



— 华谊集团 — 工业控制系统网络 安全培训

制造和数字化中心
2010年10月26日

目录

Contents

01

工控网络安全问题的由来

02

解决方案

03

集团工控网络安全加固标准解读



01 工控网络安全问题的由来

● 工业智能化趋势



工业智能化背景下，网络安全已经成为功能安全和数据安全的核心元素



功能安全包含网络安全



数据安全依赖网络安全

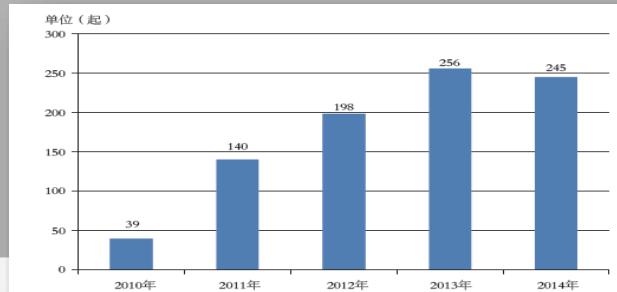
- 工控设备、物联网设备成为被攻击的重要目标

暴露在外的物联网设备与系统

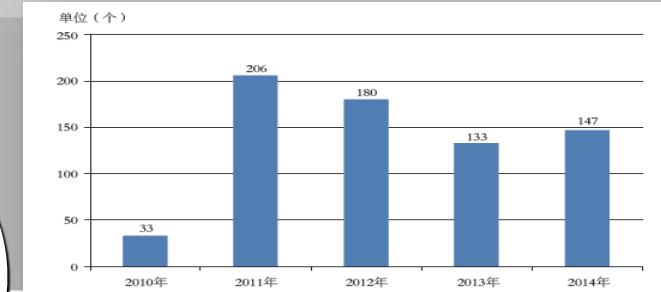


网络安全

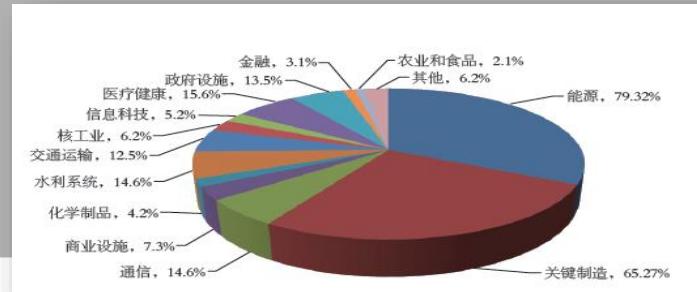
日益增多的工控网络攻击事件



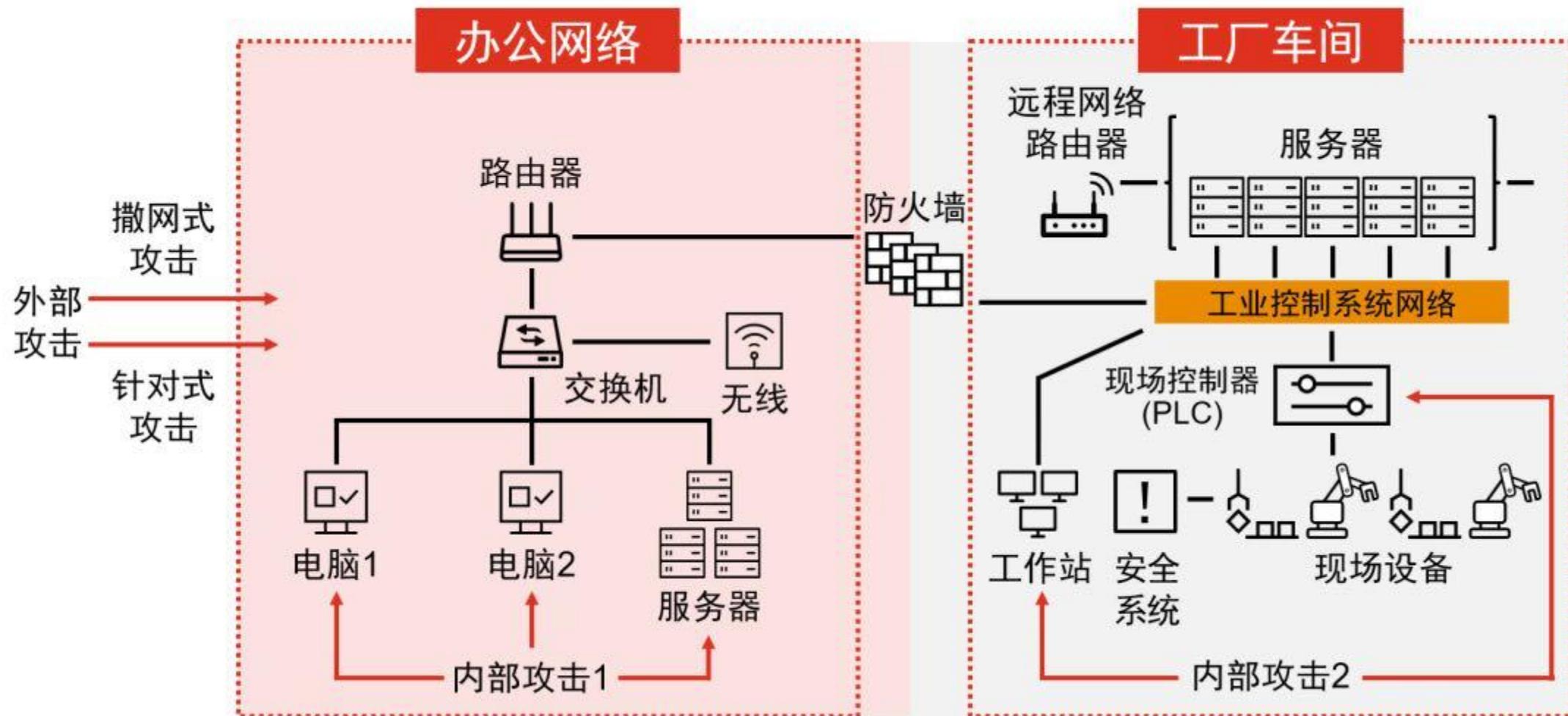
始终处于高位的高危漏洞收录



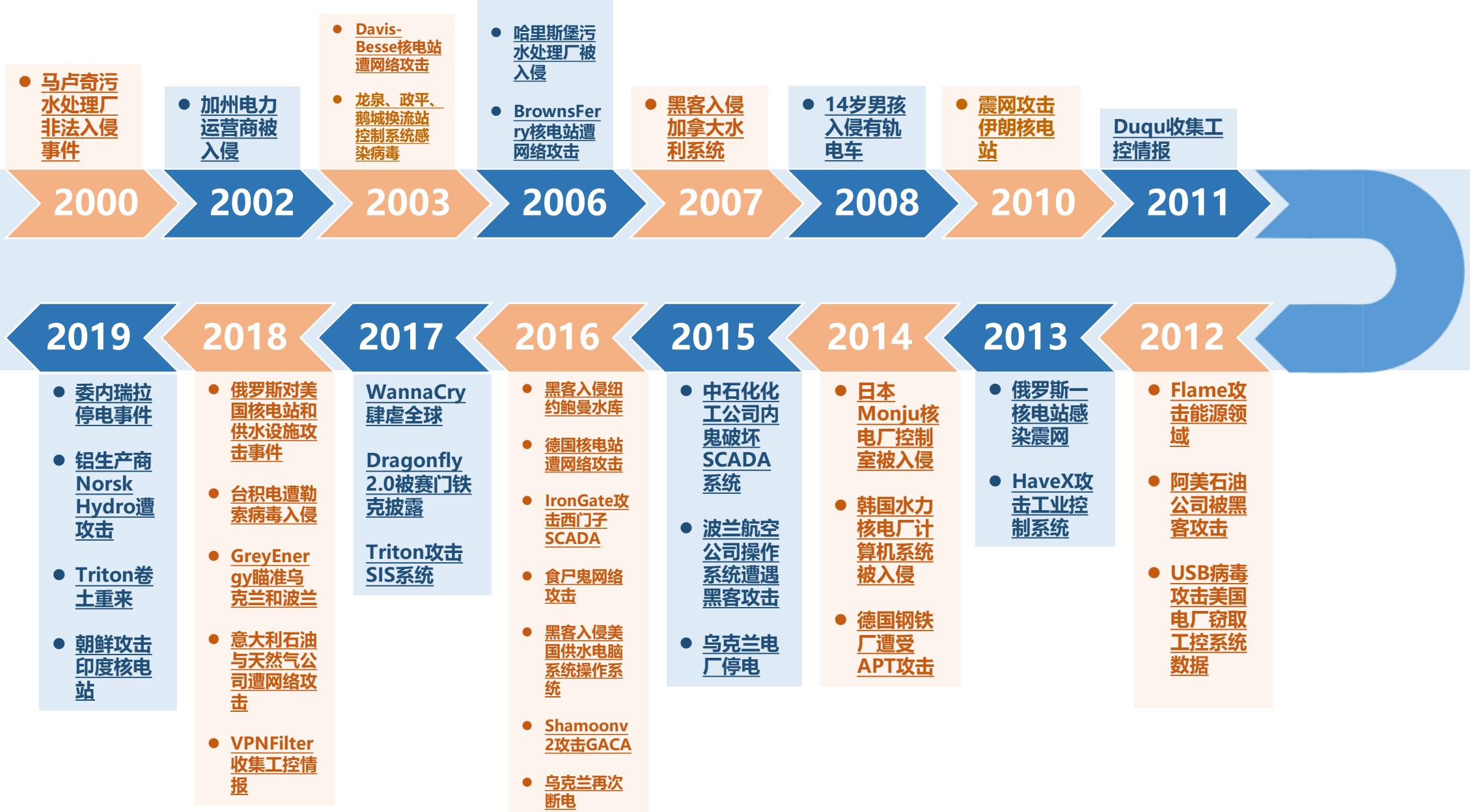
成为主要被攻击对象的重点行业 (能源、关键制造行业等)



- 办公网和生产网双向流动共享后，威胁交织渗透



● 工业控制系统安全危及国家安全



● 工业控制系统安全危及国家安全

黑客远程入侵智能汽车，
汽车也可能随时“遭遇
“恐怖袭击”



