
# 恩创工业信息安全

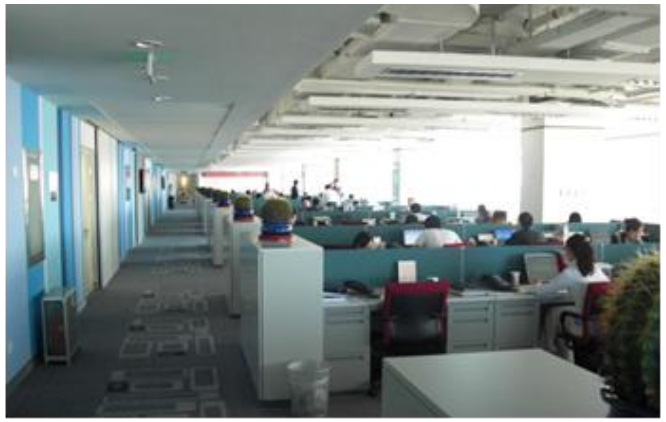
安通恩创信息技术（北京）有限公司

AVCOMM 恩创 INDUSTRIAL IT

# 目录

# 恩创历程

- **成立于2009年**
- **中关村的“土著”公司**
  - 30年电气及自动化经验
  - 15年工业软件开发经验
  - 10年工业网络经验
  - 5年工业信息安全经验
- **工业网络产品应用民航行业占有率第一**
- **工业信息安全产品应用化工行业领先**
- **产品应用遍及市政，交通，石化，电力多行业**
- **我们的使命是将先进的信息技术带入工业控制与信息领域**



