



烟草行业等保2.0工业安全建设思考

- 落实等级保护规定，夯实工控安全基础

宋 强

奇安信集团工业互联网安全产品总监

目录

- 等保2.0工控安全要求
- 工控网络安全解决方案
- 烟草行业工控安全建设思考

U.S. Escalates Online Attacks on Russia's Power Grid

- 2019年6月,《纽约时报》援引美国现任和前任安全事务官员的话称,美国正在加大对俄罗斯电网的网络攻击,“**自2012年以来,美国已将侦查探测程序植入俄罗斯的电网系统之中**,但在过去一年中,这些行动的强度和规模都在加大,美国的行动目标已经从单纯的警告考虑更多转向为**进攻性**的考虑。”



- 2019年3月7日,委内瑞拉全国23个州中的**18个州电力供应中断**。停电给委内瑞拉带来了重大损失,全国交通瘫痪,地铁系统关闭,医院手术中断,通讯线路中断,航班无法正常起降.....
- 3月9日上午,全国70%的电力供应本已恢复,但随后**电力系统再遭攻击**,导致再次发生大范围停电。

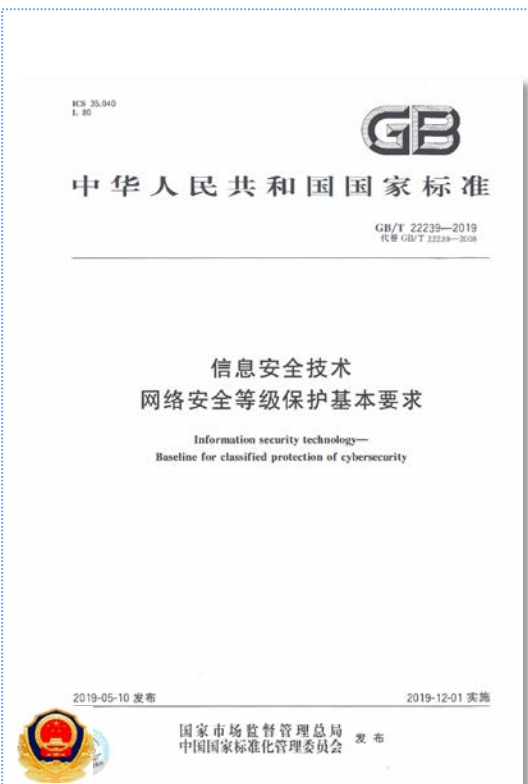


- 2019年2月21日,一名伊朗高级指挥官称,伊朗曾经**成功渗透进美国军方指挥中心系统**,并**控制了7至8架**正在叙利亚和伊拉克执行飞行任务的**美军无人机**。
- 2019年6月,在伊朗击落美国一架无人机后,**美国决定将网络战作为打击伊朗的首选项**。