智能移动



冶金

德国钢厂熔炉控制系统受攻
击，导致熔炉无法正常关闭

电厂遭USB病
毒攻击，大量
机密数据泄漏



智能电网



智能制造

数控机床关键数
据被窃取，损失
难以估量

污水处理厂遭非法
入侵，污水直接排
入自然水系



水处理



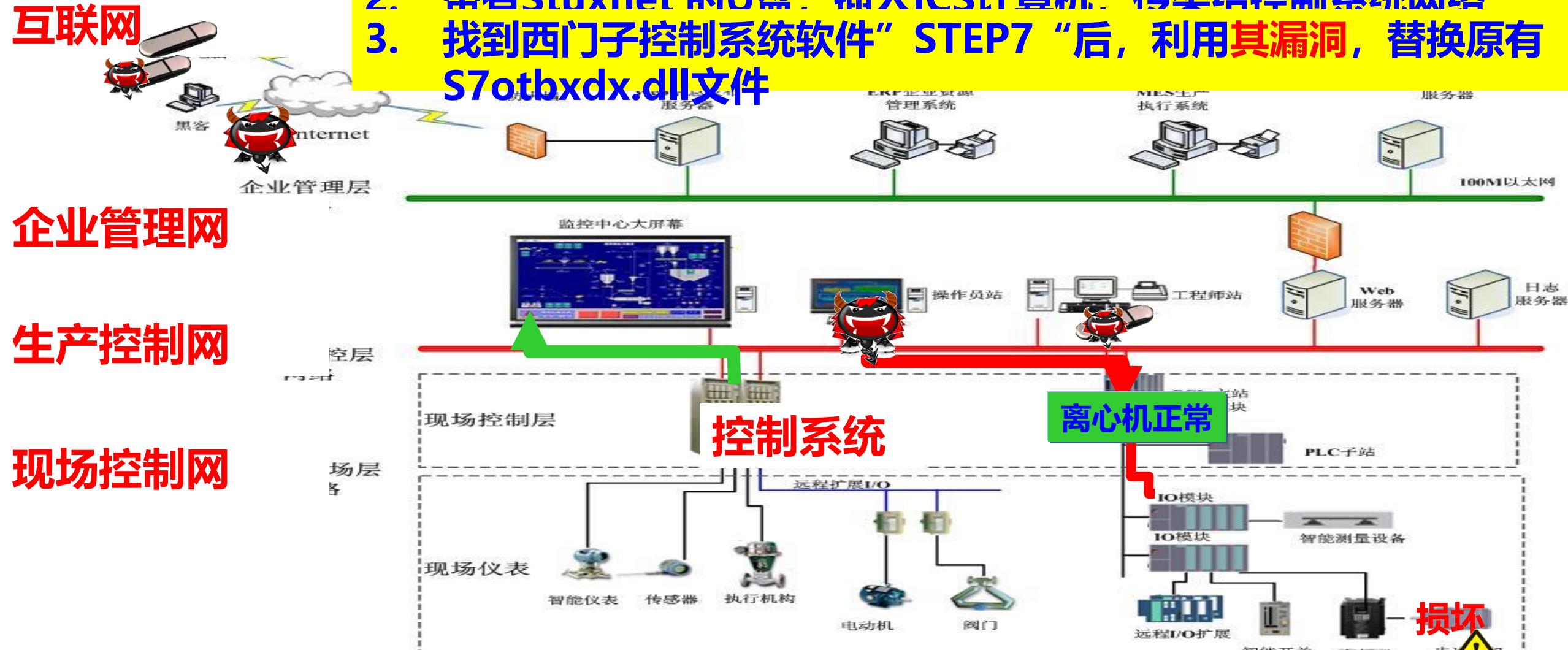
卫生事业

黑客入侵药泵，输出
致命剂量，危害人身
安全



军事

● 震网病毒事件攻击途径



1. Stuxnet 散布到互联网，感染计算机和U盘
2. 带有Stuxnet 的U盘，插入ICS计算机，传染给控制系统网络
3. 找到西门子控制系统软件“STEP7”后，利用其漏洞，替换原有 S7otbwdx.dll文件
4. 借助WinCC软件，向西门子控制器PLC注入恶意控制程序DB890
5. PLC向离心机发送恶意控制指令，使其超速；向控制室发送欺骗性的“正常”数据

● WannaCry勒索病毒大规模攻击制造业

■ WannaCry蠕虫

- WannaCry，一种“蠕虫式”的勒索病毒软件，大小3.3MB，由不法分子利用此前披露的Windows SMB服务漏洞（MS17-010）攻击手段，向终端用户进行渗透传播。
- 该恶意软件会扫描电脑上的TCP 445端口（SMB），以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。勒索金额为300至600美元。
- 2017年4月14日，黑客组织Shadow Brokers公布的Equation Group（方程式组织，隶属于美国国家安全局）使用的“网络军火”中包含了该漏洞的利用程序。



一旦程序加密，将直接造成生产基地停产，而且很难解密

- 勒索病毒打破了传统的工业安全认知

“永恒之蓝”勒索蠕虫

国内外工业企业成为勒索攻击的重灾区

- 法国雷诺汽车受勒索病毒入侵，多个工厂被迫停工
- 日产汽车桑德兰工厂IT系统受到感染，被迫停产
- 西班牙电信公司大量电脑受到感染，造成业务瘫痪
- 德国汉堡火车站系统被攻击，陷入瘫痪

.....



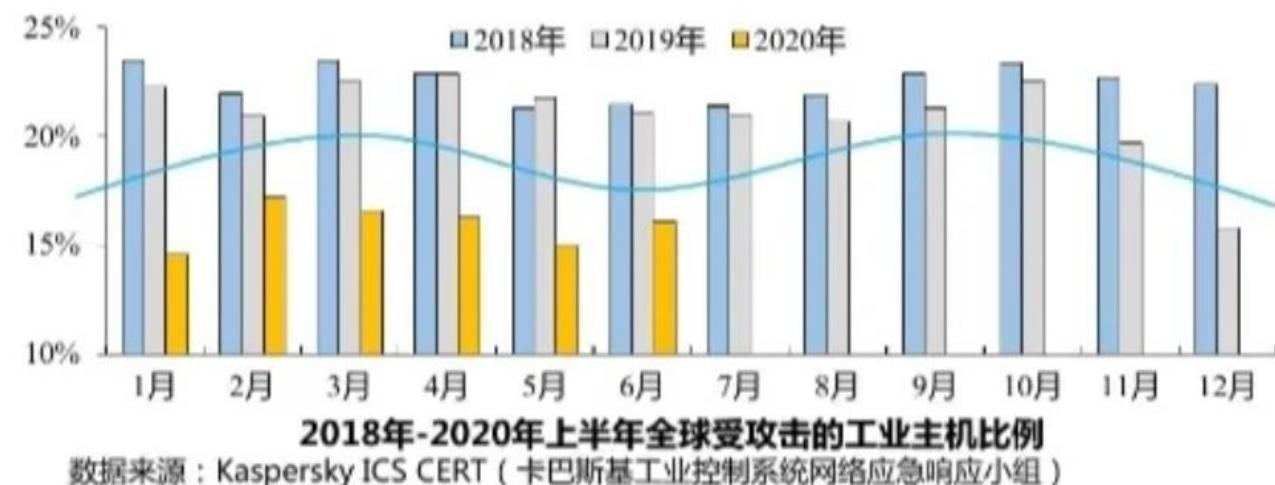
台积电遭勒索攻击

- 2018年8月，全球最大的半导体制造商台积电遭到了勒索病毒攻击，**几小时内台湾工厂生产线全数停产**。
- 此次病毒疑似去年全球爆发的“永恒之蓝”勒索病毒变种，在安装新机台时带入，**造成台积电三季度损失1.7亿美元**。



● 工控安全趋势

CNVD2018年收录工业控制系统安全漏洞数量



数据来源：Kaspersky ICS CERT (卡巴斯基工业控制系统网络应急响应小组)



- 自2009年以来网络攻击增长20倍
- 能源、制造、商业设施、水务、市政等重点领域漏洞占比达到50%
- 我国受安全问题困扰的工业主机比例是全球比例的两倍。

安全趋势已经形成，安全加固迫在眉睫

工业互联网安全常见安全隐患点

互联网暴露

分区隔离

双网卡问题

漏洞补丁

安全软件

口令管理

U盘管控

远程维修

外包商/供应商

.....

2017.5.12永恒之蓝勒索蠕虫事件



99国受灾，国内已知超过5万设备感染，实际总感染量至少20万，企业、机构是主要陷落区

- 一机双网缺乏有效管理
- 缺陷设备被带出办公区
- 协同办公网络未全隔离
- 防火墙未关闭445端口
- 办公网与生产网未隔离
- 外网设备分散无人管理

安全意识问题是
WannaCry
穿透内网的主要原因

某知名汽车制造企业遭勒索病毒攻击

现场回顾

- 2018年7月，某知名汽车零部件生产企业工业生产网络遭受“永恒之蓝”勒索病毒的攻击
- 酸轧生产线一台Windows服务器主机出现**蓝屏、重启现象**。当日晚上，**4台服务器出现重启**
- 现场工程师对病毒进行了手动处理
- 9月10日，除重卷、连退生产线外，其他酸轧、包装、镀锌生产线全部出现蓝屏/重启现象
- 此时，病毒已对正常生产造成严重影响



KERNEL_MODE_EXCEPTION_NOT_HANDLED

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use safe mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical Information:

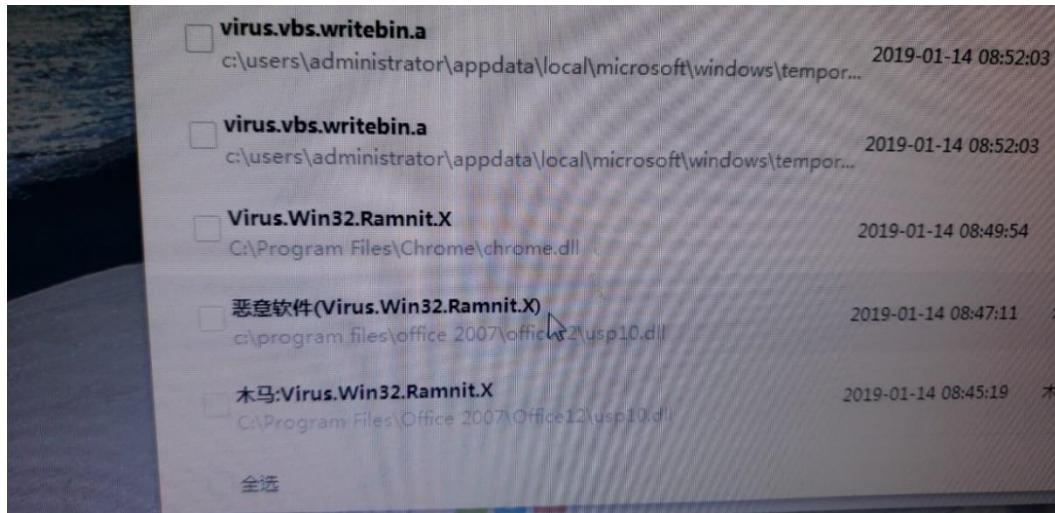
问题研判

- 各条产线互通互联，无明显边界和隔离
- 生产线为了远程维护方便，分别开通了3个运营商ADSL拨号，控制网络中的主机在无安全措施下访问外网
- 控制网中提供网线接入，工程师可随意使用自己的便携机接入网络
- U盘随意插拔，无制度及管控措施

员工使用ghost导致共享设备被感染

现场回顾

- 2019年1月，某地交通运输管理机构及下属公司发生频繁报毒事件
- 一台共享打印机的电脑频繁报毒，无法清理干净
- 报毒总是发生在两名员工打印Word文档时

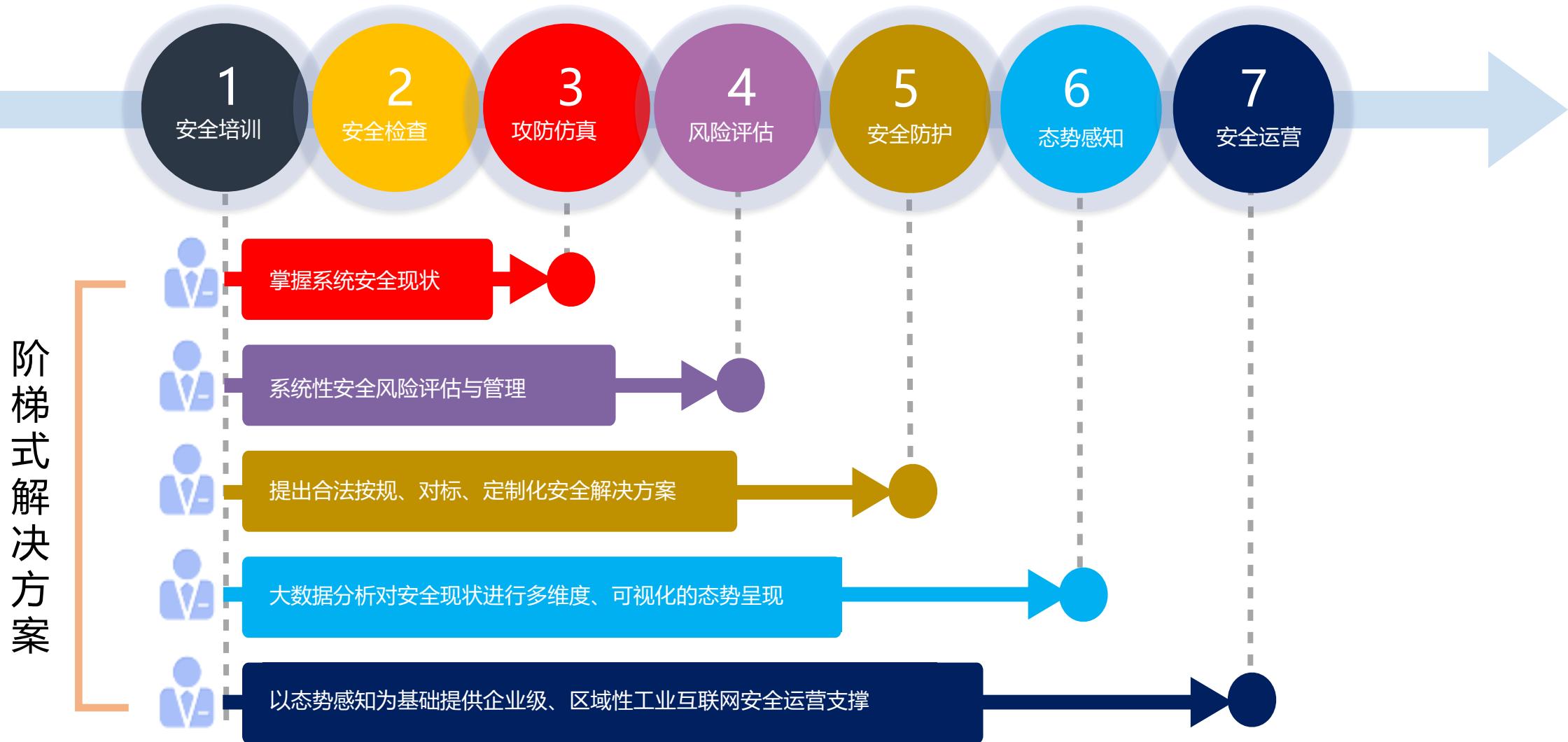


问题诊断

- 经调查，两名员工均**擅自安装**了一个网络来源的**Ghost**版本**Windows**
- 该**Ghost**版本有毒
- 员工擅自安装的原因是：**设备老旧**，无法安装新版**Windows**

