TOFINO多芬諾

专注工控信息安全

工业控制系统信息安全整体解决方案

刘安正

2014年10月

青岛多芬诺信息安全技术有限公司

目录

CONTENTS

工业控制系统信息安全现状

Part 1

您的控制系统是否面临这些问题？

使用U盘引起操作站/工程师站感染病毒
来自管理信息网络的病毒扩散
恶意程序非法启动
网络风暴
无实时报警和诊断工具

问题

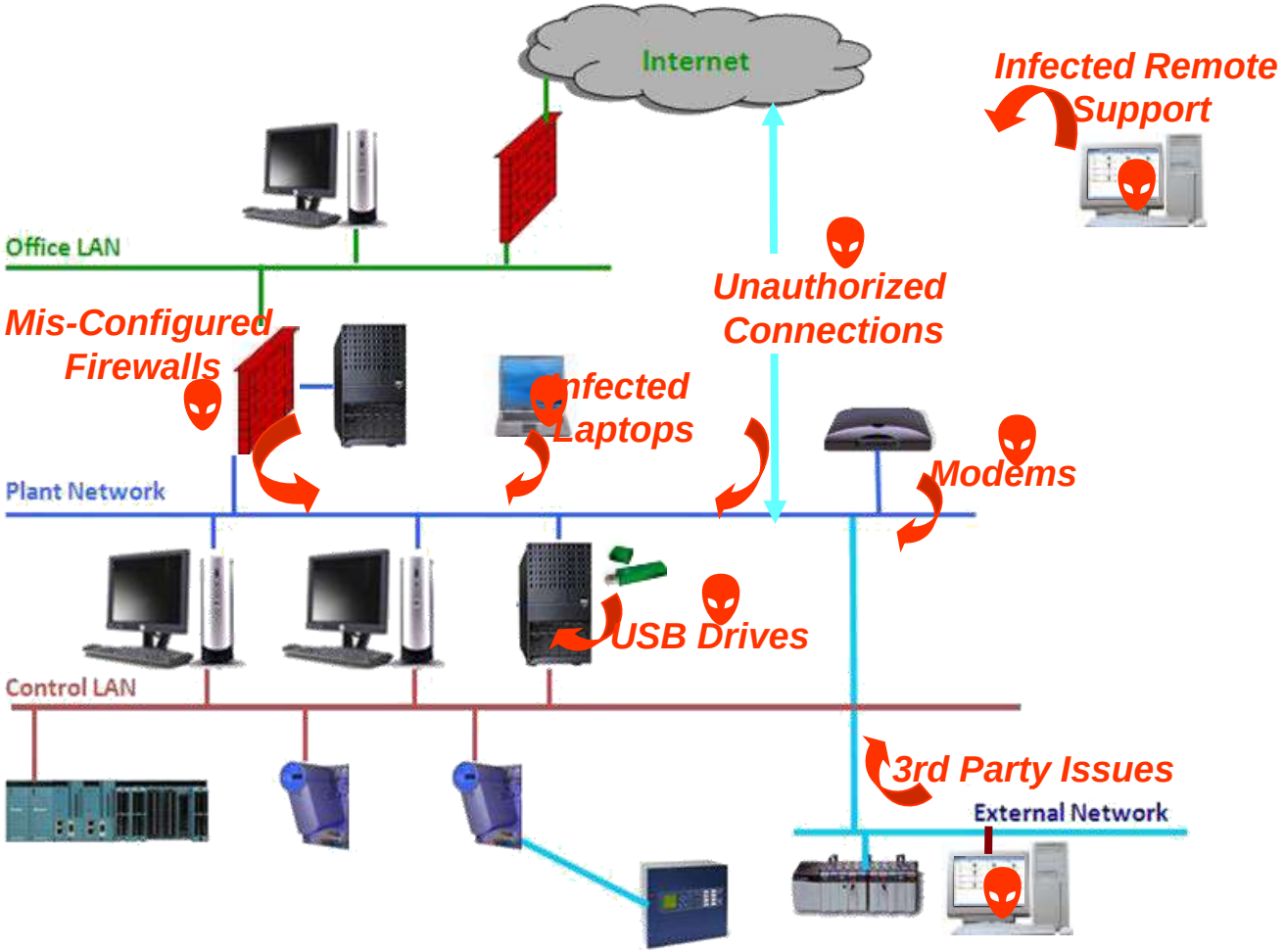
您是否听过说这些名词？

事件

2010.6 Stuxnet
2011.9 Duqu
2012.5 Flame
2014.7 Havex
2014.9 Drangonfly
… …

TOFINO多芬諾