AVCOMM 恩创 INDUSTRIAL IT

# 恩创产品线

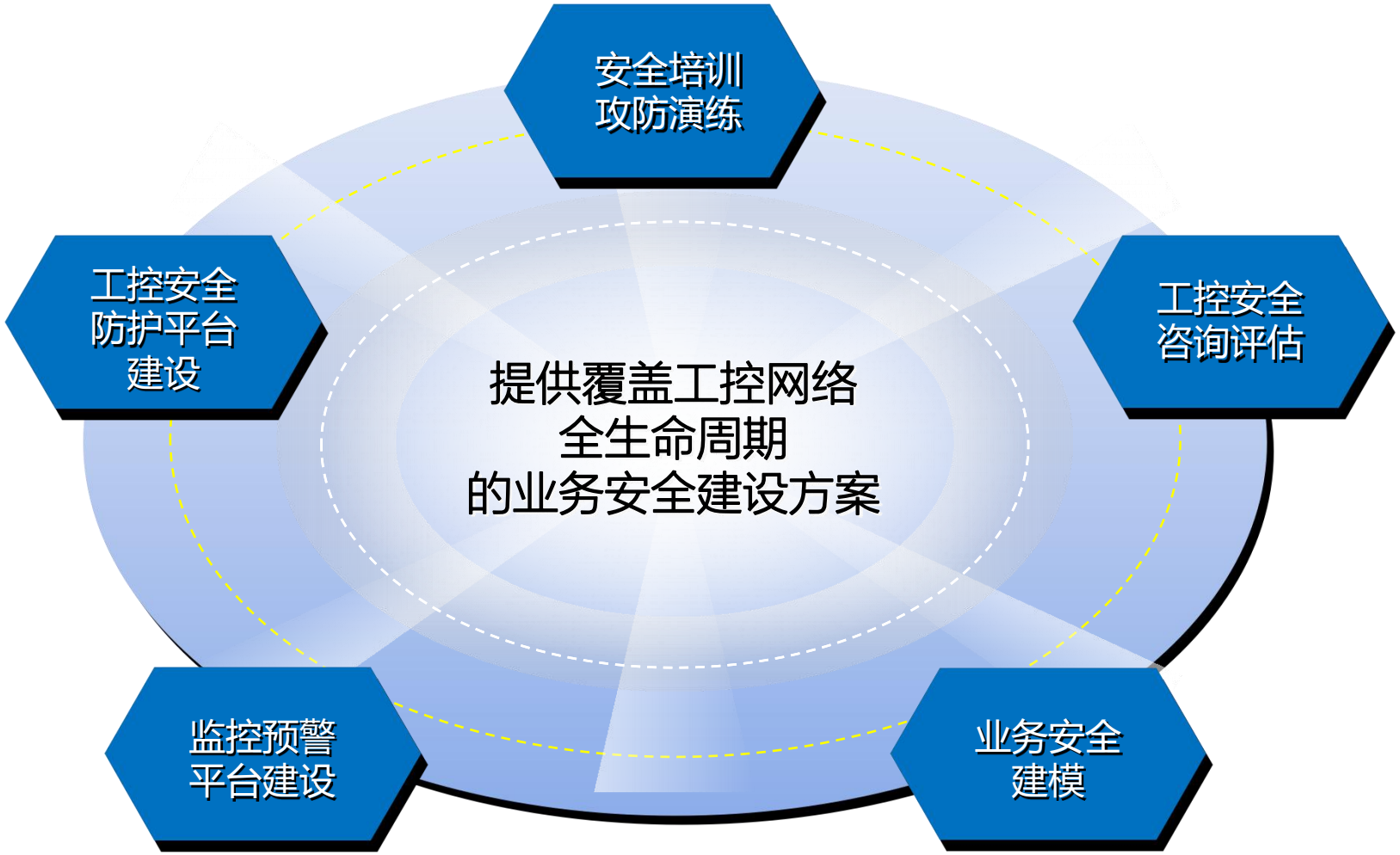
工业通信

工业信息安全


工业服务器与存储

工业X

# 恩创工业信息安全



# 公司资质


■ ISCCC信息技术服务管理体系认证


■ ISCCC信息安全管理体系认证


■ ISCCC信息技术服务管理认证

# 公司人员资质


■ PMP项目经理认证

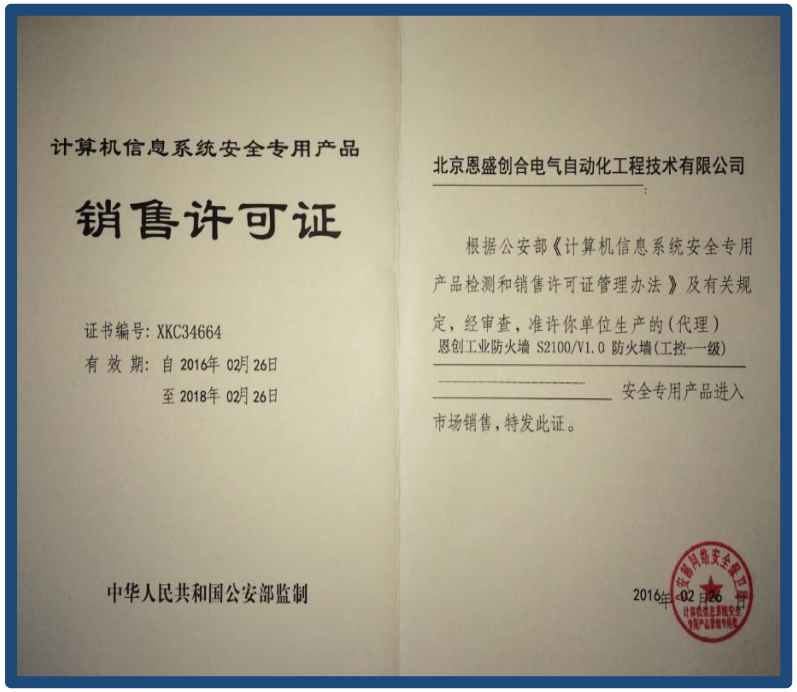

■ 信息安全保障人员认证


■ CISP注册信息安全专业认证

# 产品认证


■ CE、FCC认证


■ 公安部检验认证

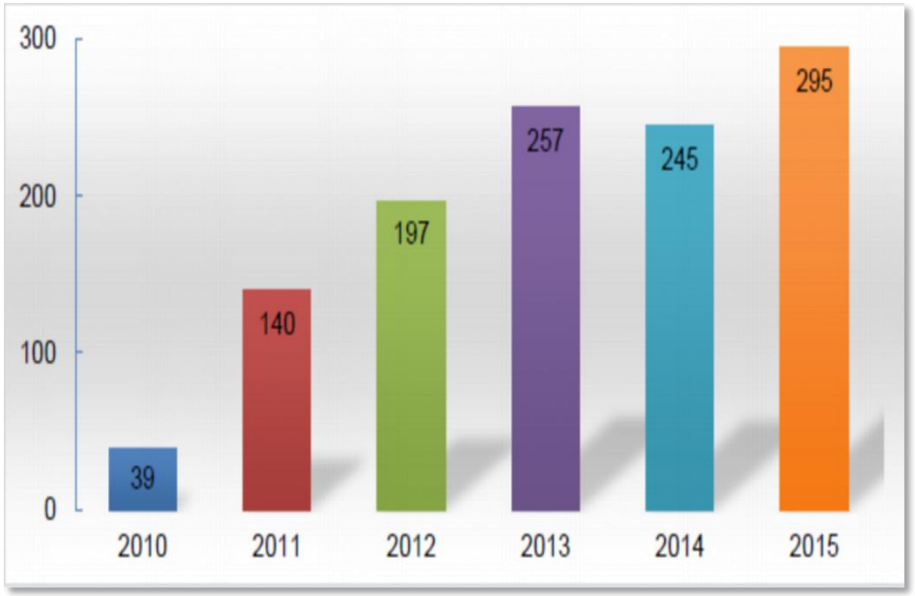


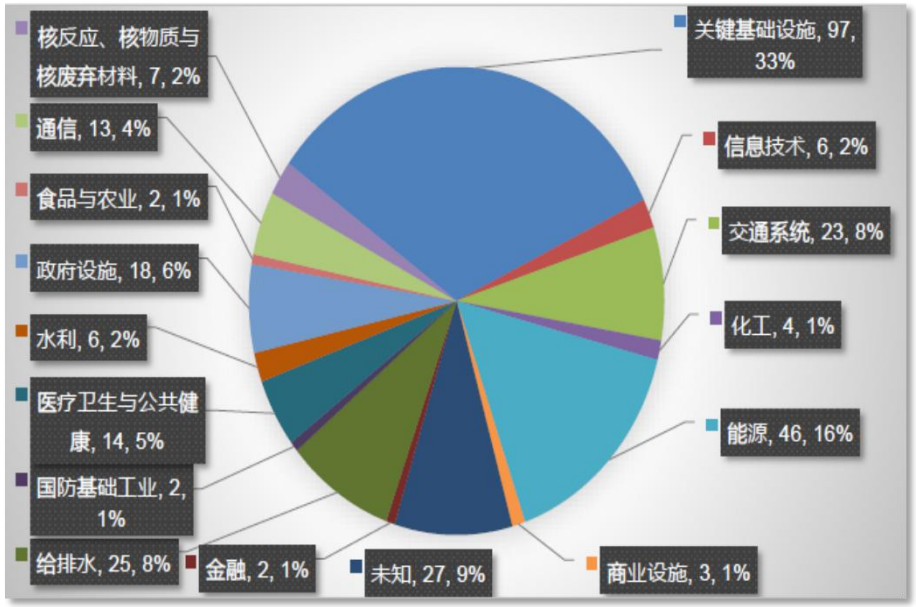

■ 公安部销售许可证

# 工控信息安全严峻形势

- ICS-CERT是美国国土安全局下设的专门针对工业控制系统信息安全应急响应的组织.

全称 Industrial Control System Cyber Emergency Respond Team (ICS-CERT)

# 能源行业工控安全政策

**2002** — 经贸委30号令

- 《电网和电厂计算机监控系统及调度数据网络安全防护规定》

**2004** — 电监会5号令

- 《电力二次系统安全防护规定》

**2011** — 工信部451号文

- 《关于加强工业控制系统信息安全管理的通知》GB/T 50609-2010《石油化工工厂信息系统设计规范》

**2013** — 能源局387号文

- 《关于开展电力工控PLC设备信息安全隐患排查及漏洞整改工作的通知》

**2015** — 能源局36号文

- 《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》

**2016** — 工信部338号文

- 《工业控制系统信息安全防护指南》

# 工控信息安全事件1-Windows操作系统

- 2011年,某国有企业生产装置控制系统感染Conficker病毒，造成控制系统服务器与控制器通讯不同程度地中断。

- conficker病毒同时具有蠕虫病毒和下载者病毒的多重属性，Conficker利用Windows系统的已知MS08-067漏洞大肆传播，甚至能够利用U盘、网络共享等方式传播，当Conflicker病毒进入系统后，首先破坏系统中的默认属性设置，接着会自动搜索局域网内有漏洞的其他电脑，一旦发现存在漏洞的计算机系统，就会激活该漏洞并同感染系统创建链接，最后进行远程感染。

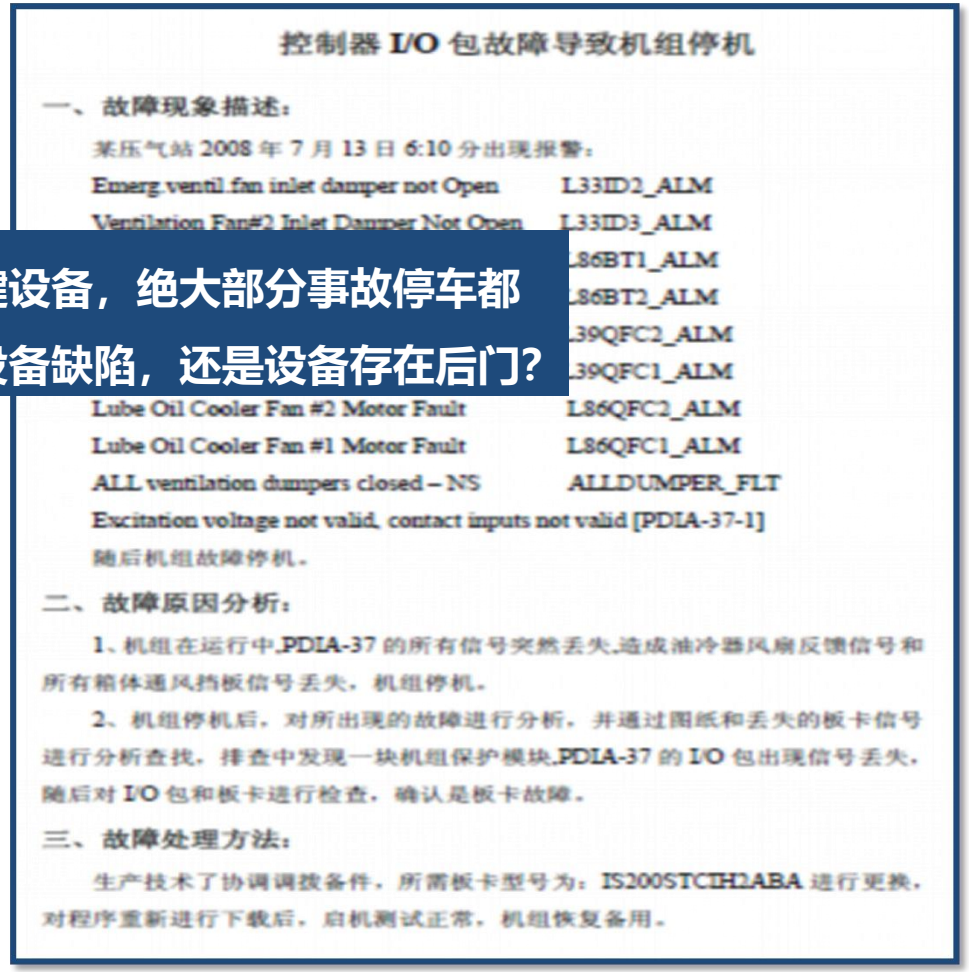
# 工控信息安全事件2-ESD控制器通信

- 某国有大型油田管道公司下属某分压站，压缩机ESD系统控制器-HIMAtrix F30（HIMA公司），发现其控制网络遭到大量-大数据包攻击，导致其控制器以太网通讯故障，造成压缩机停机。后更改为串口通讯，才得以保障其继续运行，但由于通讯能力的限制，导致其操作和数据显示有所延迟。给系统的稳定性和有效性带来隐患。


# 工控信息安全事件3- I/O通信

- 某国有大型企业生产系统采用远程IO，控制系统IO模块通讯故障，导致系统停车。


- **实地调研发现，工控系统关键设备，绝大部分事故停车都是硬件故障造成的！是控制设备缺陷，还是设备存在后门？**



控制器 I/O 包故障导致机组停机

一、故障现象描述：

某压气站 2008 年 7 月 13 日 6:10 分出现报警：

| | |
|---|---|
| Emerg ventil fan inlet damper not Open | L33ID2_ALM |
| Ventilation Fan#2 Inlet Damper Not Open | L33ID3_ALM |
| | L86BT1_ALM |
| | L86BT2_ALM |
| | L39QFC2_ALM |
| | L39QFC1_ALM |
| Lube Oil Cooler Fan #2 Motor Fault | L86QFC2_ALM |
| Lube Oil Cooler Fan #1 Motor Fault | L86QFC1_ALM |
| ALL ventilation dumpers closed – NS | ALLDUMPER_FLT |

Excitation voltage not valid, contact inputs not valid [PDIA-37-1]

随后机组故障停机。

二、故障原因分析：

1、机组在运行中,PDIA-37 的所有信号突然丢失,造成油冷器风扇反馈信号和所有箱体通风挡板信号丢失，机组停机。

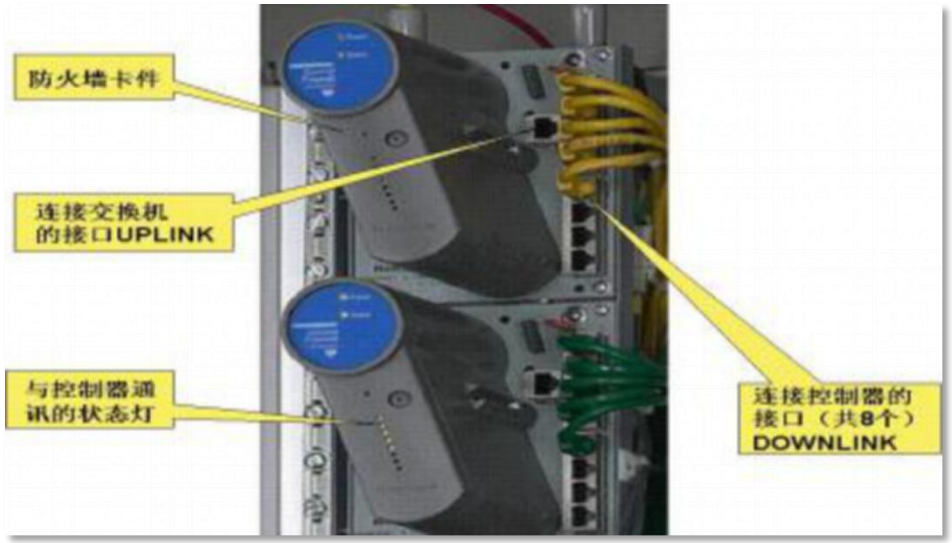
2、机组停机后，对所出现的故障进行分析，并通过图纸和丢失的板卡信号进行分析查找，排查中发现一块机组保护模块,PDIA-37 的 I/O 包出现信号丢失，随后对 I/O 包和板卡进行检查，确认是板卡故障。