02 解决方案

● 阶梯式安全解决方案



● 安全检查-工控网络安全检查



- 对标核查
- 设备扫描



- 流量侦听
- 网络探查



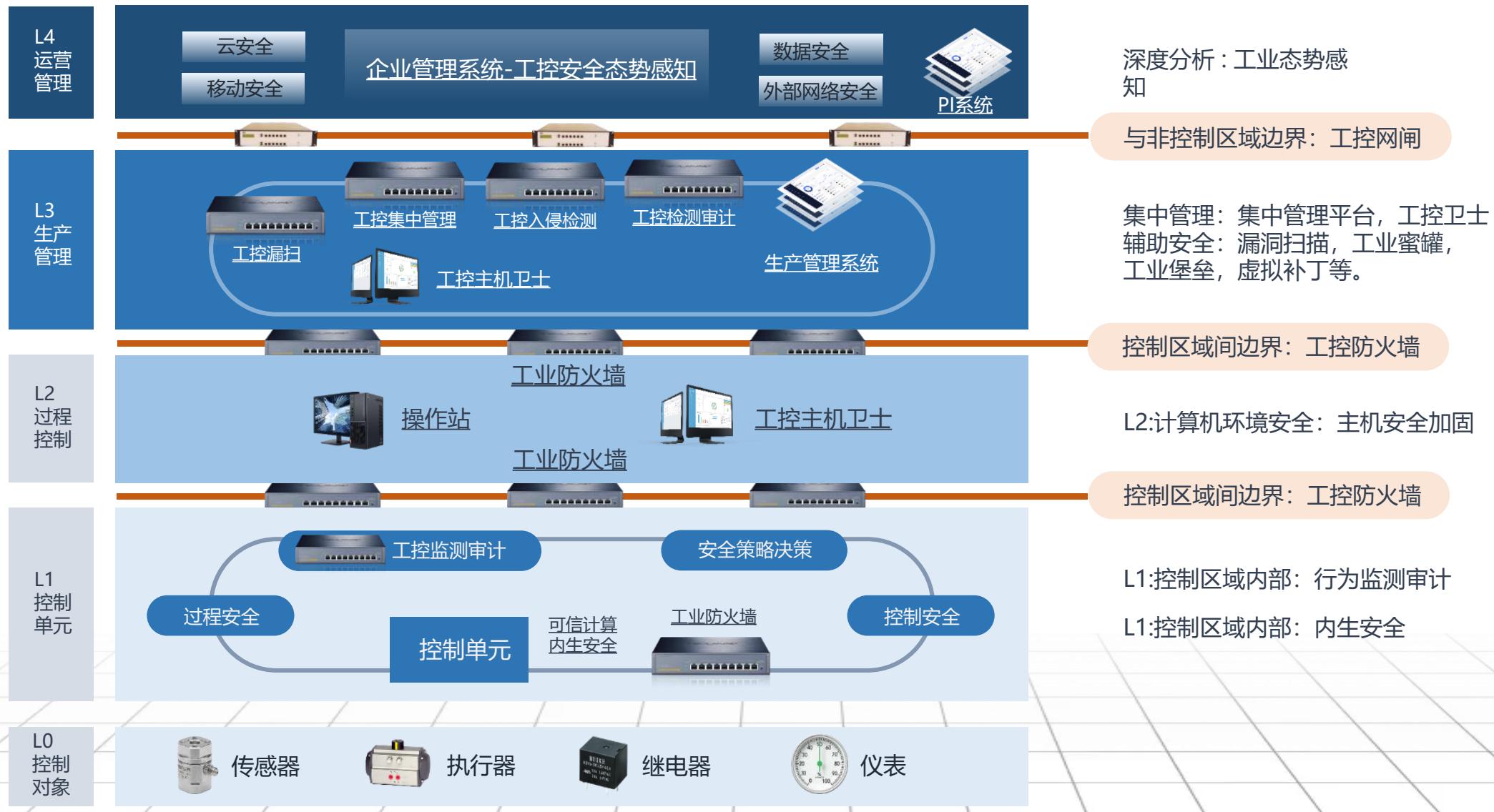
- 现场调研
- 风险评估

- 安全监测
- 态势感知

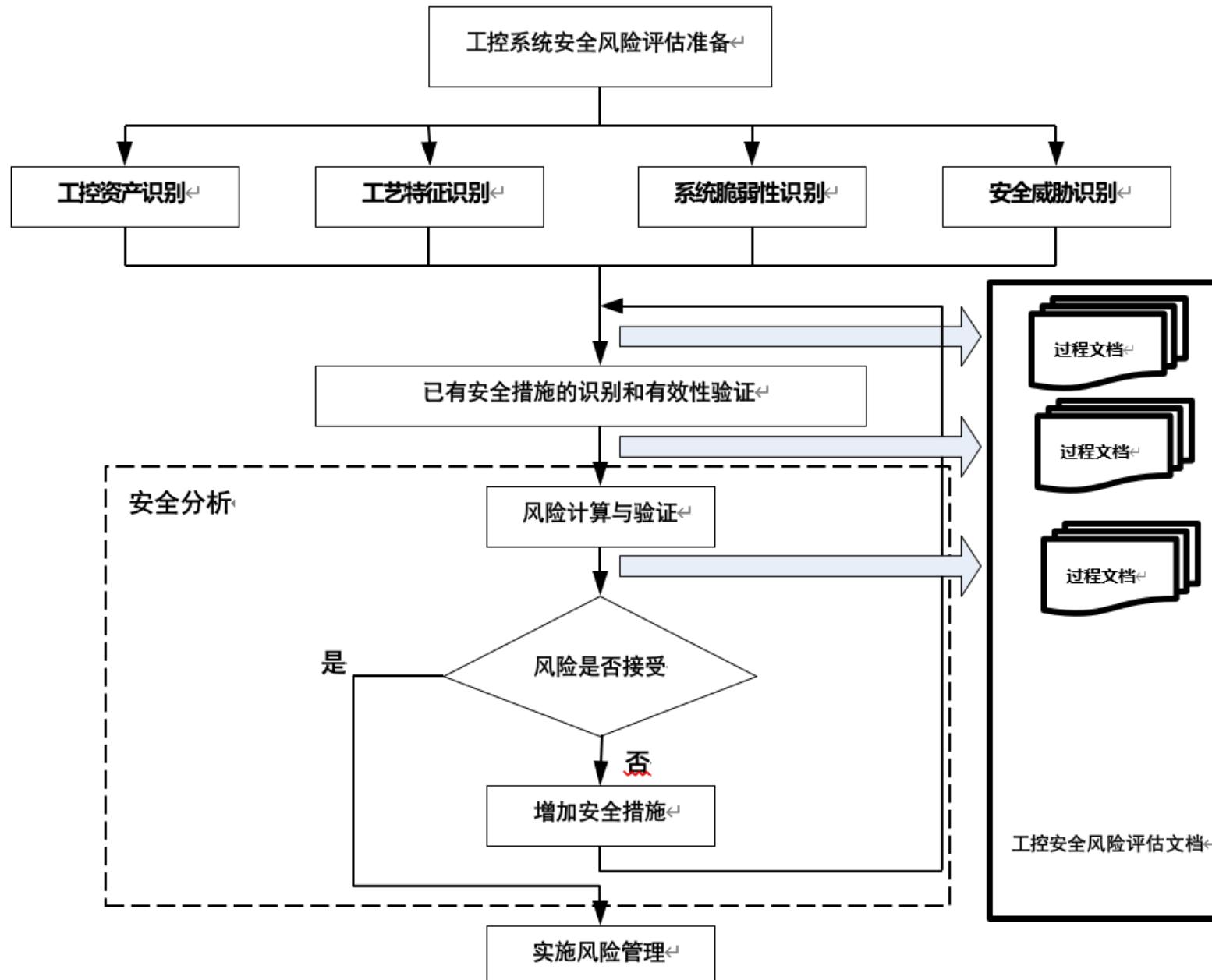


有标准可依、有工具可查、有手段可用、有结论可报

工业互联网安全防护技术框架



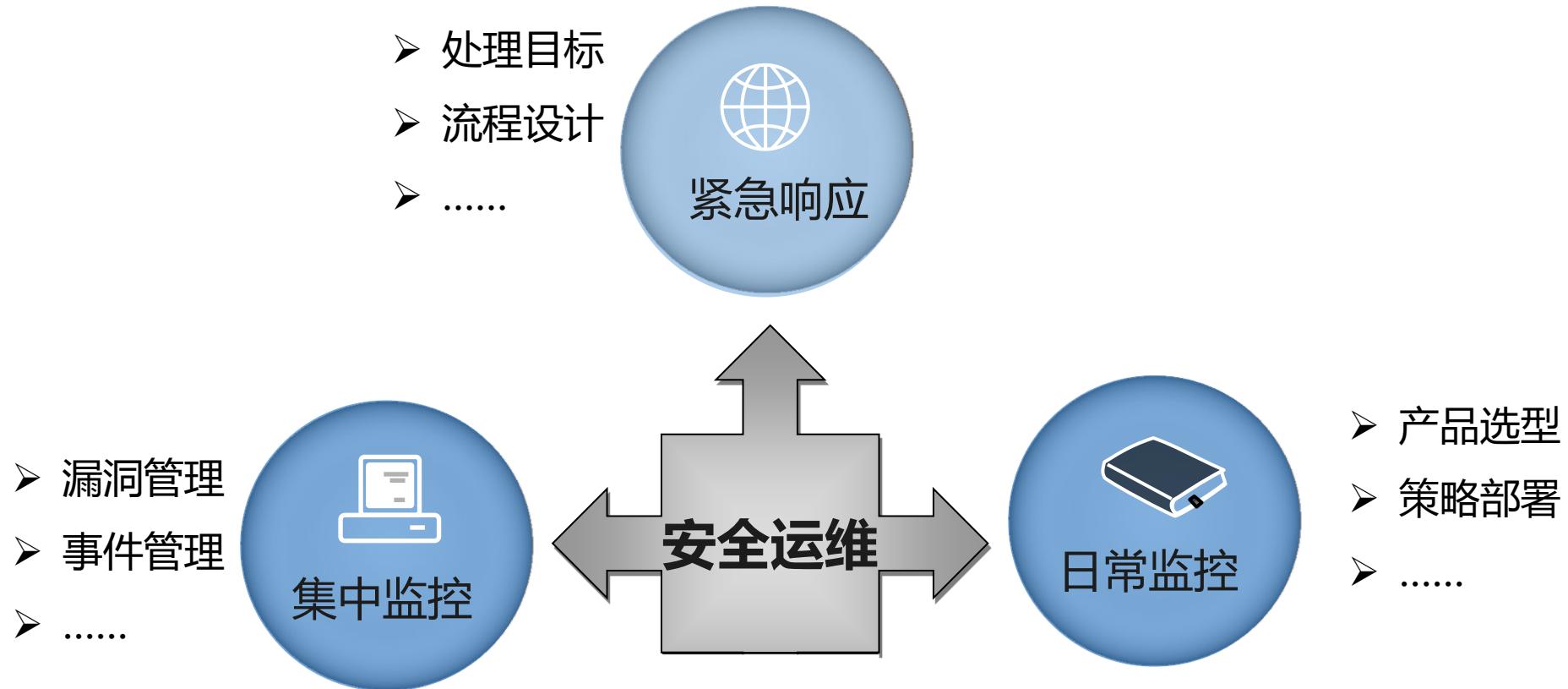
● 工控安全风险评估



● 安全技术与安全管理建设

技术防护		安全管理
(1) 物理环境安全	物理安全和制度体系建设	安全制度建立
(2) 安全策略与流程		
(3) 安全层域划分	区域隔离和控制	异常流量和行为分析
(4) 部署安全防护方案	漏洞安全管理	风险分析和威胁评估
(5) 系统安全加固	工控安全监控审计	工控安全入侵防护
(6) 应用安全管理		人员组织、制度体系、安全建设
(7) 终端安全加固	应用数据安全加固	终端安全白名单环境
(8) 持续性风险管理	威胁态势感知、安全运营	应急响应、风险处置、应急演练