病毒和黑客攻击工业控制系统的多种途径



工业控制系统网络安全的纵深防御

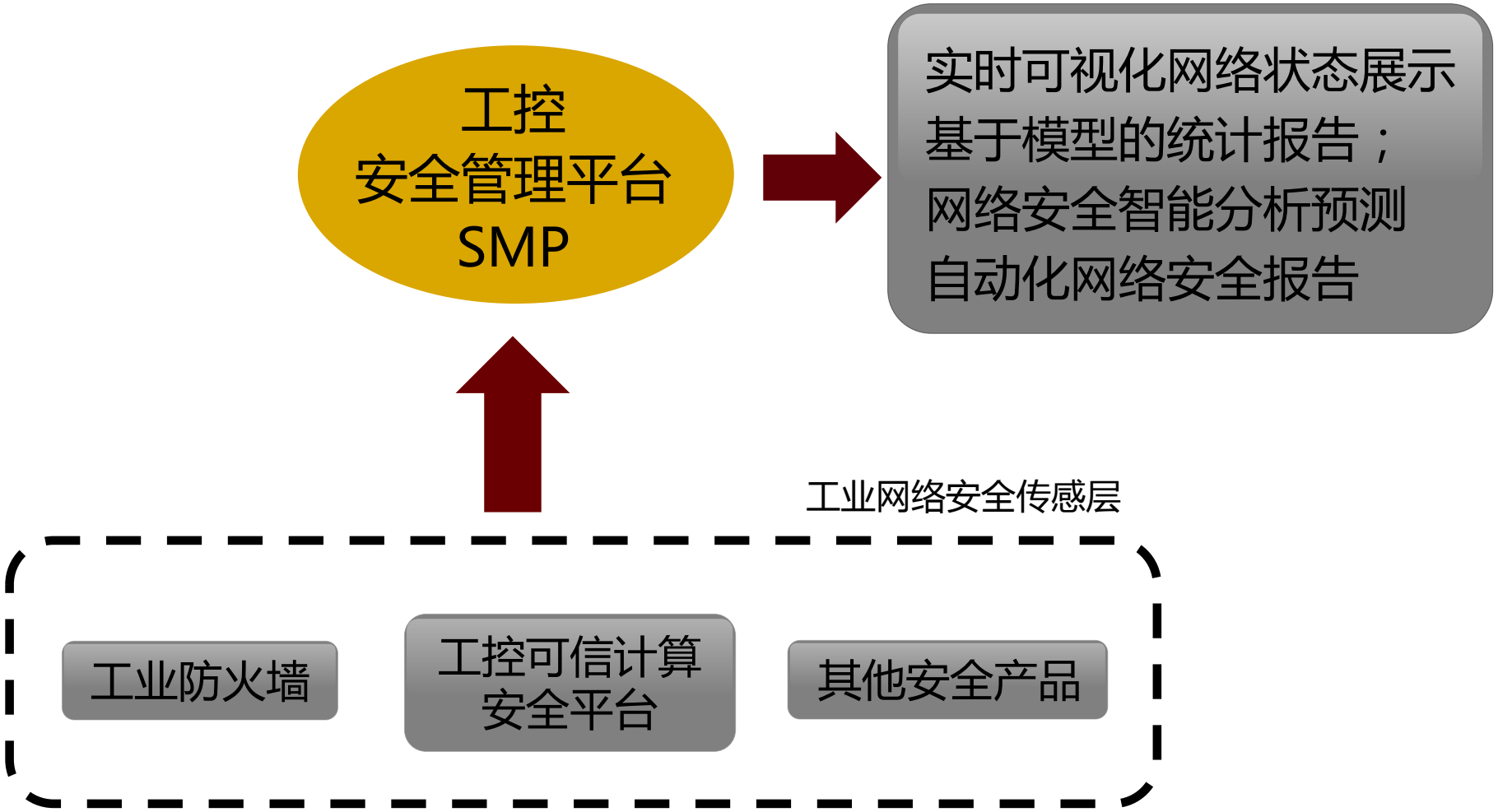
Part 2

问题总结与解决方案

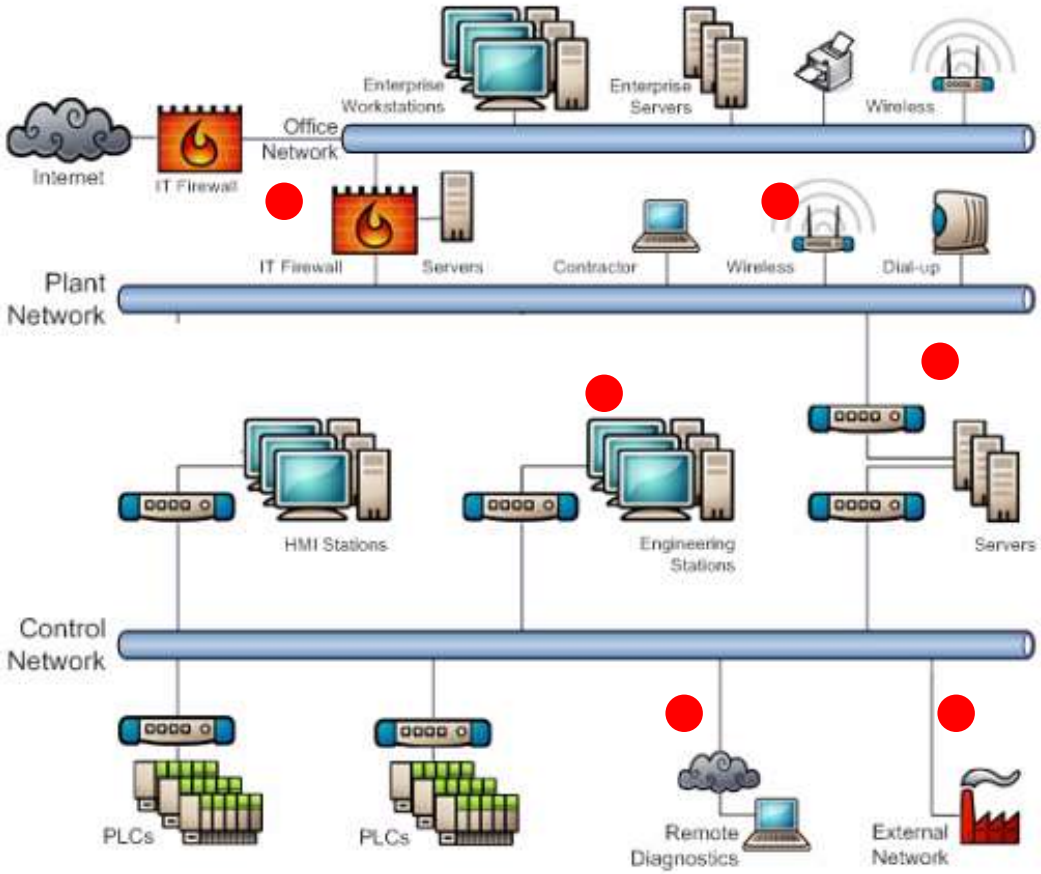
- **来自网络访问控制方面的问题：（工控防火墙-GuardIFW2400）**
- 来自管理信息网络的病毒扩散
- 网络风暴
- **来自计算机自身的安全问题：（工控可信计算平台- InTrust ）**
- 零日漏洞
- 使用U盘引起操作站/工程师站感染病毒
- 恶意程序非法启动
- **网络状态管理问题：（安全管理平台-SMP）**
- 无实时报警和诊断工具