三、故障处理方法：

生产技术了协调调拨备件，所需板卡型号为：IS200STCIH2ABA 进行更换，对程序重新进行下载后，启机测试正常，机组恢复备用。

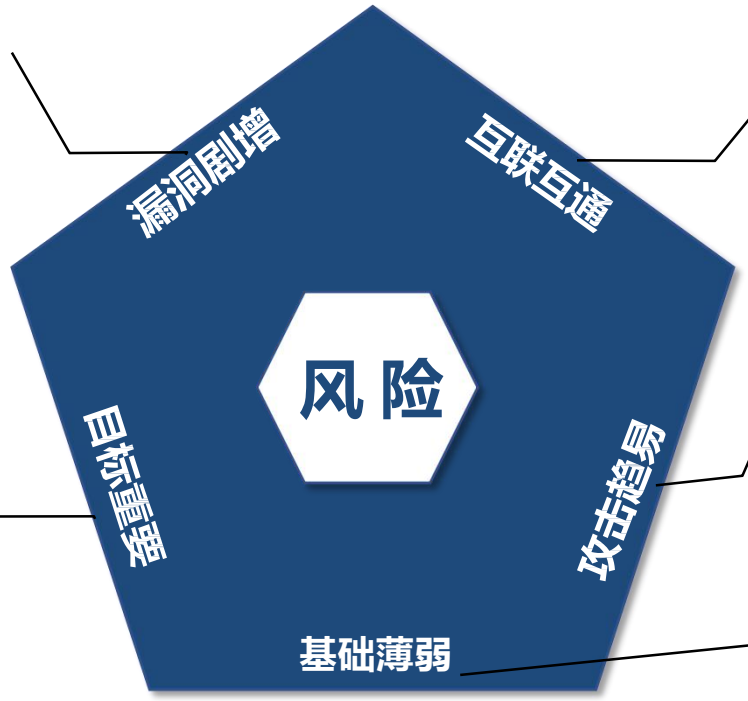
# 工控信息安全事件4- DCS系统病毒感染

- 2012年，某国有大型企业采用霍尼控制系统，系统运营商在对其DCS系统TPS3000软硬件固件版本升级过程中，由于操作不当，导致整个控制网络感染病毒，造成生产系统停车。最终，公司对所有操作终端和服务器进行了更换，DCS系统升级为PKS C300。




# 工控安全事件思考：风险存在

- 工控软硬件产品在设计之初就很少考虑安全问题，导致安全漏洞不断涌现。迄今已发现1552个工业控制软硬件设备漏洞，涉及123家工控厂商，33%(516个)没有被修复，90%的漏洞披露于“震网”事件后，465个漏洞为易利用的HMI漏洞。




- 工业控制系统正从封闭走向开放和互联，工控系统的网络安全边界明显扩大。
- 由于黑客大会、开源社区、白帽社区的出现，导致获取工控系统的攻击方法越来越容易。
- 工控系统作为国家关键基础设施的重要组成部分，已经成为网络部队、黑客、极端势力攻击的重要目标。
- 我国工控安全防护处于起步阶段，存在不少问题，难以有效应对国家级的、有组织的、高强度的网络攻击。

# 工控安全事件思考：控制设备风险

- 国内工业产线采用的工业控制设备基本上都是来自国外厂商，如艾默生、霍尼韦尔、AB、 西门子、施耐德等，而这些控制设备设计的时候更多是为了实现功能，安全性考虑不足，存在很多高危安全漏洞，一旦被攻击利用会导致严重后果。

| | | | |
|---|---|---|---|
| Honeywell Experion PKS拒绝服务... | 中 | 391 | |
| 多款Honeywell Uniformance Proc... | 高 | 1683 | |
| Honeywell XL Web Controller目录... | 高 | 1606 | |
| Honeywell Experion PKS存在多个... | 高 | 865 | |
| Honeywell Experion PKS文件包含... | 中 | 945 | |
| Honeywell Experion PKS 'confd.... | 中 | 894 | |
| Honeywell Experion PKS存在多个... | 高 | 868 | |
| Honeywell Experion PKS 'dual_o... | 高 | 856 | |

| | | | |
|---|---|---|---|
| 多款Schneider Electric产品资源... | 中 | 373 | |
| 多款Schneider Electric产品拒绝... | 高 | 278 | |
| Schneider Electric TSXP572634M... | 高 | 482 | |
| Schneider Electric Unity PRO远... | 高 | 411 | |
| Schneider Electric Modicon M34... | 高 | 1852 | |
| Schneider Electric InduSoft We... | 高 | 1082 | |
| Schneider Electric InduSoft We... | 高 | 1089 | |

| 漏洞标题 | 危害级别 | 点击数 | 评论 | 关注 | 时间 |
|---|---|---|---|---|---|
| 多个Emerson产品安全绕过漏洞 | 中 | 508 | 0 | 0 | 2016-12-06 |
| Emerson DeltaV提权漏洞 | 高 | 458 | 0 | 0 | 2016-12-02 |
| 多个Emerson Process Management... | 中 | 905 | 0 | 0 | 2014-12-05 |
| Emerson DeltaV硬编码证书安全绕... | 低 | 900 | 0 | 0 | 2014-05-27 |
| Emerson DeltaV '\DeltaV'目录授... | 中 | 800 | 0 | 0 | 2014-05-27 |
| 多个Emerson Process Management... | 高 | 750 | 0 | 0 | 2013-09-29 |
| Emerson ROC800远程终端单元远程... | 高 | 755 | 0 | 0 | 2013-09-29 |
| 多个Emerson Process Management... | 高 | 772 | 0 | 0 | 2013-09-29 |
| 多个Emerson Process Management... | 高 | 762 | 0 | 0 | 2013-09-29 |

# 工控安全事件思考：工业协议风险

- 常用的工业协议有Modbus、S7、OPC、IEC104、DNP3、Profibus等，这些协议在设计初期主要是为了保证生产的连续性与稳定性，所以协议设计上在安全性与可用性之间进行取舍，进而牺牲了安全性。

**Modbus**

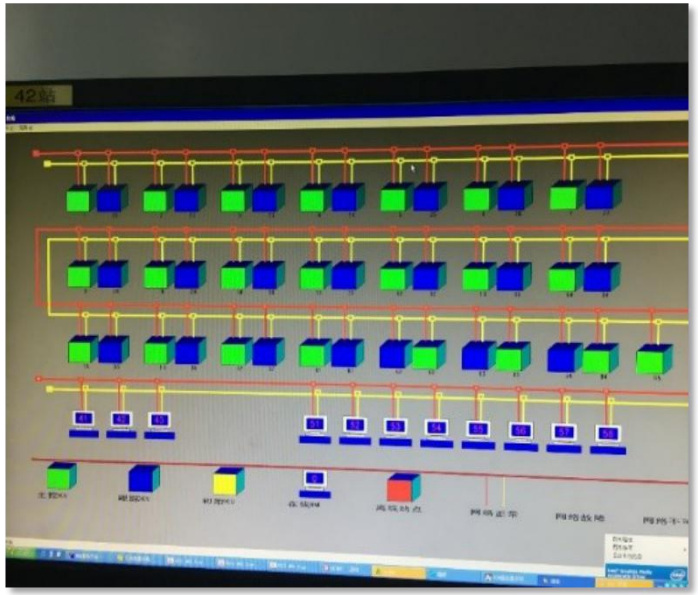
| 严重等级 | 威胁行为描述 | 潜在危害 |
|---|---|---|
| 高 | 主站下发08号功能码 | 可能导致设备进入Standby状态 |
| 高 | 主站下发90（5A）号功能码-stop（Schneider） | 导致PLC CPU进入STOP停机状态 |
| 高 | 主站下发90（5A）号功能码-download（Schneider） | PLC的内部程序可能正在被替换程 |
| 中 | 主站下发90（5A）号功能码-upload（Schneider） | 设备将工程上传至主站可能造成信息泄露 |
| 中 | 主站一次下发modbus报文超过260个字节 | 超出modbus tcp协议标准组包长度，可能导致设备拒绝服务 |
| 低 | 主站下发43（2B）号功能码 | 导致设备及其固件版本信息泄露 |

**西门子S7协议**

| 严重等级 | 威胁行为描述 | 潜在危害 |
|---|---|---|
| 高 | 主站下发STOP/RUN命令 | 导致设备进入停机状态/导致设备被启机初始化 |
| 高 | 主站下发download block命令 | PLC的内部程序可能正在被替换程 |
| 高 | 主站下发delet block命令 | PLC的内部程序块可能正在被删除 |
| 中 | 主站下发错误的密码请求 | 正在未授权访问 |
| 低 | 主站下发read szl请求 | 正在尝试获取设备模块信息、固件信息 |

# 工控安全事件思考：操作系统风险

- 工控主机、数控库服务器、应用服务器大量使用微软Windows系列操作系统，存在大量安全漏洞且很少打补丁，尤其是目前常用的老旧Windows系统，如Windows XP、Win2000、Win2003等，微软已经停止技术支持，面临无补丁可打的困境。

