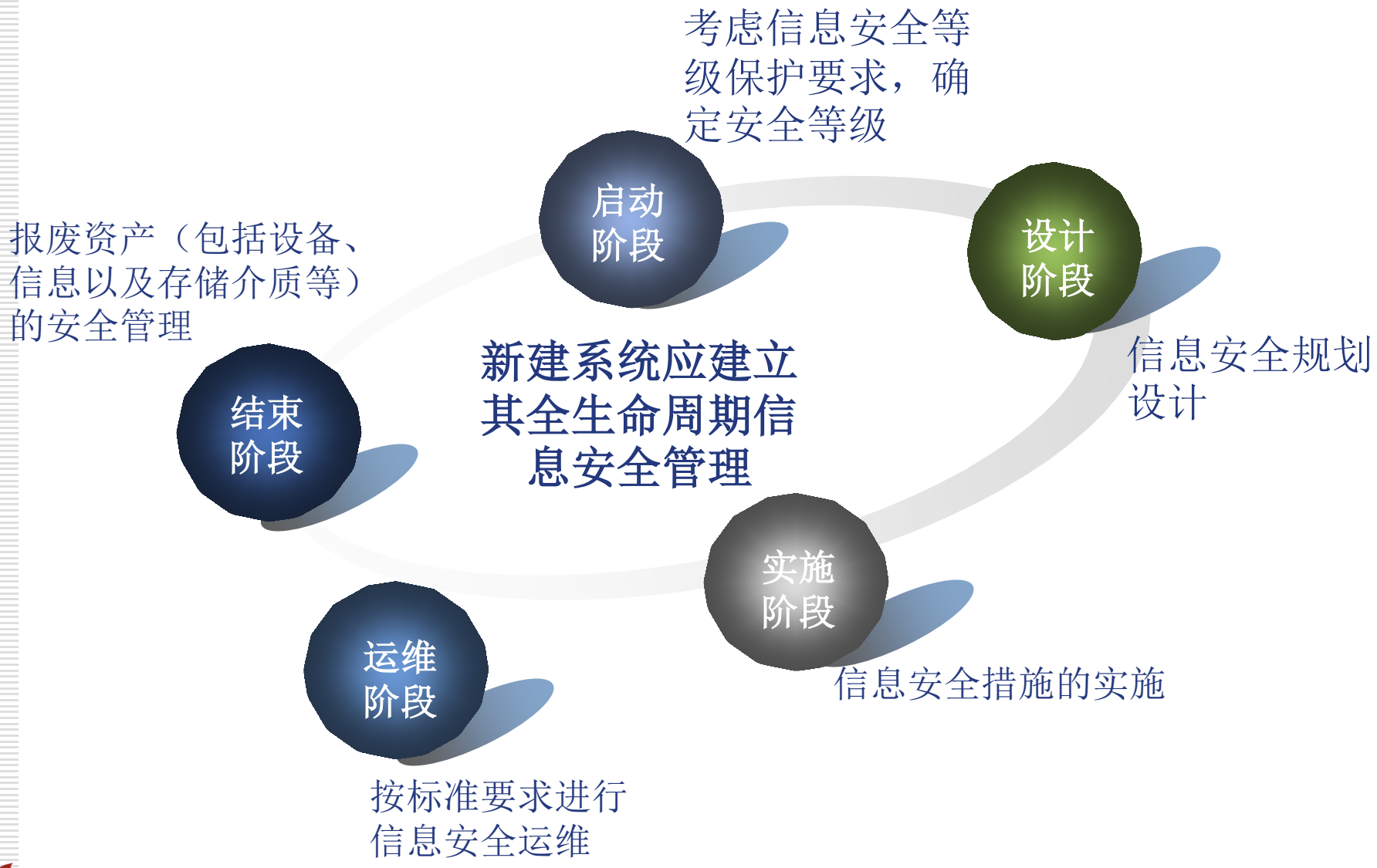
更换新的更安全的设备需要花费很长时间和很大的费用

（工控系统生命周期通常是15-20年）

已建工业系统信息安全思路



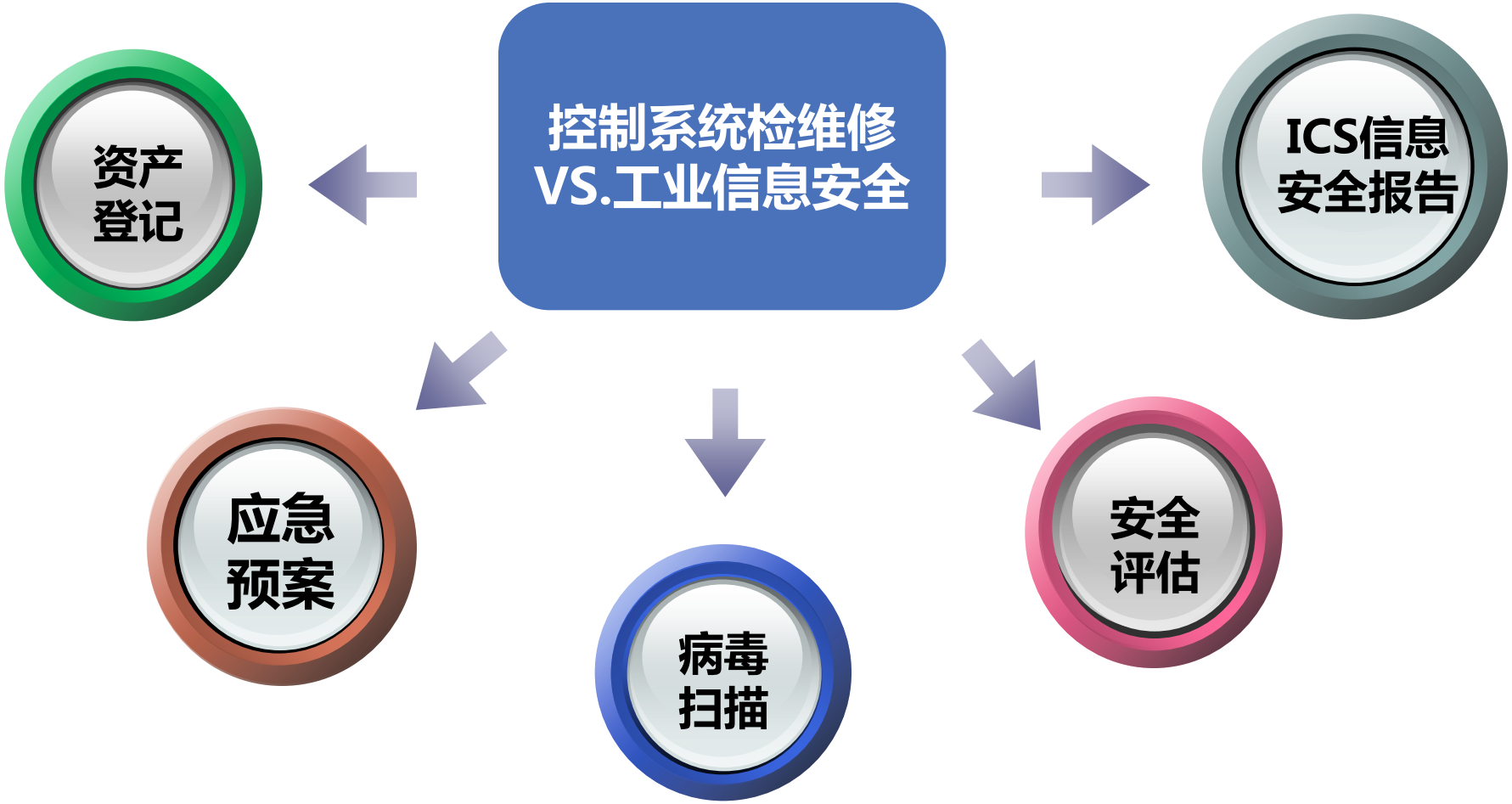
新建工业系统信息安全思路



控制系统检维修

与工业信息安全新思路

控制系统检维修与信息安全新思路



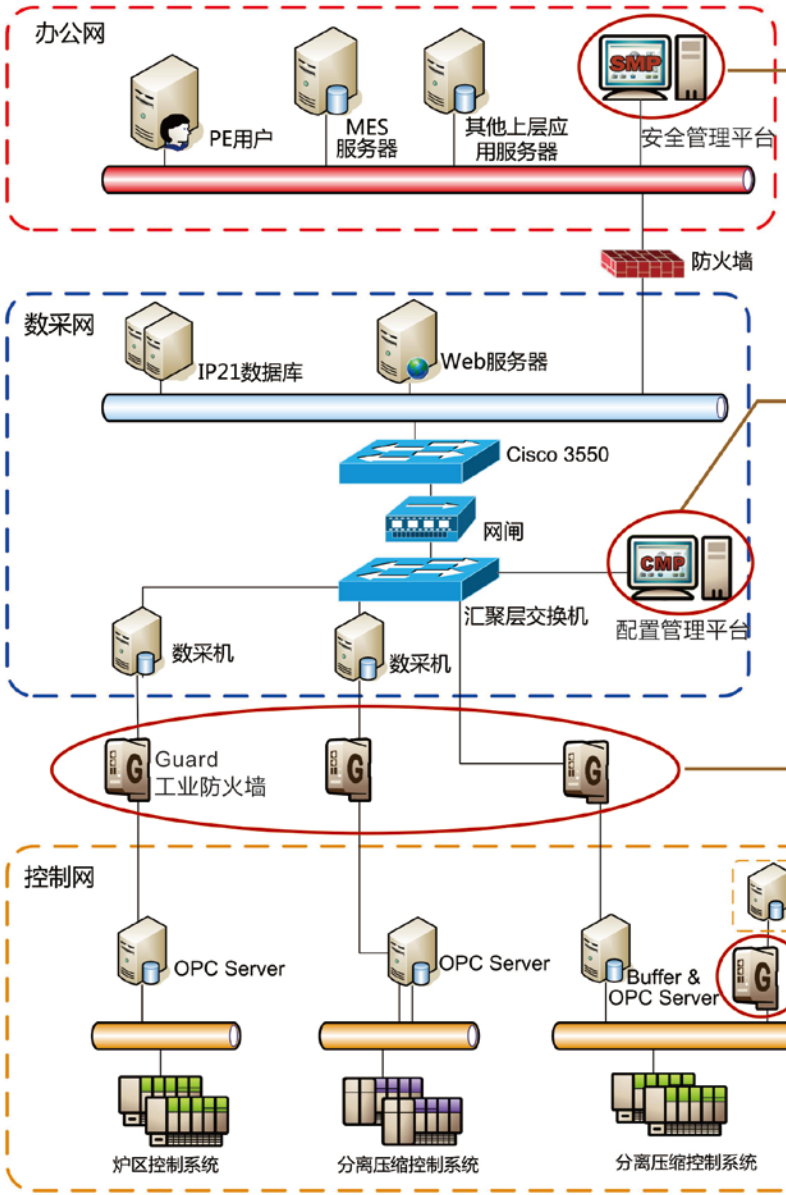
目录

1.工业信息安全现状及用户需求分析

2.全生命周期工业控制系统信息安全解决方案

3.成功案例分享

石化行业工业信息安全防护方案



安全管理平台：

对整个工业控制网络的实时监控，对报警及日志进行历史存储，便于问题追溯及分析，及时发现威胁并迅速解决