1.行业及品牌独有性强
2.策略及应用白名单化
3.可靠及实时性要求高

工控网络安全防护及预报技术架构



ICS风险引入分析及解决方案—技术层



风险隔离，纵深防御

1.OPC数采及其它网络接口

2.工程师站、APC 站引入

3.USB，笔记本等接入

4.第三方维护

5.无线接入

6.远程维护

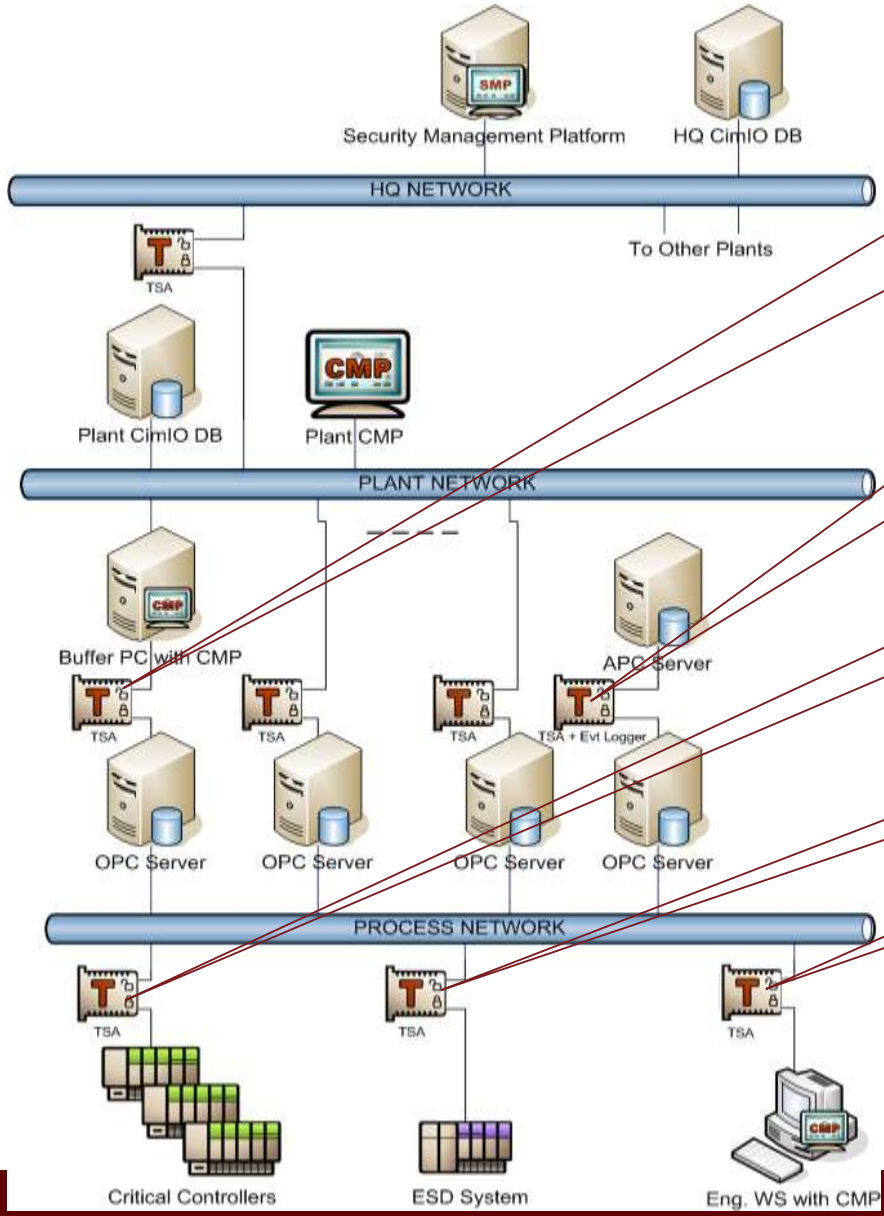
7.设备本身安全加固

Guard/Tofino工业防火墙

产品优势	解决的问题	实现效果
• 内置多种常见工业通讯协议和控制器模型 • 无IP连接技术，让入侵者无从发现攻击目标 • 工业协议深度包检测 • 网络通讯透视镜功能，智能预警分析 • 在线实施，无需停车，无需更改原有网络结构 • 工业级设计，自身强大的安全性	• 病毒扩散 • 攻击渗透	• 边界隔离、区域防护； • 从网络层面构建控制系统运行的安全环境

Guard/Tofino工业防火墙

典型应用



控制网与信息网隔离
OPC DA/HAD/A&E

APC防护

控制器防护

ESD防护

工程师站隔离

SCADA 防护
Modbus防护
其它控制防护

TOFINO多芬諾

InTrust工控可信计算安全平台

- 由**授权服务器（Intrust-S2400）**和安全**客户端（Intrust-C2400）**两部分组成
- 客户端全面度量系统所有进程，并将度量信息提交至授权服务器端
- 服务器对这些信息进行编辑后生成白名单，供客户端下载
- 客户端依据所下载的白名单对系统进行管控

产品优势

- 基于自主TCM芯片，独有加密算法，首创可信计算在工控领域的创新应用
- 强大的USB识别及管控功能
- 独有内核驻留程序，即使关闭软件也能正常执行管控功能
- 工控系统知识库智能建立，辅助客户端生成新的白名单
- 基于白名单模式，从底层BIOS开始管控所有进程