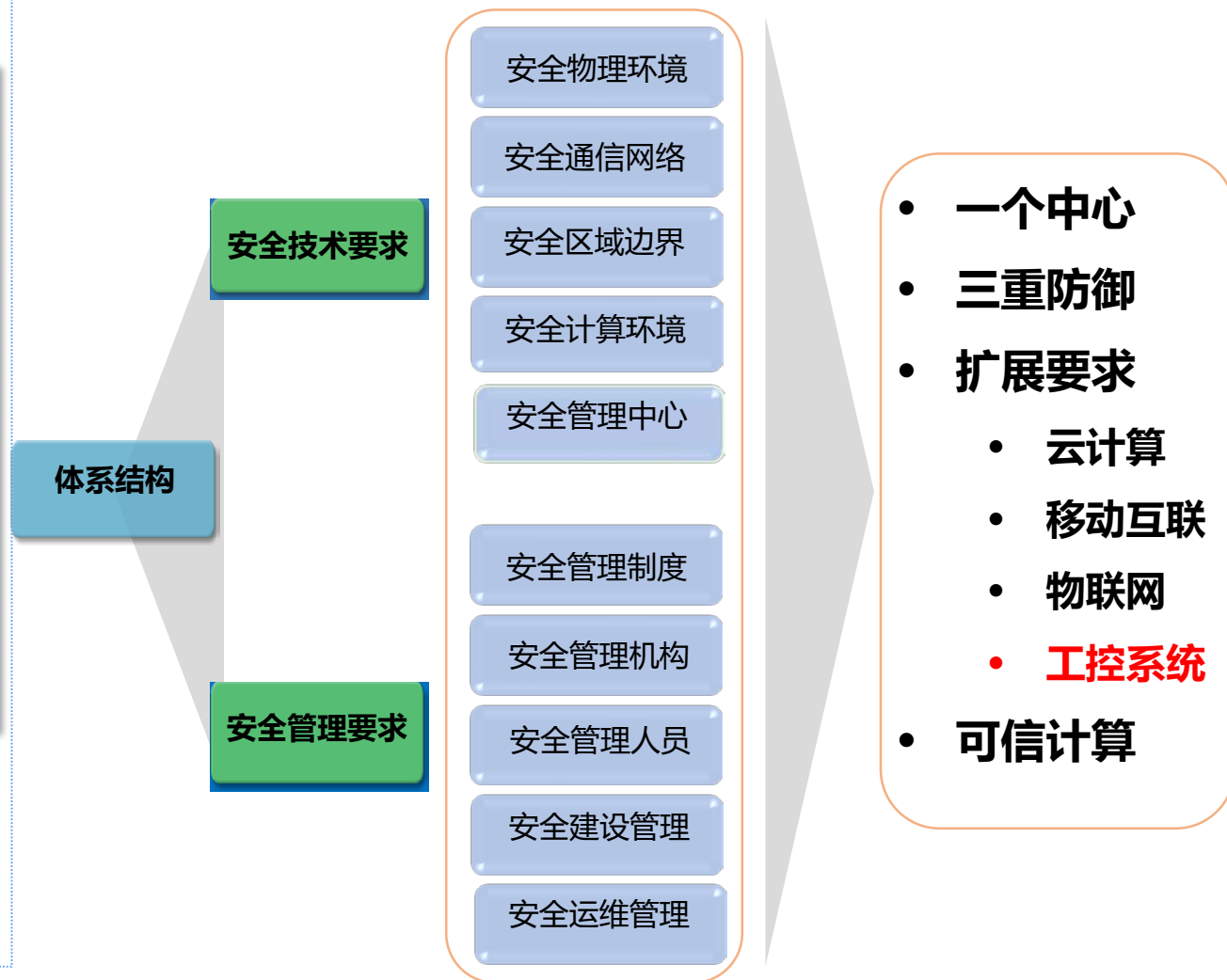
机构	时间	政策文件	政策说明
全国人大	2017.06	● 《中华人民共和国网络安全法》	第三十一条 国家对公共通信和信息服务、 能源、交通、水利、金融、公共服务、电子政务 等重要行业和领域 ... 关键信息基础设施 ，在网络安全等级保护制度的基础上，实行 重点保护 。
国务院	2017.11	● 《关于深化“互联网+先进制造业”发展工业互联网的指导意见》	建立“ 工业互联网安全保障 体系、提升安全保障能力”发展目标。
工信部	2011.10	● 《关于加强工业控制系统信息安全管理的通知》（451号）	... 加强重点领域 工控信息系统安全管理措施 ，特别提到了与国计民生紧密相关领域的控制系统，如 核设施、电力、天然气、铁路、城市轨道交通、民航、城市供水 等
工信部	2016.10	● 《工业控制系统信息安全防护指南》（338号）	工业企业开展 工控安全防护 工作的 整体性指导文件 。
工信部	2017.06	● 《工业控制系统信息安全事件应急管理工作指南》（122号）	指导做好 工业控制系统信息安全事件应急管理 相关工作，保障工业控制系统信息安全。
工信部	2017.08	● 《工业控制系统信息安全防护能力评估工作管理办法》（188号）	检验338号文的实践效果， 综合评价工业企业工业控制系统信息安全防护能力 。
工信部	2017.12	● 《工业控制系统信息安全行动计划（2018-2020）》（316号）	为全面落实国家安全战略， 提升工业企业工控安全防护能力 ，促进工业信息安全产业发展，加快我国工控安全保障体系建设，制定本 行动计划 。
工信部	2018.05	● 《工业互联网发展行动计划（2018-2020年）》	工业互联网安全指导性文件，明确并 落实企业主体责任 ，... 建立针对 重点行业、重点企业 的 监督检查、信息通报、应急响应 等管理机制。
网信办	2017.07	● 《关键信息基础设施安全保护条例（征求意见稿）》	第十八条 ...应当纳入关键信息基础设施保护范围： （一）政府机关和 能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业（供水、供热、燃气） 等行业领域的单位；
公安部	2019.05	● 《网络安全等级保护基本要求》	...针对共性安全保护需求提出安全通用要求，针对云计算、移动互联、物联网、 工业控制 和大数据等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准。。