配置管理平台：

友好的人机界面，拖放式策略配置方式，用于配置、管理、监测网络中所有的Guard工业防火墙，并接收来自防火墙的报警信息

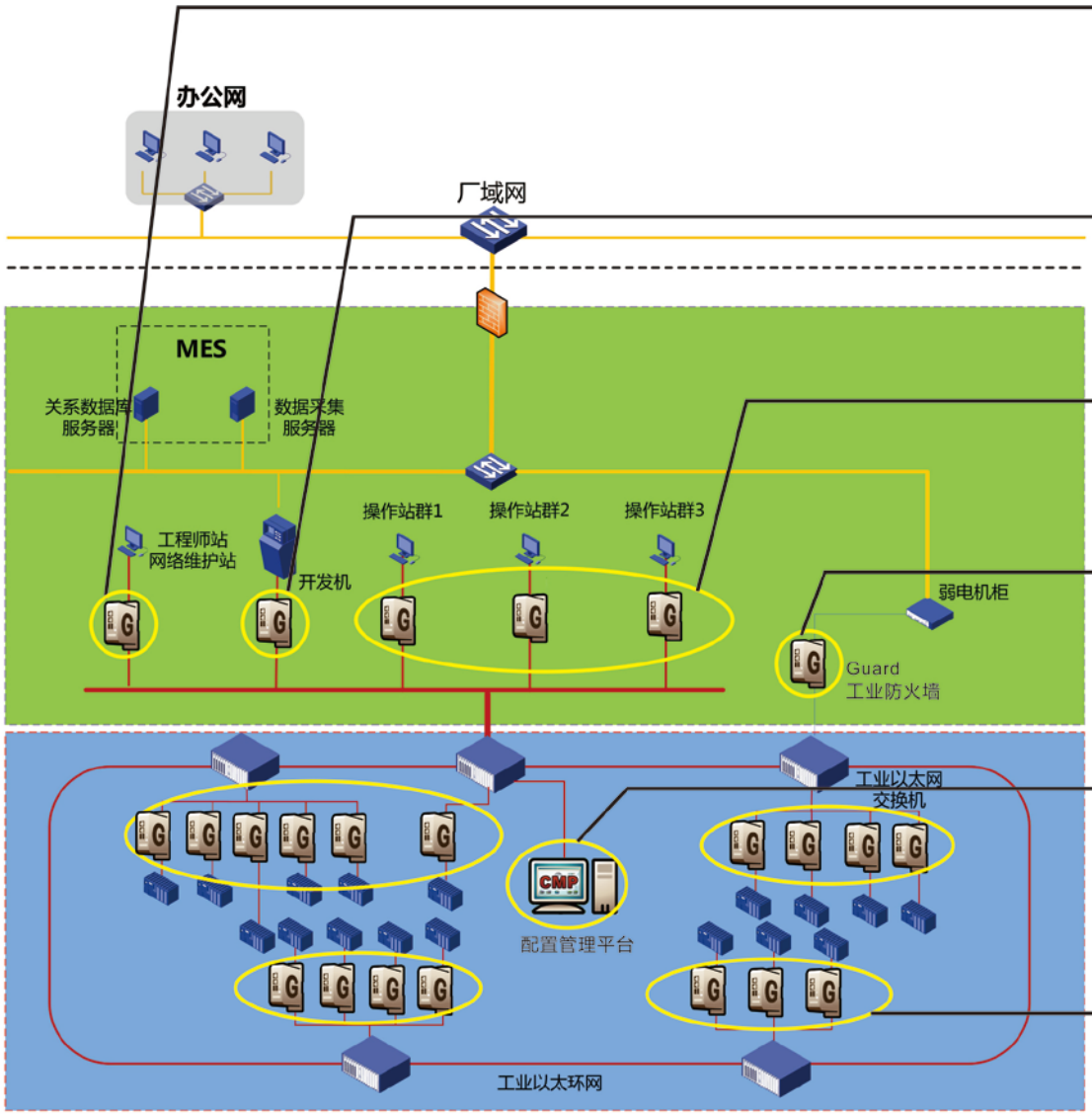
Guard工业防火墙：

对数采网与控制网进行有效隔离，只允许必要的数据包通过，防止病毒在两层网络间相互感染

Guard工业防火墙：

工程师站为控制系统风险集中点，隔离工程师站，避免风险扩散

烟草行业工业信息安全防护方案



Guard工业防火墙：

隔离工程师站，降低因工程师站作为常用对外接口易感染病毒而带来的网络风险

Guard工业防火墙：

隔离开发机，降低第三方设备接入网络带来的风险

Guard工业防火墙：