解决的问题

- 工控系统计算机病毒感染
- 已知、未知恶意代码攻击
- Windows XP等操作系统内核漏洞隐患

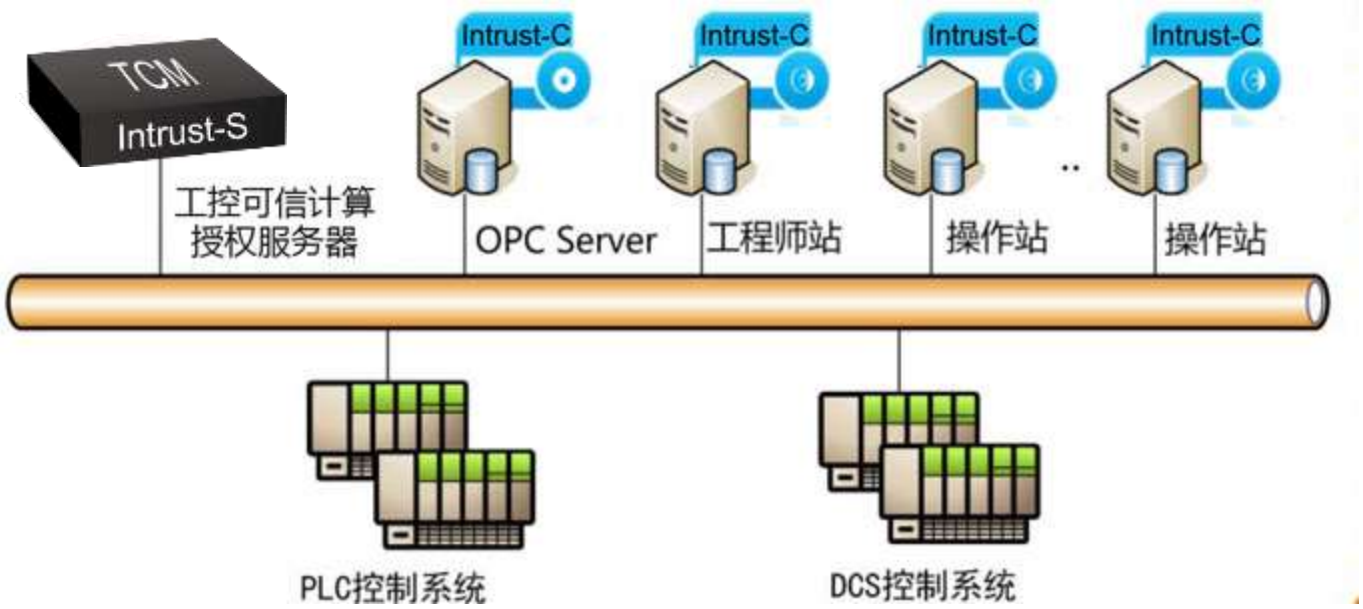
实现效果

- 提高工控系统计算机自身免疫力
- 强大的USB管控功能

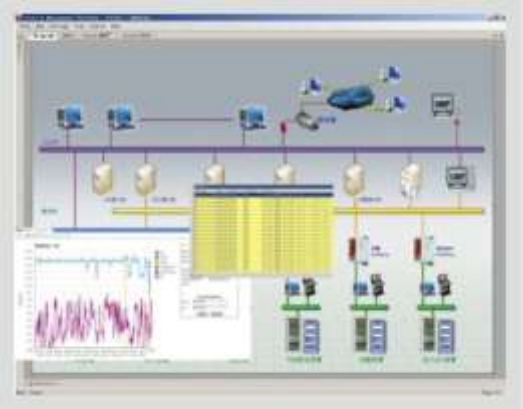
InTrust工控可信计算安全平台

典型应用

- 工控可信计算
  授权服务器
- 工控可信安全平台
  客户端软件



工控安全管理平台SMP



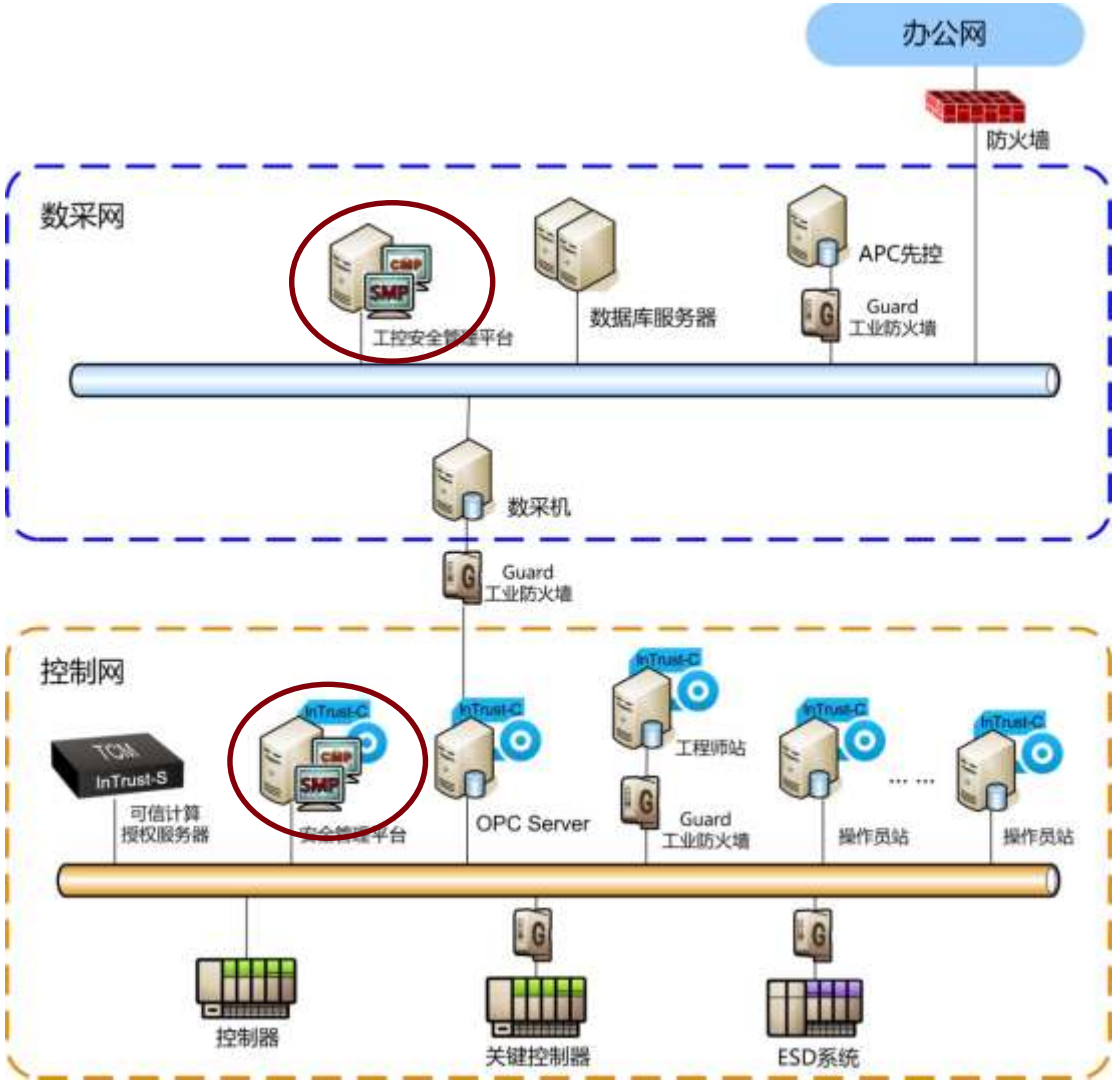
- 安全管理中心以底层工业防火墙以及其它第三方网络设备为探针
- 利用内置的“工业控制网络通讯行为模型库”核心模块，智能监控、分析控制网络行为，及时检测工业网络中出现的工业攻击、非法入侵、设备异常等情况
- 利用数据库存储、分析和挖掘技术，对危及系统网络安全的因素做出智能预警分析
- 给管理者提供决策支持，以总揽大局的方式为工厂网络信息安全故障的及时排查、分析提供了可靠的依据。

产品优势	解决的问题	实现效果
• 基于日志分类、划分等级进行报警，信息一目了然 • 依据日志重要程度的不同，采用不同的处理方式 • 设备状态监测 • 自定义过滤规则、查询条件 • 可选短信提示功能 • 网络行为智能预警分析	• 网络审计缺失； • 安全事件追踪； • 网络状态监控	• 实时监控 • 智能预警 • 自动化报告