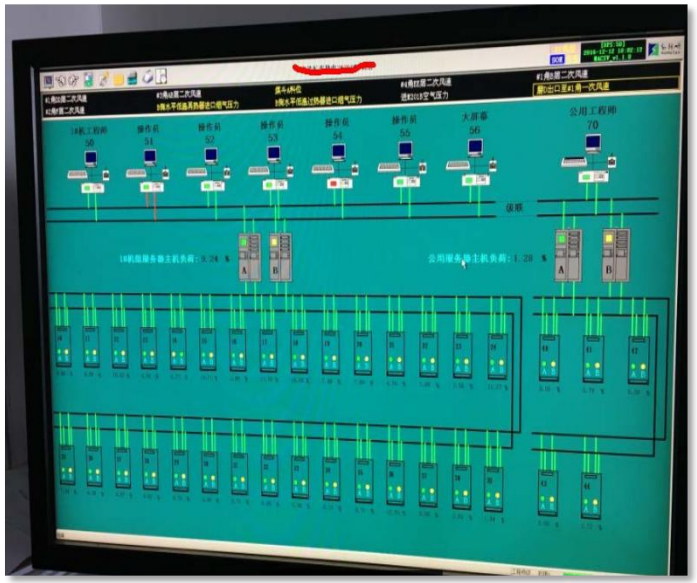


2014年4月8日，Windows XP将正式退役；也就是50天后，微软会正式放弃XP，不再提供包括自动更新等在内的技术帮助；但微软将继续积极提供更能满足现代用户需求的操作系统。

近日有这样一篇报道：《专家：WinXP停止服务后，电脑10分钟就出事》，微软中国对文章中“军用计算机专家及网络工程师Michael Menor观点”特别做出解释。据微软中国澄清，Michael Menor原意为：“如果你的电脑依然运行Windows XP，在没有安全补丁及服务更新提示的情况下，**它就有可能在10分钟内受到感染。**”

# 工控安全事件思考：应用软件风险

- 工业网络中使用的各种组态软件存在着大量的安全漏洞，如Sixnet、iFIX、SIMATIC、HollySys等，这些组态软件都已经曝出大量高危、中危等安全漏洞。这些控制软件的各类漏洞严重影响安全生产。任何黑客或别有用心人员都可以通过这些漏洞发起对工业控制系统有针对性的攻击行为。



## Sixnet Universal Protocol Undocumented函数代码远程安全绕过漏洞

报送者:北京天融信网络安全技术有限公司　★关注(0)

| | |
|---|---|
| CNVD-ID | CNVD-2013-12528 |
| 发布时间 | 2013-08-23 |
| 危害级别 | 高 (AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| 影响产品 | Sixnet RTU firmware < 4.8<br>Sixnet Sixnet UDR < 2.0 |
| BUGTRAQ ID | 61837 |
| CVE ID | CVE-2013-2802 |
| 漏洞描述 | 美国SIXNET公司是一家历史悠久的工业自动化和工业以太网产品生产厂商，自1976年起向世界各地用户提供高品质的控制系统和工业网络通讯产品。<br><br>Sixnet Universal Protocol存在远程安全绕过漏洞。攻击者可以利用漏洞绕过安全限制，获取文件描述和文件大小，读取或写入文件，创建新文件和执行任意代码。 |
| 漏洞类型 | 通用软硬件漏洞 |

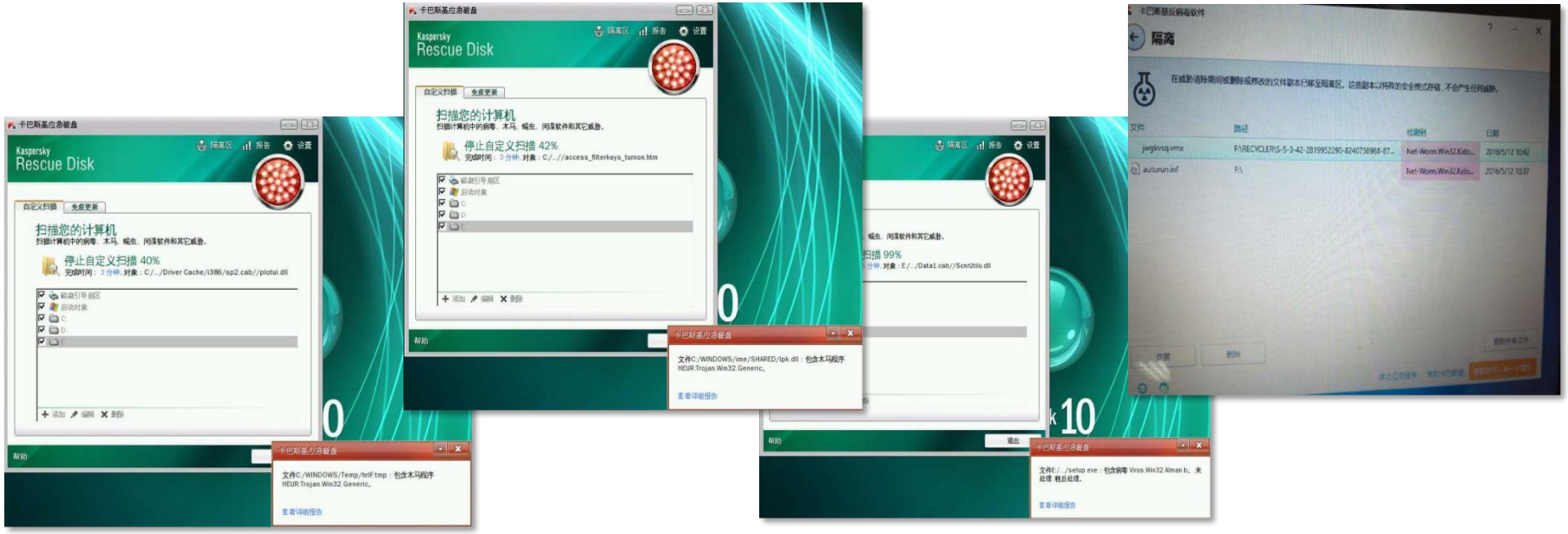
## GE Proficy HMI/SCADA-iFIX 'TCPTASK.exe'远程缓冲区溢出漏洞

报送者:北京神州绿盟科技有限公司　★关注(0)

| | |
|---|---|
| CNVD-ID | CNVD-2013-14823 |
| 发布时间 | 2013-12-03 |
| 危害级别 | 高 (AV:N/AC:L/Au:N/C:P/I:P/A:P) |
| 影响产品 | General Electric Company Proficy HMI/SCADA – iFIX 5.1<br>General Electric Company Proficy HMI/SCADA – iFIX 5.0<br>General Electric Company Proficy HMI/SCADA – iFIX 4.5 |
| BUGTRAQ ID | 63948 |
| 漏洞描述 | GE 智能平台的Proficy HMI/SCADA–iFIX 是世界领先的工业自动化软件解决方案，提供了生产操作的过程可视化、数据采集和数据监控。<br><br>GE Proficy HMI/SCADA-iFIX 4.5, 5.0, 5.1在TCP/IP任务进程(TCPTASK.exe)的实现上存在远程缓冲区溢出漏洞。成功利用后可使攻击者在受影响应用上下文中执行任意代码。 |
| 漏洞类型 | 通用软硬件漏洞 |

# 工控安全事件思考：病毒传播风险

- 经过大量的实际项目建设，大部分工业控制网络中工控主机、服务器发现了大量的病毒，这些病毒的存在已经影响到企业的正常生产。通过对这些病毒的入侵途径进行分析，发现这些病毒的传入途径多为移动存储介质的滥用造成的。



# 工控安全事件思考：安全防护

## 物理和环境安全：

门禁、指纹

环境、温湿度监测

火灾、烟雾报警

视频监控

设备及备件存储

## 工控主机：

病毒防护

接口授权管理

安全操作审计

密码简单、易攻破、无

密码管理

## 工控生产网络安全：

各个生产区域之间边界

网络病毒防护

安全监测与审计

# 工控安全事件思考：安全管理及安全意识

## 安全管理制度：

工控安全管理机构

工控安全管理制度

工控安全人员管理、资料管理

## 安全运维：

人员队伍建设

思想意识建设

关键软、硬件识别、验证

第三方工控安全建设

## 参考标准：

GB/T 50609-2010 《石油化工工厂信息系统设计规范》

GB/T 30976.1-2014《工业控制系统信息安全 第1部分:评估规范》等

## 工控安全

1. 等级测评，风险评估，渗透测试；
2. 解决顶层设计问题；
3. 解决投入不足问题；
4. 安全建设落地；
5. 广泛参与及积极建设；
6. 持续改进、安全认证及人员培养；