操作站群分区，防止站群间交叉感染

Guard工业防火墙：

隔离弱电机柜与控制网络，降低第三方设备接入网络而带来的风险

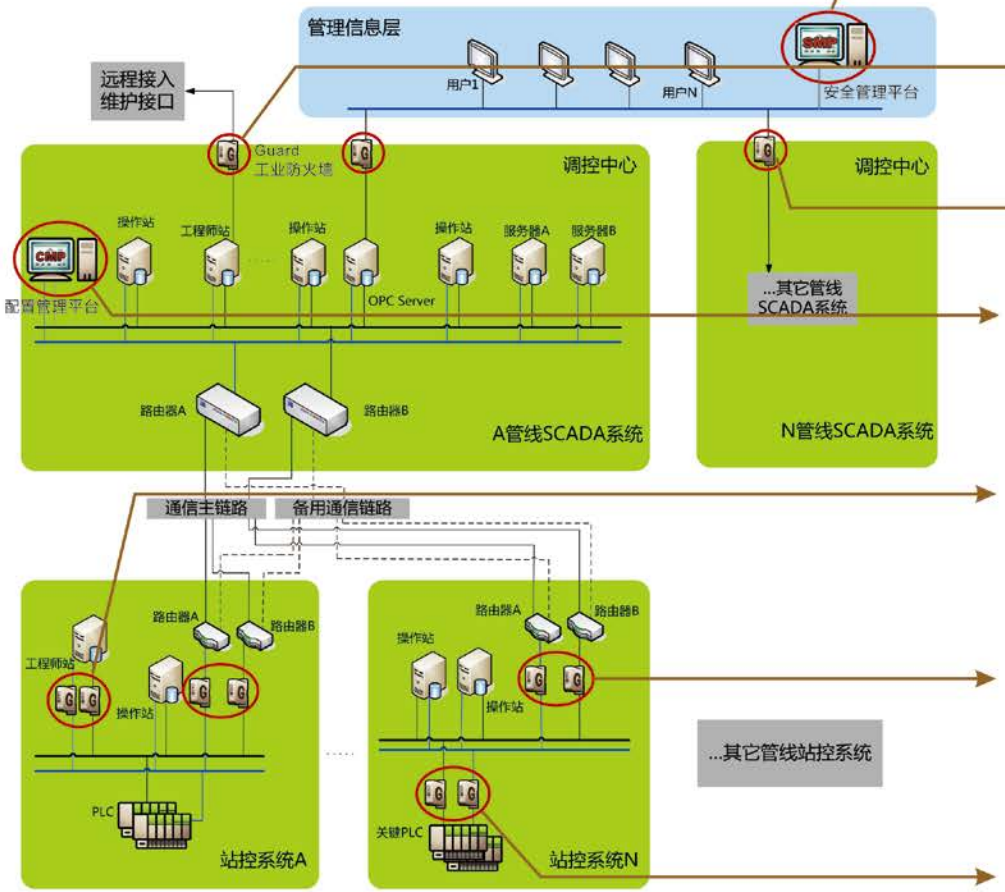
配置管理平台：

用于配置、管理、监测网络中所有的Guard工业防火墙，并接收来自防火墙的网络报警信息

Guard工业防火墙：

保护控制器，阻止对控制器的任何非法访问及控制

油气储运SCADA系统信息安全防护方案



安全管理平台：
对整个工业控制网络的实时监控，及时发现威胁并迅速解决；对报警及日志进行历史存储，便于问题溯源及分析

Guard工业防火墙：
阻止来自第三方接入点的威胁

Guard工业防火墙：
隔离SCADA系统与信息网，阻止来自上层信息网的威胁

配置管理平台：