工控安全管理平台SMP

典型应用

- 设备状态监测
- 工业网络状态实时监控
- 网络报警历史存储
- 网络日志检索分析
- 网络行为智能分析

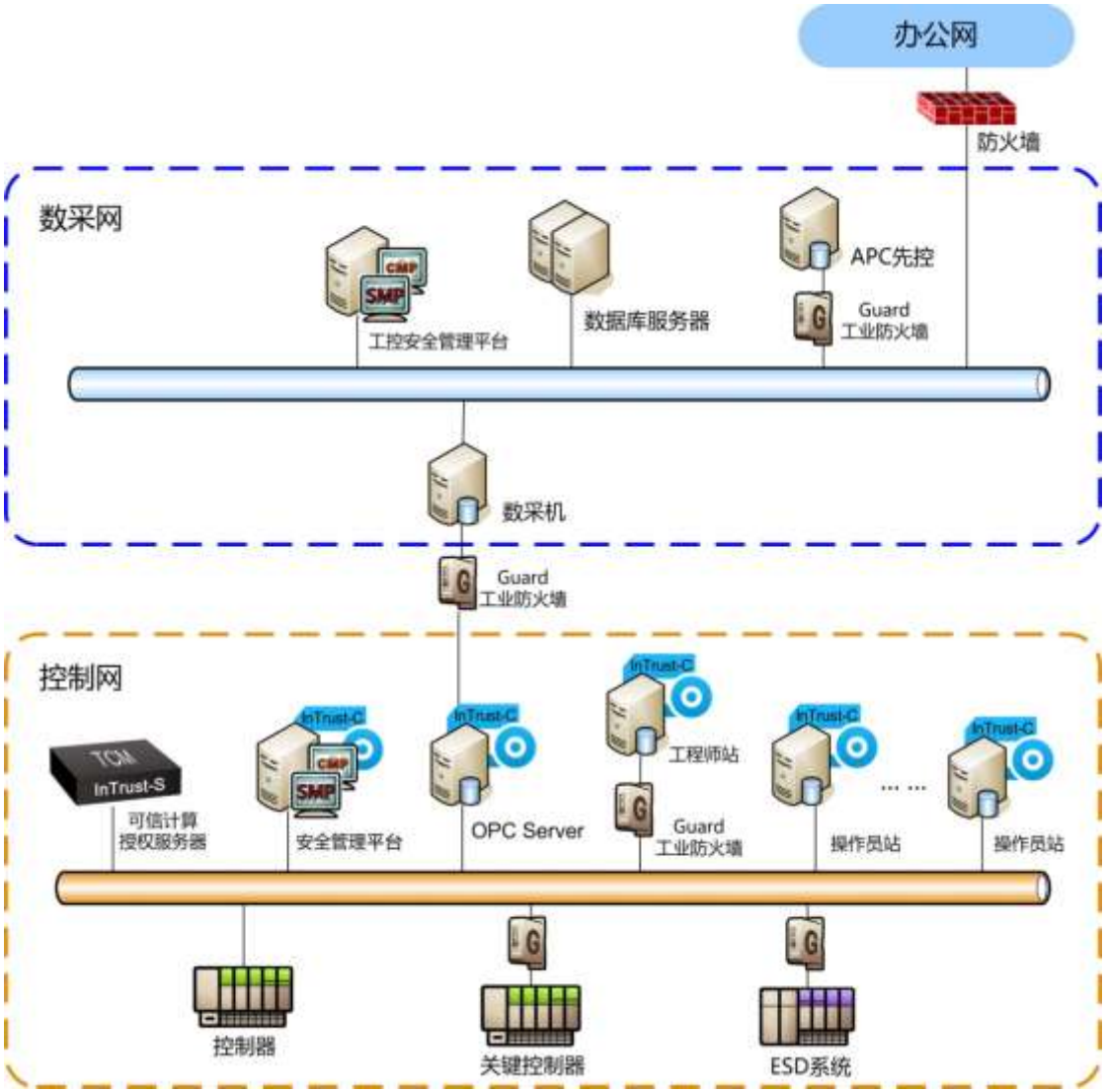


行业整体解决方案&案例分享

Part

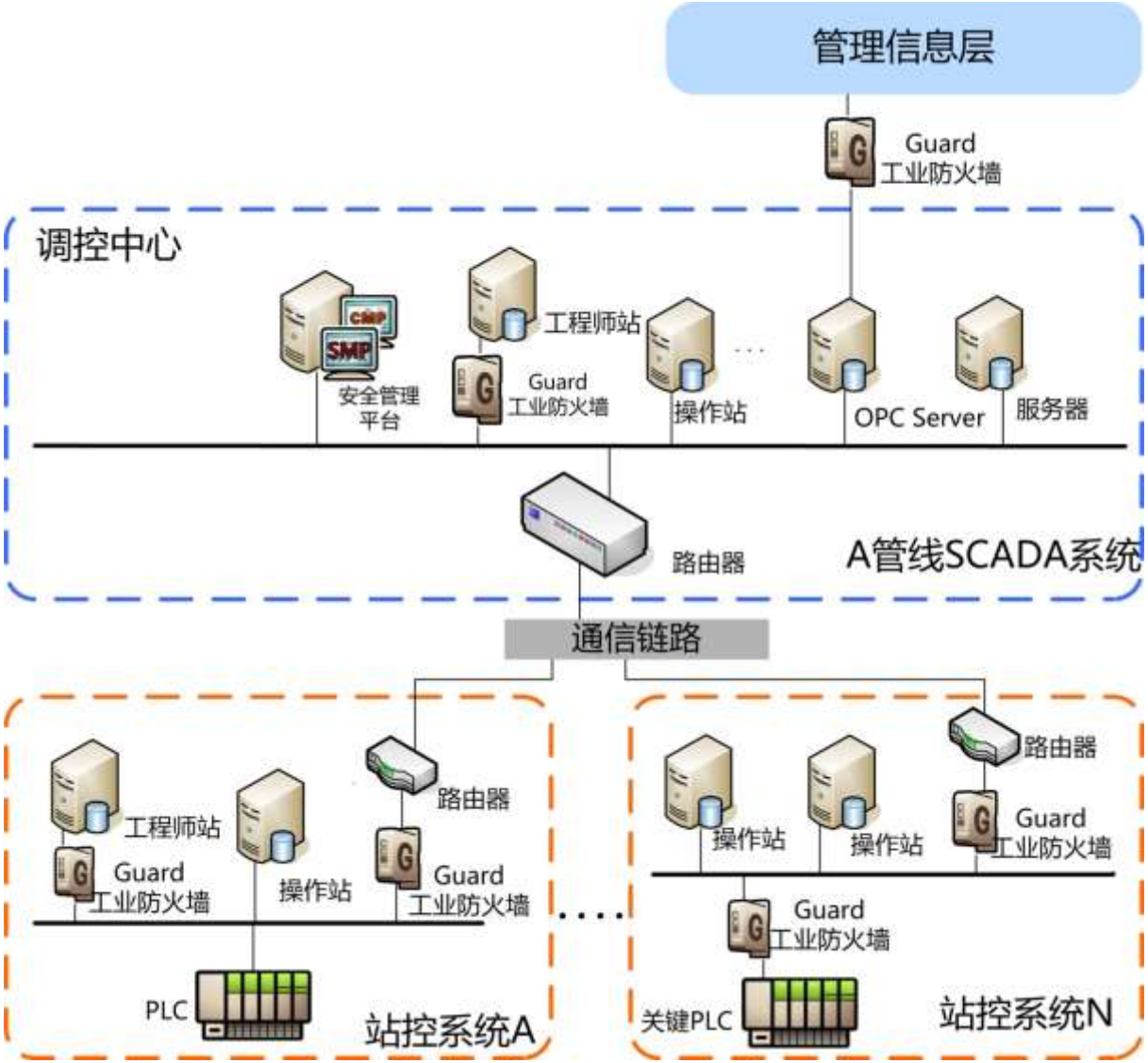
3

石化行业工控信息安全整体解决方案