● 安全运维体系



日常监控

维护安全基线

- 定期的安全审计
- 定期的安全威胁分析
- 资产的安全基线检查
-

定期安全审计

- 网络安全设备审计
- 日志审计
- 系统审计
- 主机安全审计
-

定期安全检查

- 网络设备
- 操作系统
- 应用服务
- 业务软件
-

安全监控/管理中心

建立以管理者和资产为核心的管理体系

将所有的安全产品和事件通过统一的界面联系起来

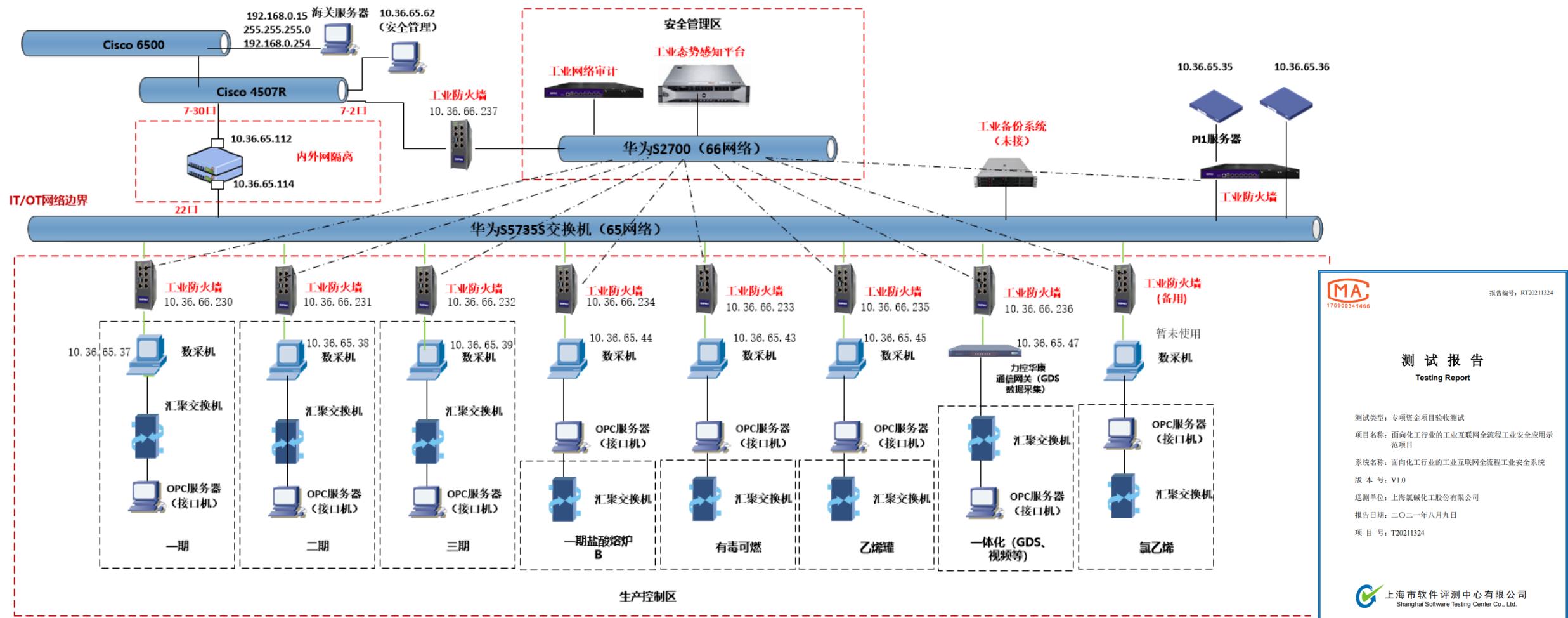
提供智能学习、各种关联分析

提供完善的安全功能，漏洞管理、威胁管理、响应管理等

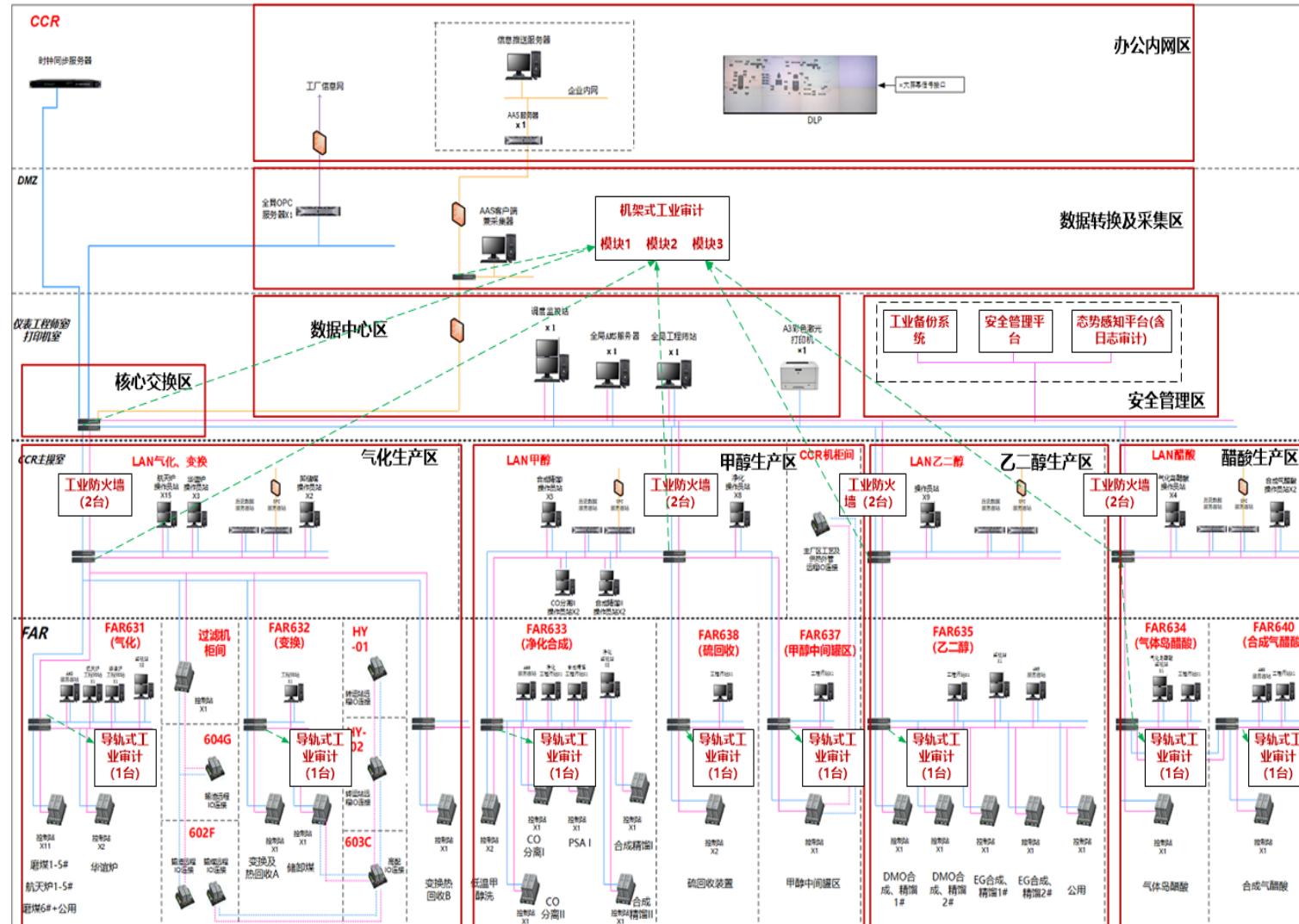
03 案例分享

01华谊氯碱化工

✓ 本项目的主要目的是提升氯碱化工华胜厂全流程工业安全系统的网络安全防护能力，确保该系统对外可以应对监管机构的合规要求，对内可以保证工厂安全生产。



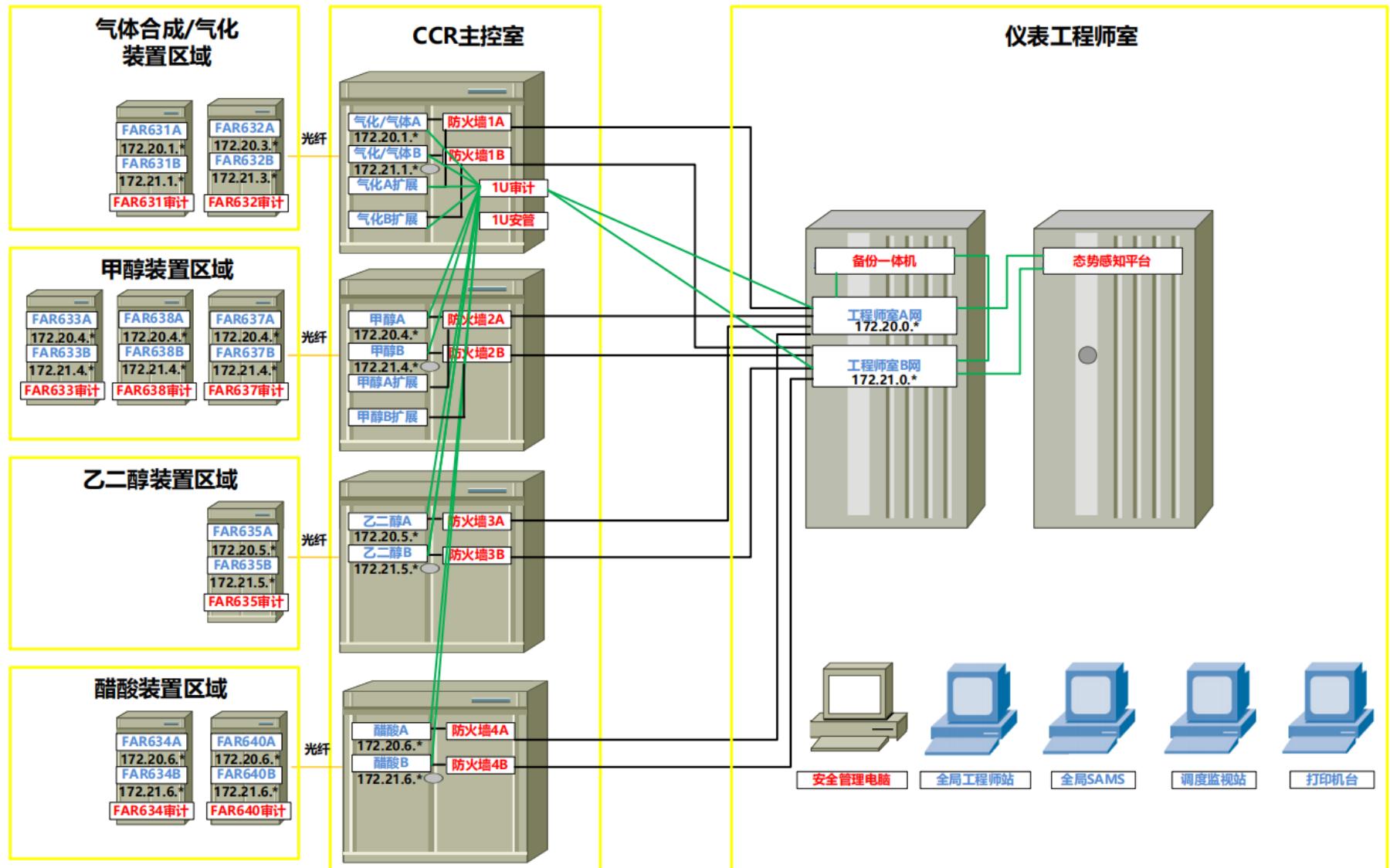
已完成网络边界、网络审计、数据备份、集中管理、态势感知加固工作



02 广西钦州能化

- ✓ 以广西钦州能化的工业互联网安全保障为重点，实时监测工业设备、工业主机、工业生产网络和管理网络、工业数据的安全状况、风险隐患及企业安全管理运行情况等信息。
- ✓ 采用工业防火墙、工业入侵监测、工业日志审计等安全技术和产品的应用，形成防恶意软件传播、防恶意控制指令、防边界渗透、防内网非合规行为等安全防护能力。
- ✓ 通过工业控制网络安全平台的工业信息安全态势感知系统对工业企业安全状态进行未来趋势预测，实现对网络安全监测信息的分类汇聚、精准研判，实现网络安全事件和风险的监测、分析、审计、追踪溯源和风险可视化。

已完成网络边界、网络审计、数据备份、集中管理、态势感知加固工作



完成下列设备安装及调试:

- 1、7台导轨式工业审计；
- 2、1台机架式导轨审计；
- 3、8台导轨式工业防火墙；
- 4、1台机架式工业安管平台；
- 5、1台态势感知服务器；
- 6、1台安全管理电脑；
- 7、网线、PDU等材料的穿接线及整理。