用于配置、管理、监测网络中所有的Guard工业防火墙，并接收来自防火墙的网络报警信息

Guard工业防火墙：
隔离工程师站，避免因工程师站感染而导致的病毒扩散

Guard工业防火墙：
分区隔离，避免病毒扩散

Guard工业防火墙：
保护控制器，阻止对控制器的任何非法访问及控制

典型业绩

客户名称	应用范围	控制系统
中石化齐鲁石化	MES数采网与生产网隔离	Honeywell Yokogawa Foxboro 国电智深 上海新华
中石化广州石化	MES数采网与生产网隔离	Emerson Supcon
中石化燕山石化	MES数采网与生产网隔离	Siemens Hollysys Honeywell
酒泉钢铁集团	SCADA工业系统安全防护	AB-Rockwell
中石化长岭炼油	APC先进控制站隔离防护	Supcon Honeywell
中石油大庆石化	MES数采网与生产网隔离	Honeywell Emerson Foxboro

典型业绩

客户名称	应用范围	控制系统
中石油克拉玛依石化	工程师站隔离	Supcon Honeywell Yokogawa
中石油华北石化	MES数采网与生产网隔离	ABB AC800F
中石化徐州管道局	工控系统远程接入防护	Foxboro Schneider
内蒙古乌海化工	MES数采网与生产网隔离	Supcon
广西金桂浆纸业	数采网与生产网隔离	Hollysys
北京冶金自动化研究院	OPC通讯安全防护	Siemens
中科院软件所	MES数据安全性提升	Agilor实时数据库
中石化荆门石化	LIMS系统与生产网络隔离	Yokogawa