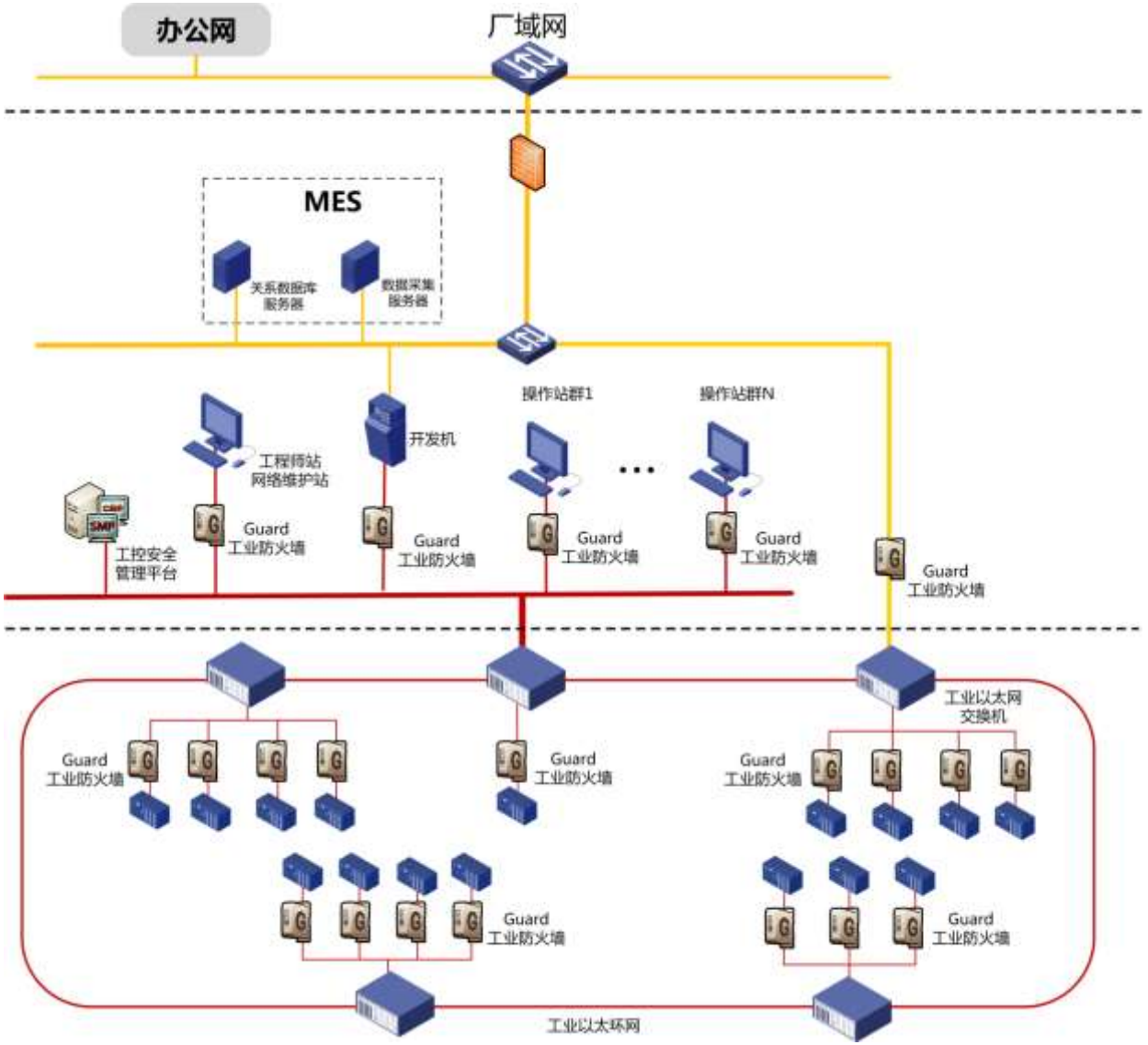
- 网络分区
- 计算机终端加固
- 智能监控

SCADA系统信息安全整体解决方案



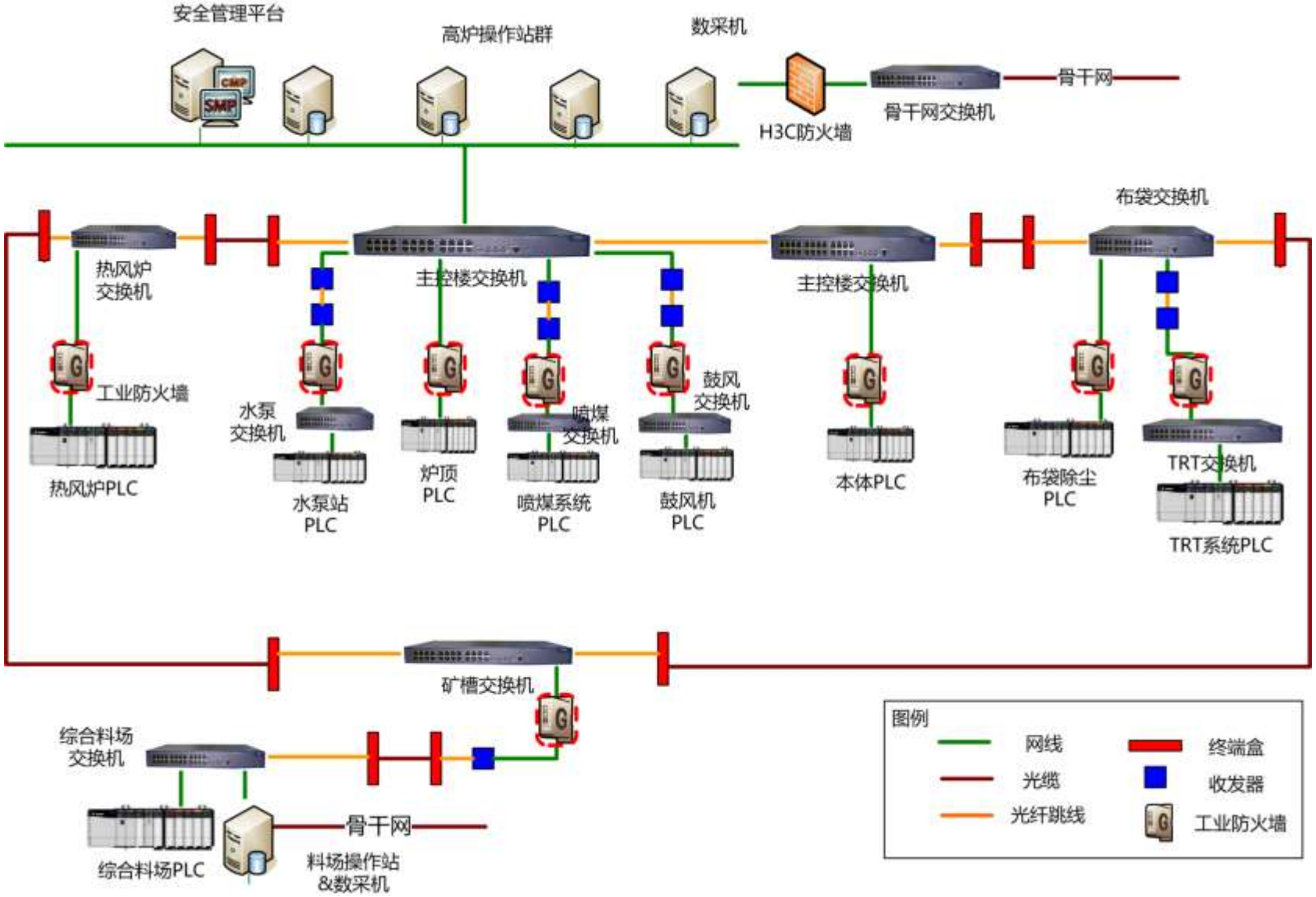
- 网络分区
- 计算机终端加固
- 智能监控

工业以太环网信息安全整体解决方案



TOFINO多芬諾