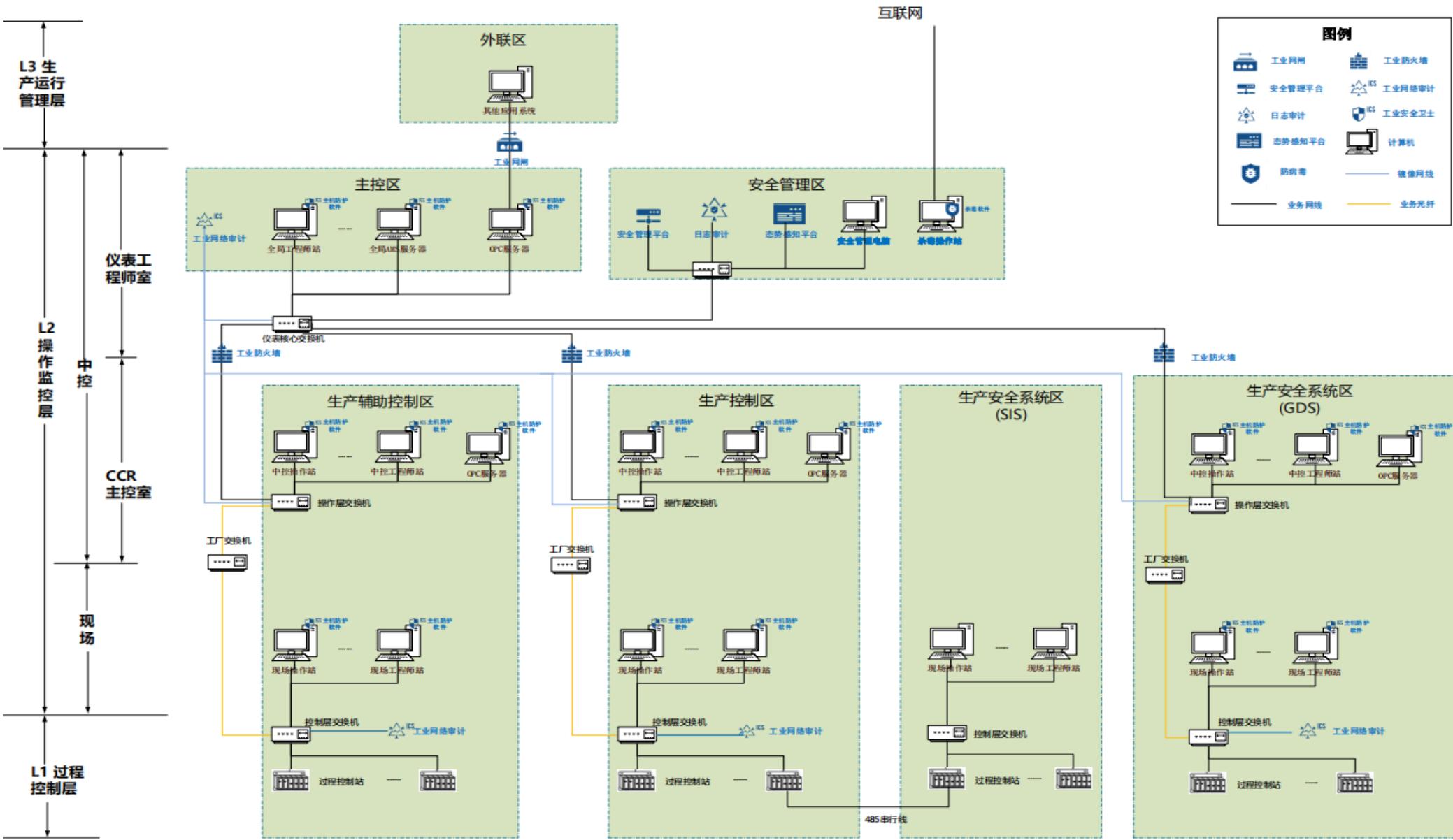
2021年5月13日，所有设备上架工作均已完成，2021年5月20日，所有具备条件的设备均完成调试。



已完成网络边界、网络审计、数据备份、集中管理、态势感知加固工作

04 集团工控网络安全加固 标准解读

● 企业工业网络安全防护技术框架建议



横向分区

纵向分层

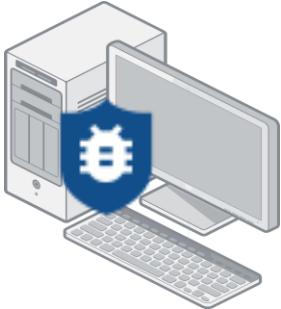
入侵检测

威胁感知

统一管理

● 1、工控网络安全技术管理建议

1.1 安全软件选择与管理

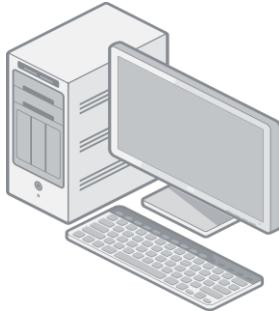


杀毒专用计算机

- (1) 每个生产型企业配备一台杀毒专用计算机，该计算机需要进行定期升级，供应商等外部带入工控网络的U盘，必须经过该计算机杀毒操作，方可接入到生产系统中。
- (2) 企业新建、升级工业控制系统的，必须在DCS等控制系统的选型招标中明确提出同步采购、安装国家有关机构认证过的白名单软件的需求。
- (3) 现存工业控制系统电脑无法安装白名单软件的情况下，需购买专业的离线杀毒工具或杀毒服务，尽量选择停产时进行外挂式杀毒，并安排工控系统集成商进行全程陪同，一旦上位机杀毒后出现故障，立即进行系统和软件恢复。

● 1、工控网络安全技术管理建议

1.2 配置和补丁管理



盗版操作系统和软件



高危服务和端口



工控操作软件



大修期间打补丁

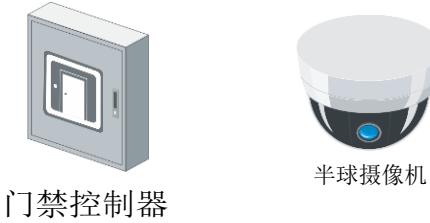


可部署补丁管理服务器

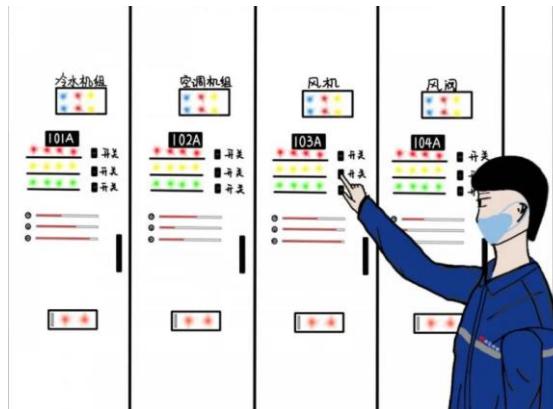
- (1) 禁止在工业控制网络计算机中安装盗版操作系统和软件，工控计算机仅安装必须的工控操作软件。
- (2) 应对工业控制电脑的操作系统、网络设备、控制器开展安全加固工作，确保操作系统、网络设备、控制器的高危服务和端口处于关闭状态。
- (3) 应在装置大修阶段及时开展操作系统、工控操作软件、网络设备、控制器等的打补丁操作。
- (4) 建立补丁更新流程，基于“审批-更新-检查”的可控化补丁更新流程。可考虑在工控网络内统一部署补丁管理服务器，但需实现离线补丁库更新。

● 1、工控网络安全技术管理建议

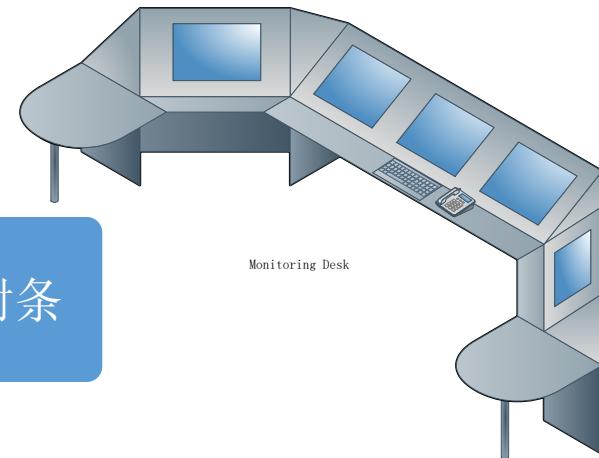
1.3 物理和环境安全防护



- (1) 工业控制网络设备机房采取视频监控、专人值守等物理安全防护措施，严格执行出入登记措施。
- (2) 工业控制网络计算机拆除不必要的USB、光驱等，主机箱应放置在控制台内，并采取上锁、贴封条等防护措施。