# 工控安全总体策略

01

- 着眼全局，注重细节
  - ✓ 关注工业控制系统整体安全，重点对关键部位进行有效的威胁感知和防御能力部署

02

- 立足现实，放眼未来
  - ✓ 评估掌握工控安全现状，基于数据分析进行前瞻性安全防护体系建设

03

- 统筹安排，全面覆盖
  - ✓ 安全体系要覆盖公司所有企业及方案设计服务商、关键组件供应商、系统运营和维护的服务商

04

- 顶层规划，感知全局
  - ✓ 形成以公司总部为核心的工控安全全局态势感知技术体系，掌握公司工控安全现况及趋势

# 工控信息安全总体目标

# 工控信息安全总体规划

# 口 方案依据

文件：
《工业控制系统信息安全防护指南》
《关于开展2016年工业控制系统网络与信息安全检查工作的通知》
标准：

① GB/T33007-2016 《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》

② GB/T33008.1-2016 《工业自动化和控制系统网络安全 可编程序控制器(PLC)》

③ GB/T33009.1-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第1部分：防护要求》

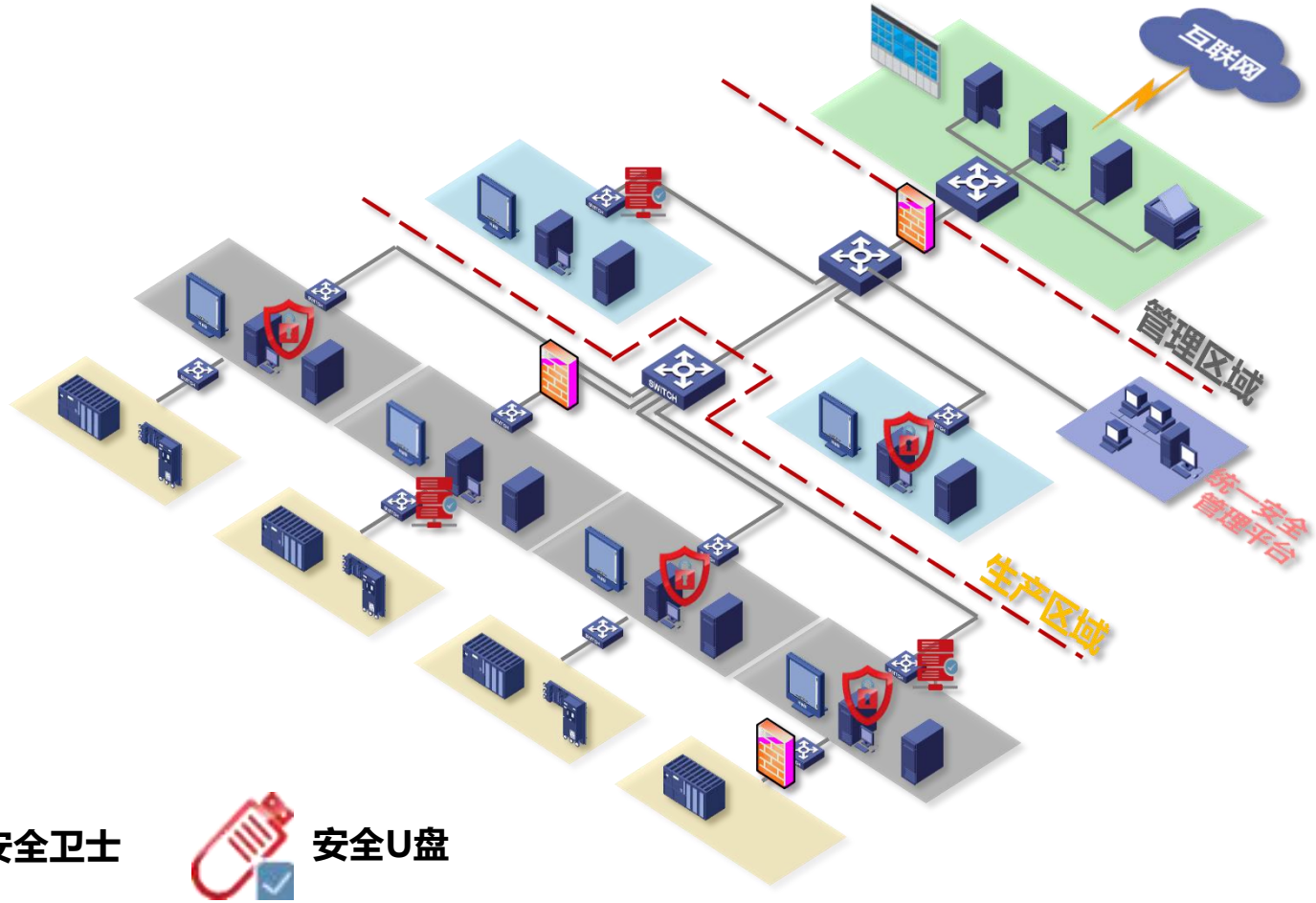
④ GB/T33009.2-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第2部分：管理要求》

⑤ GB/T33009.3-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第3部分：评估指南》

⑥ GB/T33009.4-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第4部分：风险与脆弱性检测要求》

# 防控威胁-工控信息安全策略

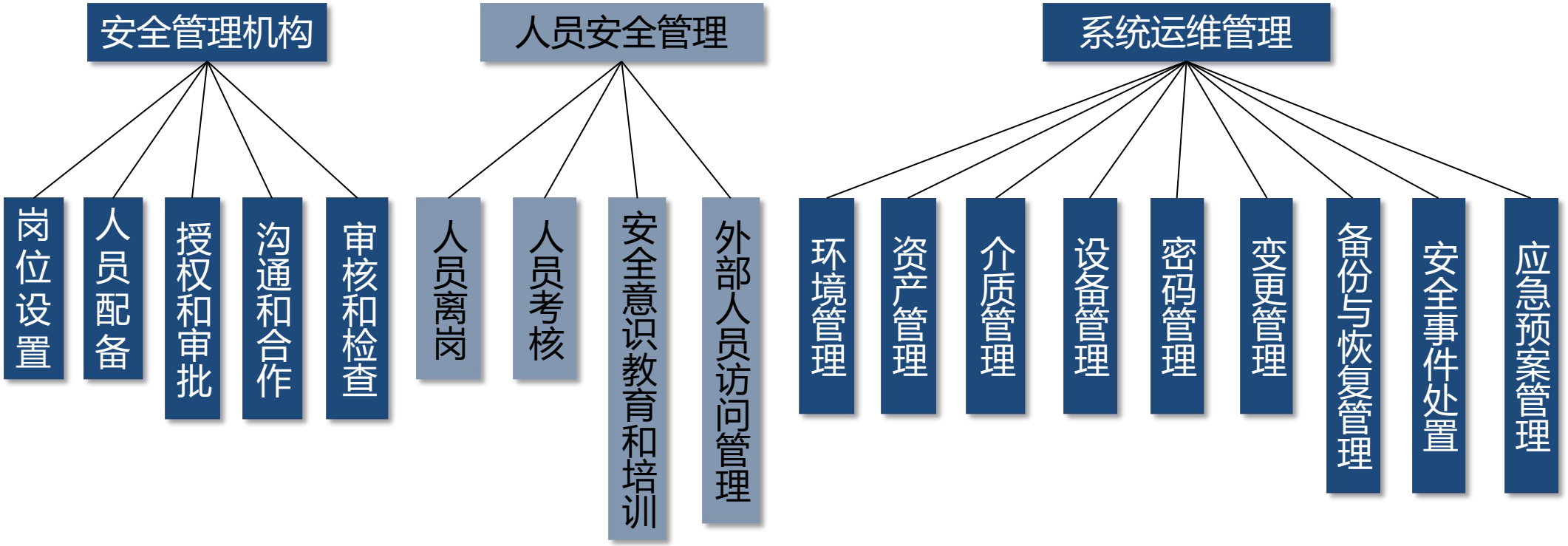
- 由“黑” 到“白”
- 由“被动” 到“主动”
- 由“大区域” 到“小区域”
- 由“粗狂” 到“精准”
- 由“分散” 到“集中”