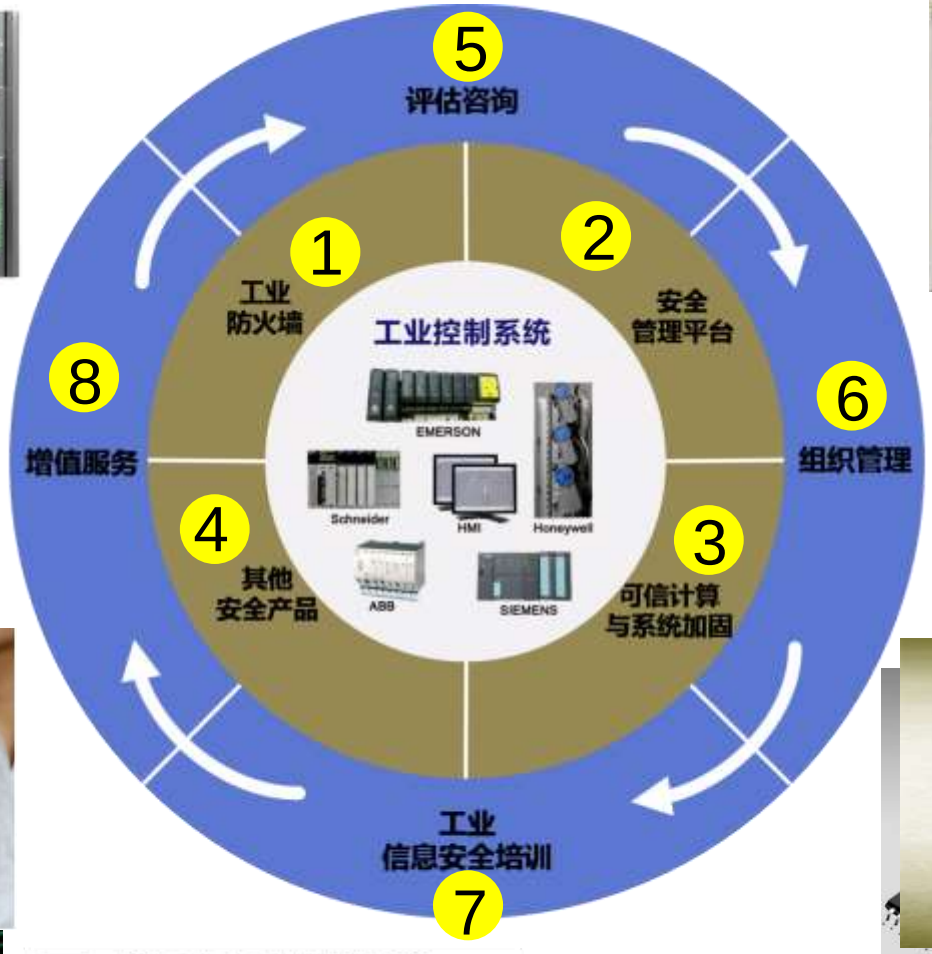
钢铁行业工控信息安全整体解决方案



全生命周期
工控系统网络安全整体解决方案

Part
4

全生命周期工控信息安全整体解决方案



核心工业生产控制系统ICS
相关工业信息安全防护及加固产品
全生命周期信息安全服务与支持

TOFINO多芬諾

部分业绩展示

石化 储运 钢铁 自动化 烟草 纸业 科研 ...