拆除USB、
光驱 → 上锁 → 贴封条



1.4 身份认证



口令至少应
该由8个字符
组成



口令应包含
大小写字母



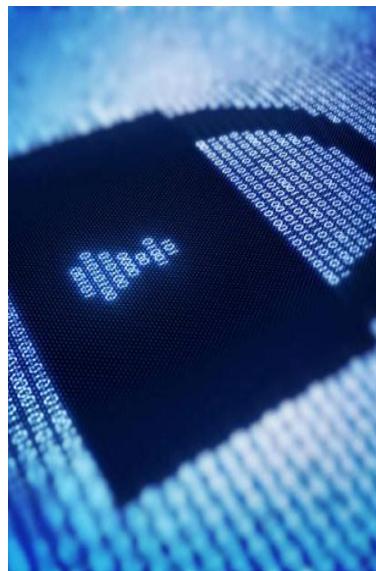
口令应包含
数字、特殊
字符



不要使用字
典中的单词



不要基于人
的姓名、生
日



示例



密码



ppnn13% dkstFeb.1st,

解释

娉娉袅袅十三余，豆蔻梢头二月初



FLZX3000c, Y4yh!9day

飞流直下三千尺，疑似银河落九天



Wwj1wdmm

我忘记了我的密码



hold?fish:palm

鱼和熊掌不可兼得

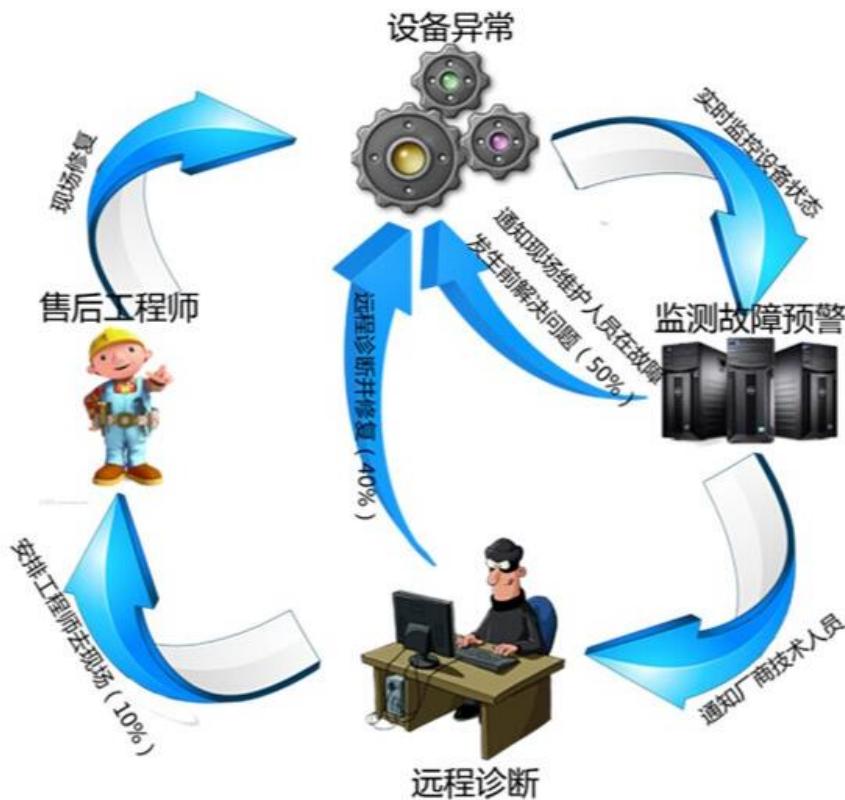
(1) 在操作系统和各类控制软件中需要设置复杂口令，口令长度不小于8位，并同时包含大小写字母、数字和特殊字符中至少三种。

(2) 在上位机软件中需要设置3类帐号权限和口令认证，包括系统管理员、普通操作用户、审计管理员。

(3) 在控制器中需要设置上传下载的密码，防止无认证修改程序。任何系统严禁使用默认密码。

● 1、工控网络安全技术管理建议

1.5 远程访问安全



严格禁止远程接入工控系统运维，必须现场运维。



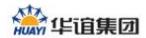
禁止远程接入工控系统运维

● 1、工控网络安全技术管理建议

1.6 安全检测与应急预案



工控安全事件应急预案



2021年5月

工控安全事件应急预案

演练



2021年5月

应在工业控制网络中部署工业网络审计设备进行安全监测。
监测范围应覆盖到每套工业控制系统。
应为每套工业控制系统制定一份该装置遭受网络攻击的应急预案，并定期演练。

● 1、工控网络安全技术管理建议

1.7 资产安全

工业控制系统配置清单		
1	工程师站	XX变更内容
2	操作员站	XX变更内容
3	DCS	XX变更内容
4	PLC	XX变更内容
5	OPC服务器	XX变更内容
6	

应建立工业控制系统资产清单，明确资产责任部门，建立资产使用、处置规则。控制器设备每一次的配置变更，需要进行记录；不进行组态变更的时候，应及时在控制器的硬件上切换到只读模式，防止程序被恶意下载。



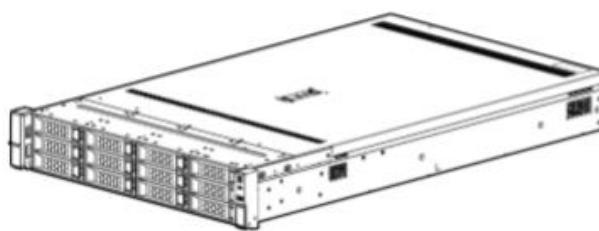
硬件切换到只读

● 1、工控网络安全技术管理建议

1.8 数据安全

每一次，保留一个大修周期

1	工程组态文件	备份时间
2	控制回路设定参数	备份时间
3	报警及连锁设定值	备份时间
4	

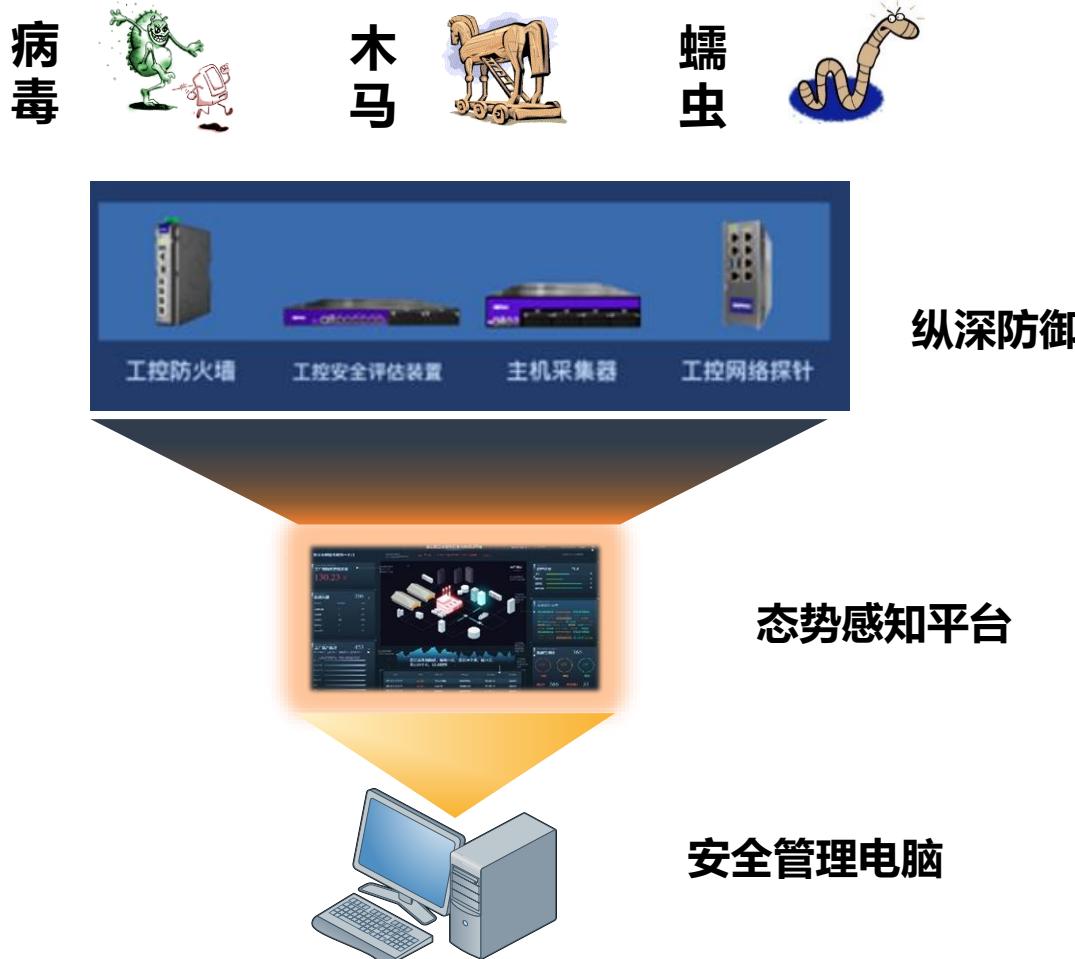


备份一体机自动备份

应定期（每年至少备份一次，每次备份至少保留一个大修周期）对上位机程序、DCS、PLC等程序开展备份操作。包括操作监控层的工程组态文件、控制回路设定参数、报警及连锁设定值等重要数据。在每次系统程序升级后，要求供应商备份最新程序。每个单位应配备一台冗余硬盘的备份专用计算机，统一管理所有的工控备份资料，有条件的可以采用专业的备份一体机设备，对需要备份的关键数据通过预定的备份策略自动进行备份。

● 1、工控网络安全技术管理建议

1.9 安全管理中心



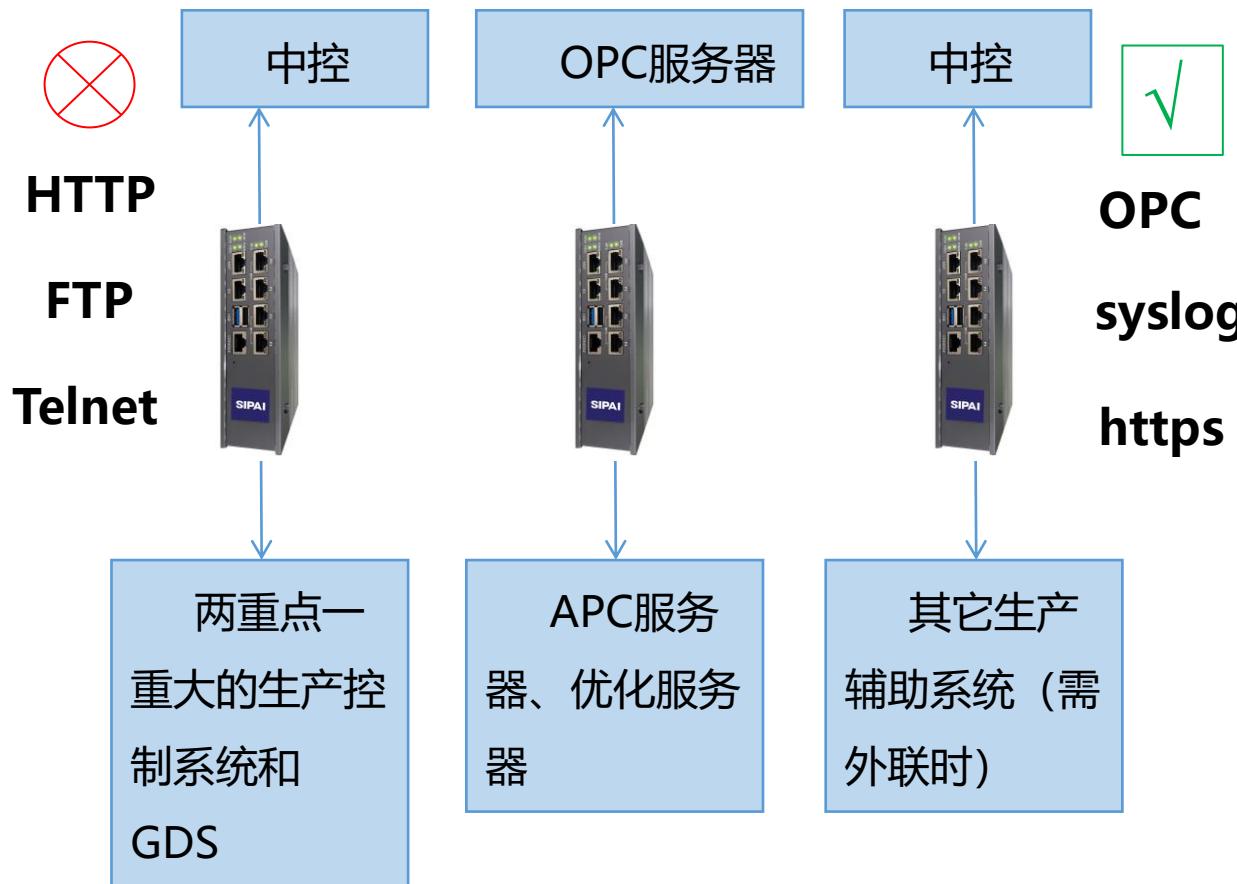
工控网络中应至少配备一台安全专用管理电脑，可以通过B/S架构访问上述安全产品的管理页面，方便进行安全策略的配置、安全告警数据的查看和追溯、以及安全产品的日常运维工作。