工业防火墙　监测与审计　工业安全卫士　安全U盘

## 管理先行-安全管理制度

建立完善规章制度、管理办法，对移动介质使用、系统口令、第三方及远程运维、控制操作规程等进行严格管理与要求。

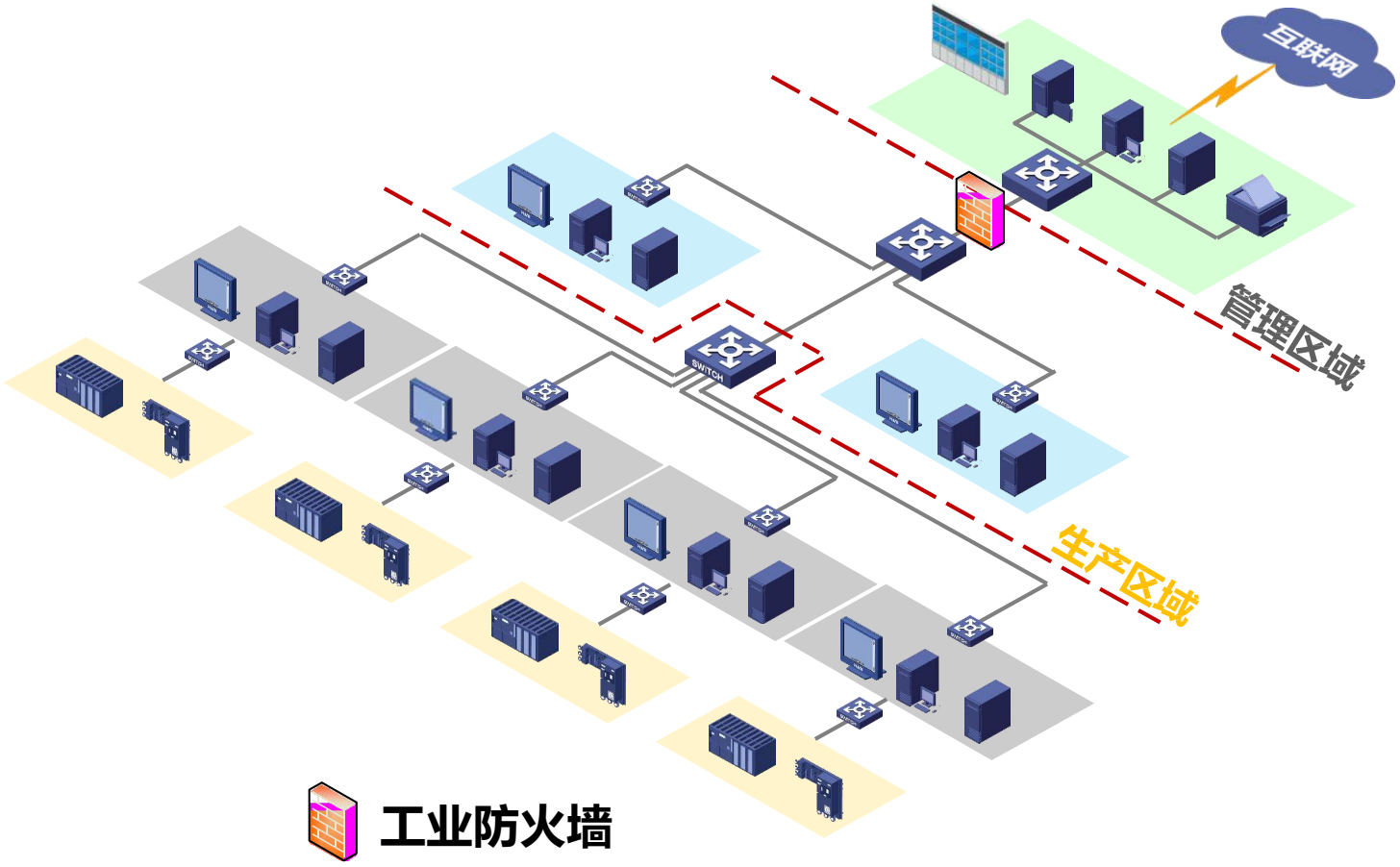


## 技术并重-建设内容

实施有效的技术手段，部署隔离、防护设施设备，总体有以下几方面：

1、边界防护：依据《工业控制系统信息安全防护指南》第三条第2项：通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。

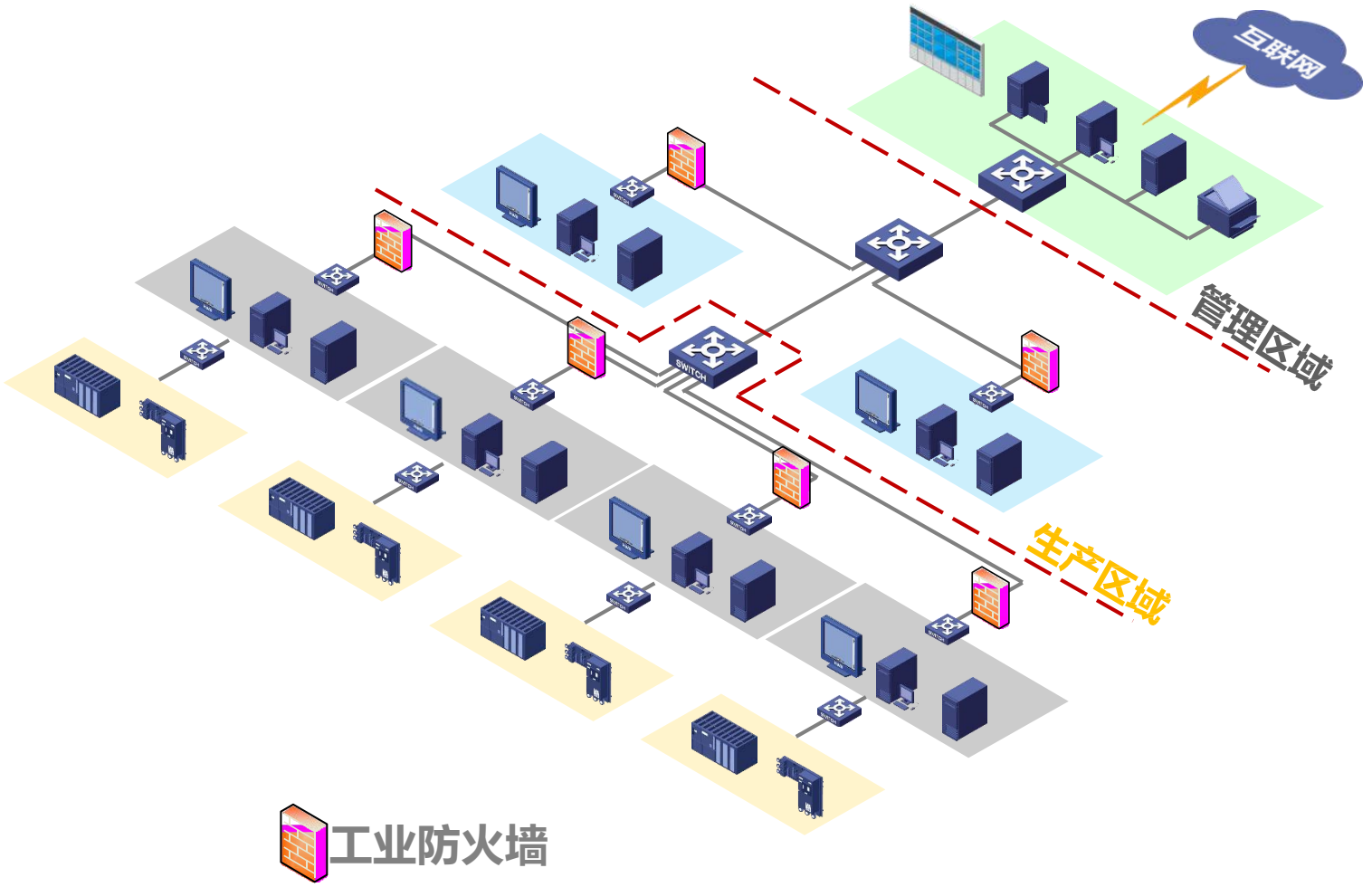
**防护措施：在生产网网络边界部署工控防火墙。**



## 口 技术并重-建设内容

2、区域隔离防护（工业防火墙）：依据《工业控制系统信息安全防护指南》第三条第3项：通过工业防火墙等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。

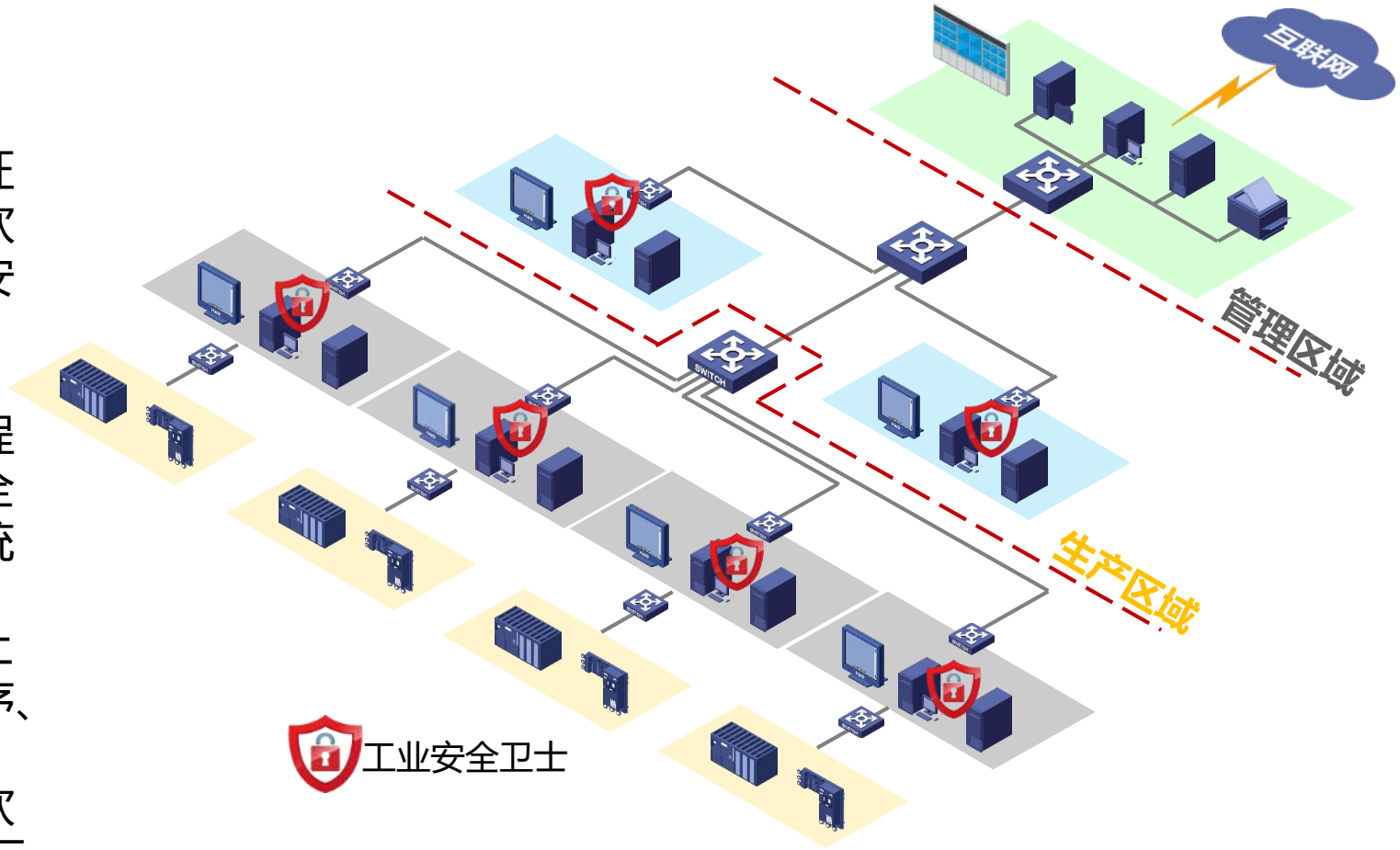
**防护措施：**在生产网出口、各子系统网络边界部署工业防火墙，实现各子系统之间区域隔离，防止病毒、木马等在网络中蔓延。