最终用户	施工时间	使用数量	用户的控制系统
中国石油化工股份有限公司广州石化分公司	2011	37	Honeywell/浙江中控
	2012	10	西门子/横河/honeywell
	2013	18	Honeywell/Foxboro
	总共	**65**	
中国石油化工股份有限公司齐鲁石化分公司	2012	85	艾默生DELTAV，横河CS3000，Honeywell PKS，横河CS3000，AB SLC500 RSview32，浙江中控 ESC-700，OMRON GX620，Honeywell HC900，国电智深，上海新华等
	总共	**85**	
中国石油化工股份有限公司燕山石化分公司	2012	44	横河CS3000；Triconex等
	2013	8	横河CS3000
	2014	7	横河CS3000
	总共	**59**	
中国石油化工股份有限公司镇海炼化分公司	2012	18	横河CS3000，Honeywell PKS，西门子
	2013	15	横河CS3000，Honeywell PKS
	总共	**33**	

部分业绩展示

行业	客户名称		应用范围	控制系统制造商	时间
石化	中石化 北京燕山分公司	炼油一厂	数采网络与DCS网络隔离	Yokogawa	2012年11月
		炼油二厂	数采网络与DCS网络隔离	Yokogawa	2012年11月
		化工一厂	数采网络与DCS网络隔离	Yokogawa Honeywell SUPCON	2012年11月
		化工三厂	数采网络与DCS网络隔离	Yokogawa	2012年11月
		化工六厂	数采网络与DCS网络隔离	SUPCON	2012年11月
		化工七厂	数采网络与DCS网络隔离	Yokogawa	2012年11月
		化工八厂	数采网络与DCS网络隔离	Honeywell SUPCON	2012年11月
		橡胶一厂	数采网络与DCS网络隔离	Honeywell HollySys	2012年11月
石化	中石化 镇海炼化分公司	四部	数采网络与DCS网络隔离 ESD安全防护 APC安全隔离	Yokogawa Honeywell	2012年11月
		五部	数采网络与DCS网络隔离 ESD安全防护 APC安全隔离	Yokogawa Honeywell	2012年10月
		一部	数采网络与DCS网络隔离 ESD安全防护 APC安全隔离	Yokogawa Honeywell Triconex	2012年9月
		三部	数采网络与DCS网络隔离 ESD安全防护 APC安全隔离	Yokogawa Honeywell	2012年9月
石化	中石化 上海石油化工 股份有限公司	炼油部	数采网络与DCS网络隔离	Honeywell Emerson	2014年6月
		烯烃部	数采网络与DCS网络隔离	Schneider Foxboro	2013年1月

部分业绩展示

行业	客户名称		应用范围	控制系统制造商	时间
石化	中石化 广州分公司	炼油一部	数采网络与DCS网络隔离	Foxboro	2011年10月
		炼油二部	数采网络与DCS网络隔离	Honeywell SIEMENS IP21	2011年10月
		炼油三部	数采网络与DCS网络隔离	Yokogawa Siemens	2011年10月
		炼油四部	数采网络与DCS网络隔离	SUPCON	2011年10月
		化工一部	数采网络与DCS网络隔离	Yokogawa SUPCON	2011年10月
		化工二部	数采网络与DCS网络隔离	Yokogawa Emerson	2011年10月
		动力事业部	数采网络与DCS网络隔离	SUPCON Siemens	2011年10月
		贮运部	数采网络与DCS网络隔离	Honeywell AB	2011年10月
		公用工程部	数采网络与DCS网络隔离	SUPCON	2011年10月
石化	中石化 荆门分公司		OPC防护 MES网络与数采网络隔离 LIMS网络安全隔离	Yokogawa SUPCON Honeywell	2014年3月
			数采网络与DCS网络隔离	Yokogawa	2012年5月
石化	中石化 仪征化纤股份有限公司		数采网络与DCS网络隔离	SUPCON	2013年12月
			数采网络与DCS网络隔离	SUPCON	2012年5月
石化	中石化长岭炼化		APC服务器安全防护	SUPCON	2013年11月
			APC先控站隔离	SUPCON	2013年3月
石化	中石化 青岛炼化		数采网络与DCS网络隔离 ESD安全防护	Honeywell	2013年4月
			数采网络与DCS网络隔离 ESD安全防护 APC安全隔离	Siemens Honeywell	2012年8月

部分业绩展示

行业	客户名称		应用范围	控制系统制造商	时间
石化	中石化 海南炼化		控制网络防护	Siemens HollySys Triconex	2013年3月
石化	中石化 湖北化肥厂		数采网络与DCS网络隔离	Honeywell	2013年5月
			数采网络与DCS网络隔离	Yokogawa	2012年7月
石化	中石化 西安石化		数采网络与DCS网络隔离	HollySys	2012年10月
石化	中石油 大庆炼化分公司		数采网络与DCS网络隔离	SUPCON	2014年5月
石化	中石油 大庆石化分公司	化肥厂	数采网络与DCS网络隔离	Honeywell	2011年11月
		炼油厂	数采网络与DCS网络隔离	Foxboro Honeywell Yokogawa Emerson	2011年11月
		化工一厂	数采网络与DCS网络隔离	Yokogawa	2011年11月
		化工三厂	数采网络与DCS网络隔离	Honeywell	2011年11月
		储运公司	数采网络与DCS网络隔离	SUPCON	2011年11月
石化	中石油 华北石化		控制网络防护	ABB AC800F	2012年9月
石化	中石油 独山子石化分公司		OPC防护	Yokogawa	2012年3月
石化	中石油 克拉玛依分公司炼油厂		OPC防护 操作站隔离	浙大中控 Honeywell Yokogawa	2010年10月
石化	中海油 东方精细化工		控制网络防护	Emerson	2013年4月

部分业绩展示

行业	客户名称		应用范围	控制系统制造商	时间
储运	中石油 天津LNG项目		SCADA系统防护	Foxboro	2014年4月
储运	中石化 徐州管道局	廉江茂名线	SCADA系统防护	Foxboro	2014年7月
		长阜宁复线	数采网络与DCS网络隔离	Foxboro	2013年11月
		天津商储	控制网络防护	Foxboro	2013年4月
储运	中石化 安庆-怀宁原油管道工程 SCADA系统		控制网络防护	Schneider	2013年4月
化工	焦作佰利联化工有限公司		OPC安全防护	SUPCON	2014年4月
煤化工	内蒙古乌海化工		数采网络与DCS网络隔离	SUPCON	2011年10月
烟草	上海卷烟厂		生产监控网络隔离	ROCKWELL	2014年3月
烟草	川渝中烟成都卷烟厂		OPC安全防护	ROCKWELL	2013年8月
烟草	中烟常德卷烟厂		控制网络防护	Siemens	2013年4月
冶金	酒泉钢铁(集团)有限责任公司		SCADA防护	ROCKWELL	2013年11月
冶金	北京冶金自动化院		生产网与控制网隔离 控制网区域管控 控制器防护	SIEMENS	2011年8月

TOFINO多芬諾

专注工控信息安全

谢谢！

刘安正

E-mail：Alex.Liu@tofinosecurity.com.cn

TEL：4006-556-776

青岛多芬诺信息安全技术有限公司