成熟工业企业应建立安全态势感知平台，将所有上述安全产品的数据进行采集、提取、理解和预测，找出安全风险点，并提供有效的安全处置建议，使安全工作形成闭环。

运筹帷幄之间，决胜千里之外

● 2、网络分区分域规范和安全加固建议

2.1 工控网络边界安全加固



网络边界作为攻击工业控制网络的入口，其安全防护主要措施包括网络分域（网络隔离）管理。不同横向分区应根据安全性需求的不同而设置不同的安全等级，并根据相应的安全等级采取不同的安全防护措施。生产控制系统，如需与外部进行数据交换，必须加设工业防火墙，独立配置的APC服务器、优化服务器与OPC服务器之间应加装工业防火墙等网络隔离设备。

隔离设备仅允许通过OPC协议数据、syslog协议、https协议、数据库协议数据，不允许通过其它工控协议数据以及HTTP、FTP、telnet等高危服务。

● 2、网络分区分域规范和安全加固建议

2.2 工控入侵检测防护



入侵检测和防御



Modbus TCP



OPC DA/UA

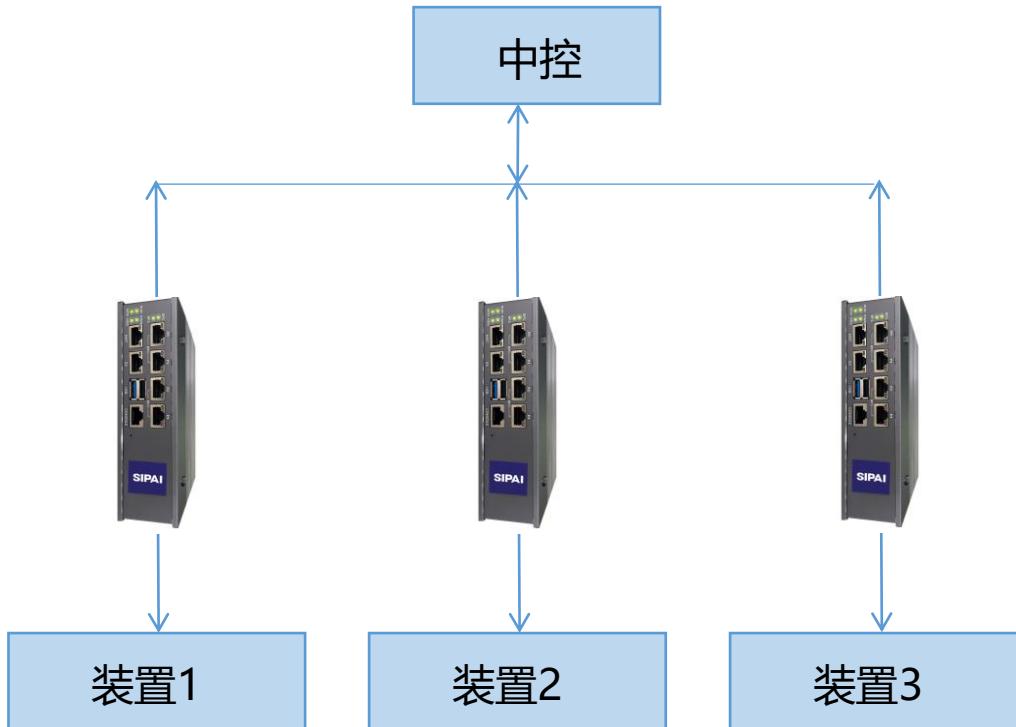


S7、Profinet等

办公网络和工业控制系统网络的边界需要具备入侵检测和防御功能，能够检测传统的网络安全攻击行为，另外还需要支持Modbus TCP、 OPC DA、 S7、 OPC UA、 Profinet等工业控制协议的解析和识别，解析内容包括源目的IP、 源目的端口、 协议名称、 协议内容等。

● 2、网络分区分域规范和安全加固建议

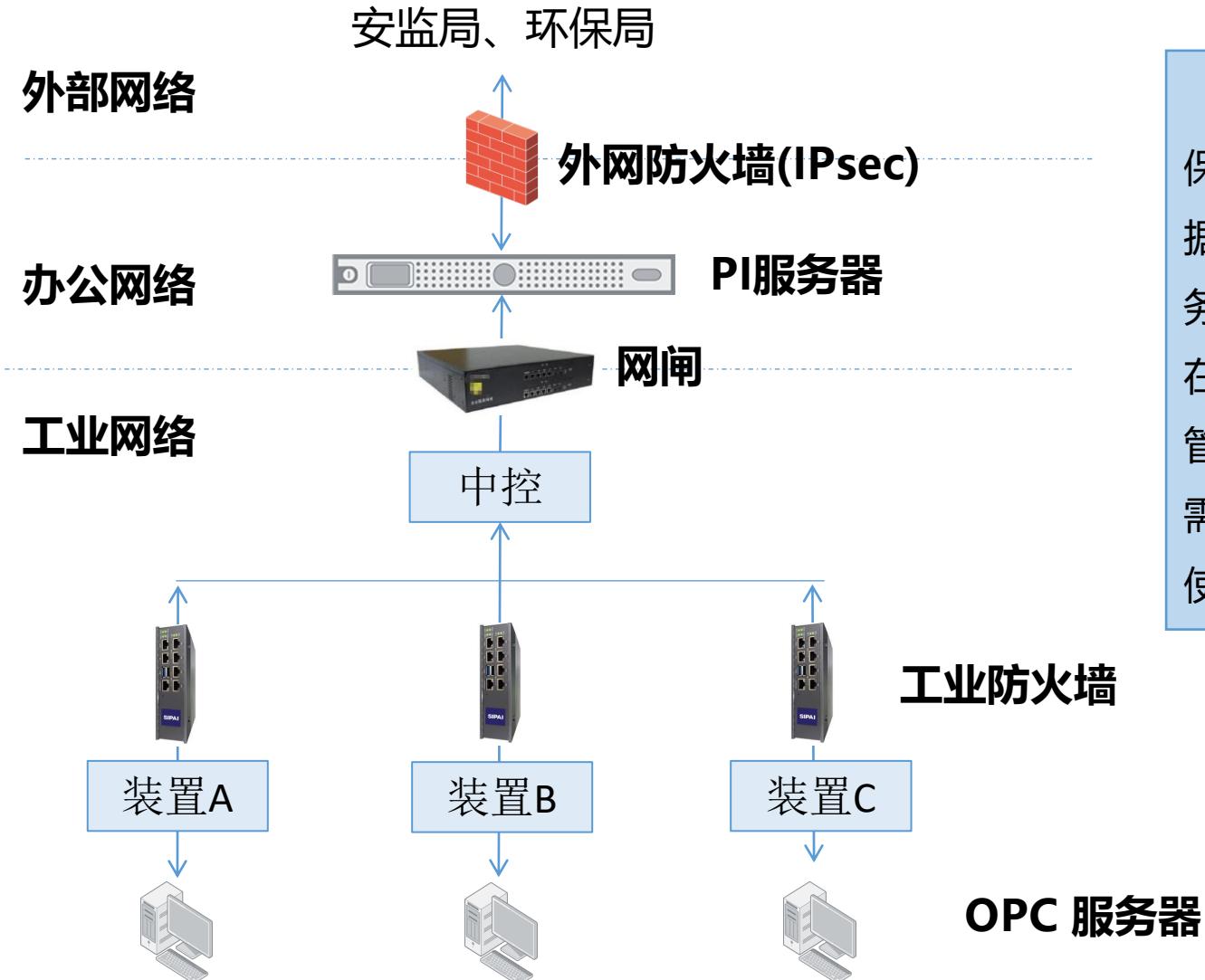
2.3 工业控制内部安全防护



工业控制内部网络作为实现工业控制正常运行的核心，必须考虑其自身的安全性，其主要考虑工业控制系统间的网络分区隔离，将工业控制网络划分成不同的网络区间，通过工业控制防火墙实现不同DCS系统之间的网络隔离，实现精细化的控制网络管理。同一套装置内部各套系统间，如无必要数据交换的，应各自采用独立交换机接入。

● 2、网络分区分域规范和安全加固

2.4 数据传输安全防护



在生产网数据要传输到外部网络，如安监局、环保局等监管部门时，不应直接从OPC服务器上取数据；应当从上层网络（如部署在办公网络中的PI服务器、数据网关、代理服务器）上取数，同时需要在企业出口部署防火墙，此时安全防护要求可视同管理网安全防护要求；除了配置访问控制策略，还需要进行IPsec加密的配置工作，必要情况下，可以使用专用加密设备。

- 我们可以

认识到网络安全的重要性并积极落实

- 落实网络安全责任，是我们做好安全的第一步
- 同步规划、同步设计、同步建设是原则
- 工控网络安全和生产安全一样重要
- 安全应急预案和安全应急演练是检验安全措施是否有效的有力措施。
- 网络安全问题不能仅依靠一次性投入解决，要建立安全运营、主动防御的思路，配置相关的制度和人，才能有效降低网络安全风险。



欢迎扫码加入群答疑