## 技术并重-建设内容

3、主机防护：依据《工业控制系统信息安全防护指南》第一条第1项：在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。

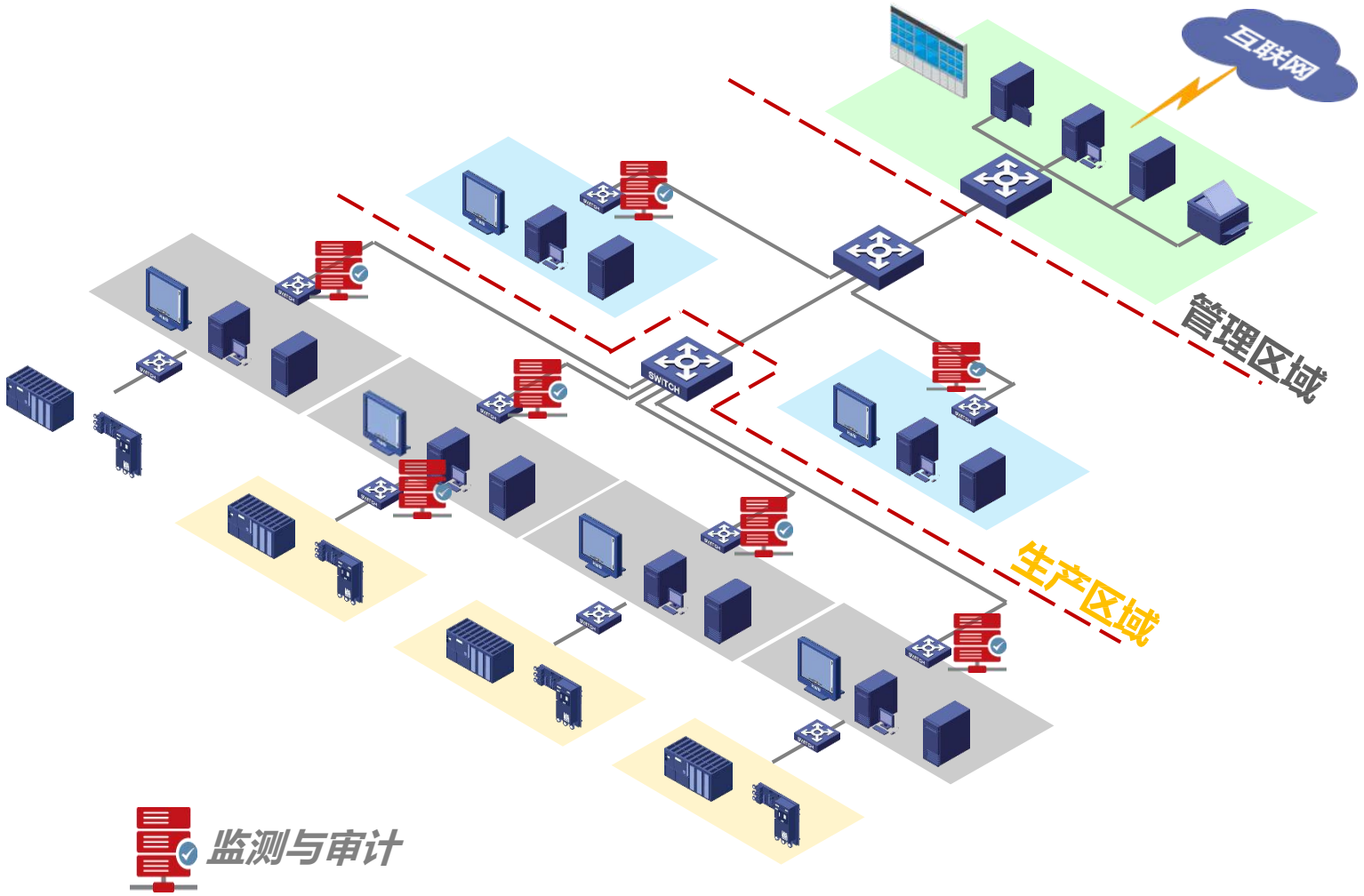
**防护措施：**在生产网中的服务器、工程师站、操作师站等主机上安装工控安全卫士等，监控进程运行，保护工业系统中的主机，通过对应用程序、网络、USB移动存储等实施白名单策略，防止用户违规操作、误操作，防止不明程序、移动存储介质或网络接入的不法使用，避免内部人员未授权安装软件、运行软件， 阻止病毒及恶意代码等的安装、运行以避免受到攻击。



## 运维审计是重点-建设内容

4、监控与审计：依据《工业控制系统信息安全防护指南》第七条第1项：在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。

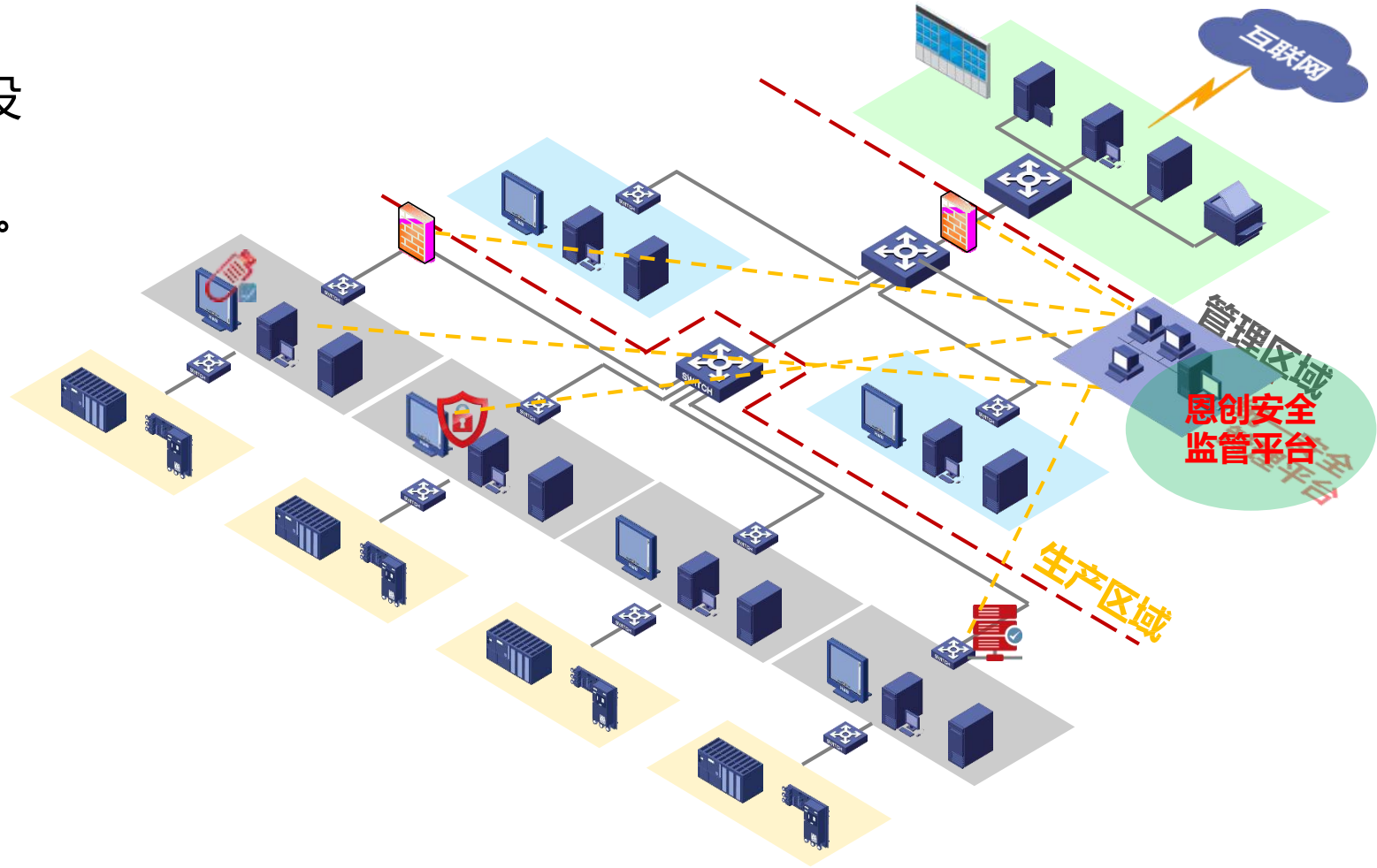
**防护措施**：在主干网核心交换机上旁路部署安全审计平台，对工控网络中的数据进行实时监测、实时告警，帮助用户实时掌握工控网络运行状况，并对网络中存在的所有活动提取行为审计、内容审计、协议审计，生成完整的记录便于时间追溯，还可以对网络中未知设备的接入进行实时监测、告警、记录，迅速发现工控网络中存在的非法接入。



## ■ 提升运维质量-建设内容

5、统一安全管理：针对工控安全设备进行统一的安全可视化管理，为安全运维管理提供有力的技术支撑。

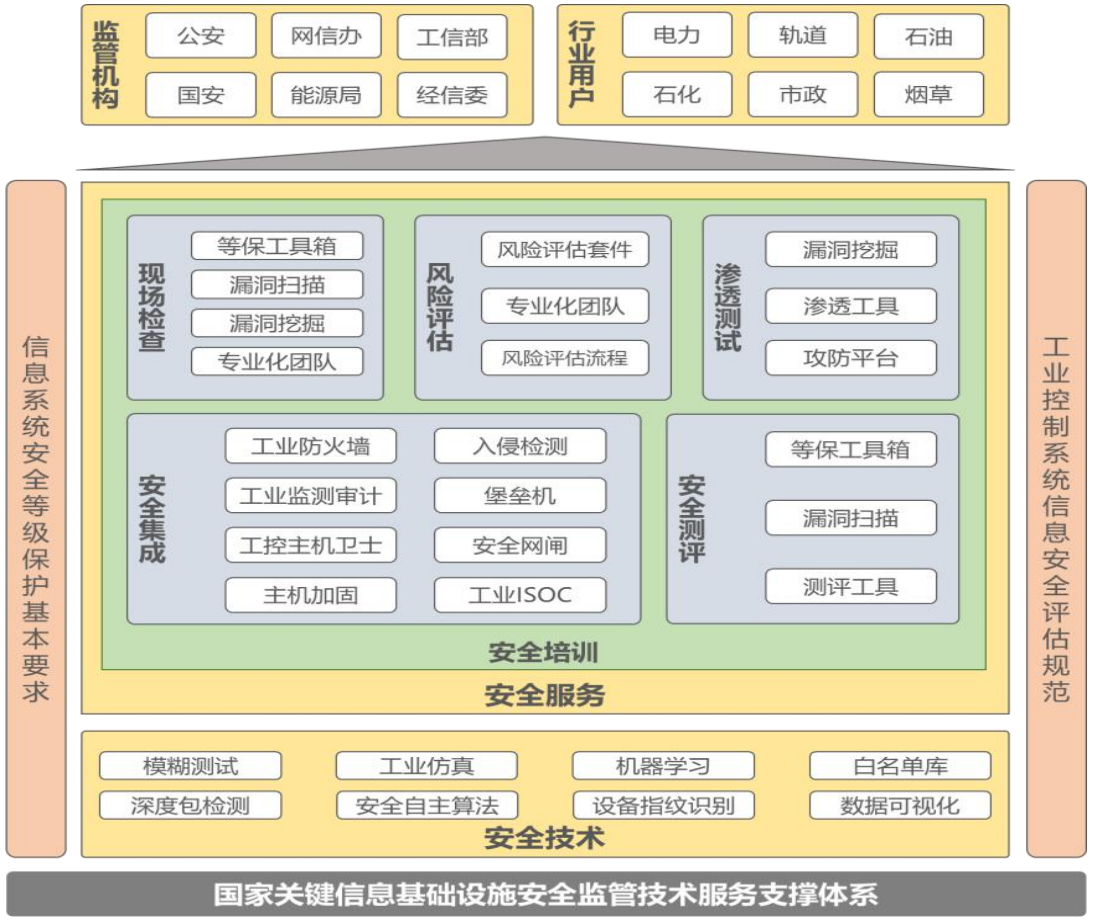
**措施：**在新机房网络数据中心部署统一安全管理平台，可以对工业控制生产网中部署的工控安全设备和系统进行管理、配置和运维，实现对工业控制全网中每个节点的安全设备进行策略配置下发、网络流量分析，实时掌握工业控制网络运行情况，以便出现问题时及时定位发生位置和原因。



## ■ 检查评估是保障-建设内容

6、2017年6月1日起《中华人民共和国网络安全法》正式施行，其中
**第三十八条** 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险**每年至少进行一次检测评估**，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

从健全统一的工控信息安全策略体系、工控安全组织管理体系、工控安全技术和工控运行体系，有效的工控安全监管体系、工控安全防护体系、工控安全运维体系几个层面进行，发现安全问题。



# 恩创工业信息安全产品线


- 态势感知系统
- 漏洞扫描系统
- 恩创工业防火墙
- 工业安全卫士
- 监测与审计平台

# 恩创工业防火墙

## 产品定位

- 保护控制网与管理信息网的边界
- 阻止来自管理信息网的威胁
- 防止安全域内的攻击扩散


1. 仅放开OPC动态端口
2. 工业协议(如OPC)深度白名单
3. 工业协议(如OPC)的只读控制
4. 白名单智能学习

## 产品特点

- 自主产权千兆工业防火墙
- 工业协议深度解析/数采只读控制
- 低延迟 <50us

5. 状态检测防火墙
6. 静态路由与动态路由(OSPF)
7. 违规报警及报告(支持短信)
8. 统一安全管理平台

# 恩创工业安全卫士


1. 应用白名单
2. 实时报警
3. 智能学习
4. 自身保护
5. 安全U盘
6. 观察模式
7. 日志审计

- 利用“白名单”技术保护工控系统主机安全的加固软件。保证只有经过认证的“白名单”软件才可以运行，其他病毒、木马、违规软件都被阻止。

# 工控安全监测与审计平台

- **产品定位**
  - 监控并记录工控系统运行过程中的一切操作行为
  - 为事故追溯、责任划分提供证据
- **产品特点**
  - 对工控网络“零影响”
  - 忠实记录网络一切动态
  - “白名单”思想，无需升级

1 **网络异常检测**
忠实记录工控协议通信记录，自学习建立正常通信行为基线模型，对偏离基线异常操作行为进行告警上报；

2 **网络攻击检测**
识别并检测工控协议攻击、TCP/IP攻击、网络风暴、参数阈值检测

3 **关键事件检测**
例对工程师站组态变更、操控指令变更、PLC程序下装以及负载变更等关键事件告警

4 **工业网络可视化**
提供多维度网络流量视图，统计视图

# 恩创统一安全监管平台


## □ 统一监管：

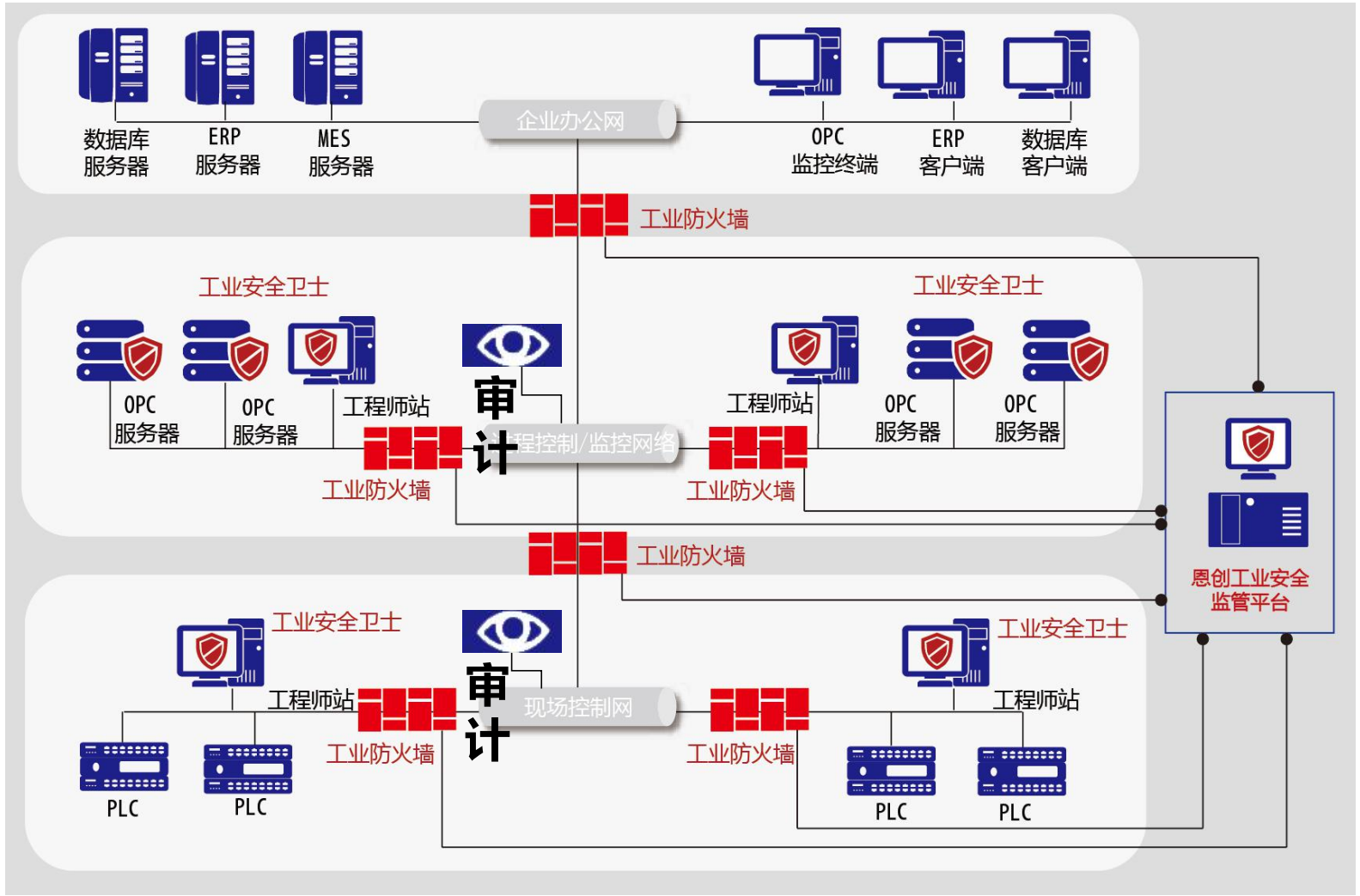
**工业防火墙**

**主机防护软件**

**监测审计平台**

**统一预警**

**统一分析**




- 安全软件选择与管理

应用程序“**白名单**”

- 边界安全防护

网络边界“**工业防火墙**”

- 安全监测和应急预案演练

**“工业协议深度包检测功能的防护设备”**

AVCOMM 恩创
INDUSTRIAL IT

# 交流结束-请领导指正

安通恩创信息技术（北京）有限公司