2017.06.01
从合规到合法

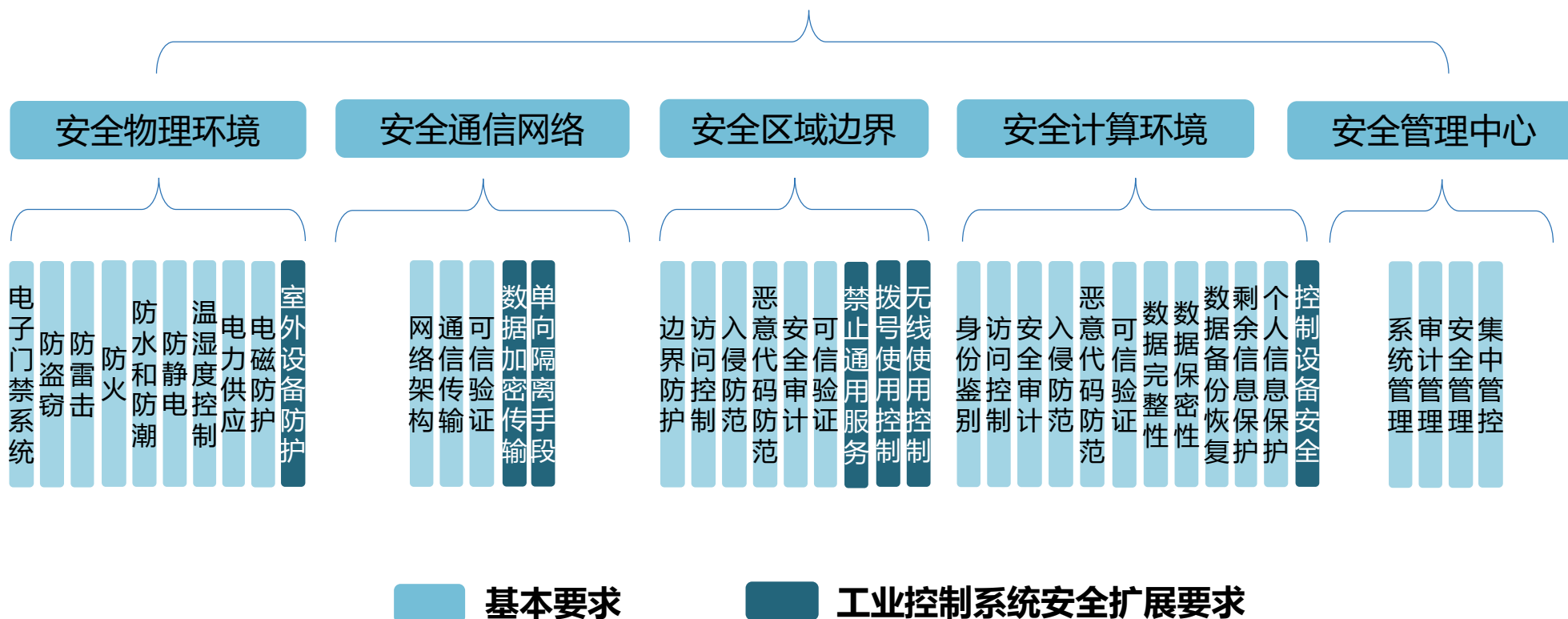


2019.05.10
“等保2.0”



《信息安全技术 网络安全等级保护基本要求》

第三级安全要求（技术）



	控制点 (10)	一级	二级	三级 (22)	四级
安全物理环境	室外控制设备防护	2	2	2	2
安全通信网络	网络架构	2	3	3	3
	通信传输	0	1	1	1
安全区域边界	访问控制	1	2	2	2
	拨号使用控制	0	1	2	3
	无线使用控制	2	2	4	4
安全计算环境	控制设备安全	2	2	5	5
安全建设管理	产品采购和使用	0	1	1	1
	外包软件开发	0	1	1	1
安全运维管理	安全事件处置	0	1	1	1

	工控安全扩展要求项
安全域隔离	<p>8.5.2.1 网络架构</p> <p>a) 工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段；</p> <p>b) 工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；</p> <p>c) 涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离。</p> <p>8.5.3.1 访问控制</p> <p>a) 应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务；</p>
控制非法外联	<p>8.5.3.3 无线使用控制</p> <p>b) 应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；</p>
安全功能上移	<p>8.5.4. 1 控制设备安全</p> <p>a) ... 如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；</p>
慎重更新补丁	<p>8.5.4. 1 控制设备安全</p> <p>b) 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；</p>
尽量关闭接口	<p>8.5.4. 1 控制设备安全</p> <p>c) 应关闭或拆除控制设备的软盘驱动、光盘驱动、USB接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；</p>

目录

- 等保2.0工控安全要求
- 工控网络安全解决方案
- 烟草行业工控安全建设思考



补丁打不上
漏洞百出

- 担心影响生产不想打
- 主机不联网无法升级
- 系统老旧无补丁可打



病毒杀不完
带病运行

- 硬件配置太低装不上杀毒软件
- 无法升级杀毒软件病毒库老旧
- 担心误杀工业软件，干脆不装



资产查不清
暗藏隐患

- 工业主机家底不清楚
- 资产配置分布不可视
- 整体安全隐患不了解

网络空间正在发生什么？



传统防火墙不适用工业控制网络



挑战一：不支持工控协议

- ① 特有的工业协议（OPC、S7、Modbus、DNP3等），以及存在较多私有协议
- ② 工控系统特有的安全漏洞，与IT系统应对机制不一样



挑战二：不适应物理环境

- ① 工业现场环境相对比较恶劣（如高低温、粉尘、潮湿、酸碱等），要求专门的硬件设计，做到全密闭、无风扇，支持 - 40°C ~ 70°C 宽温



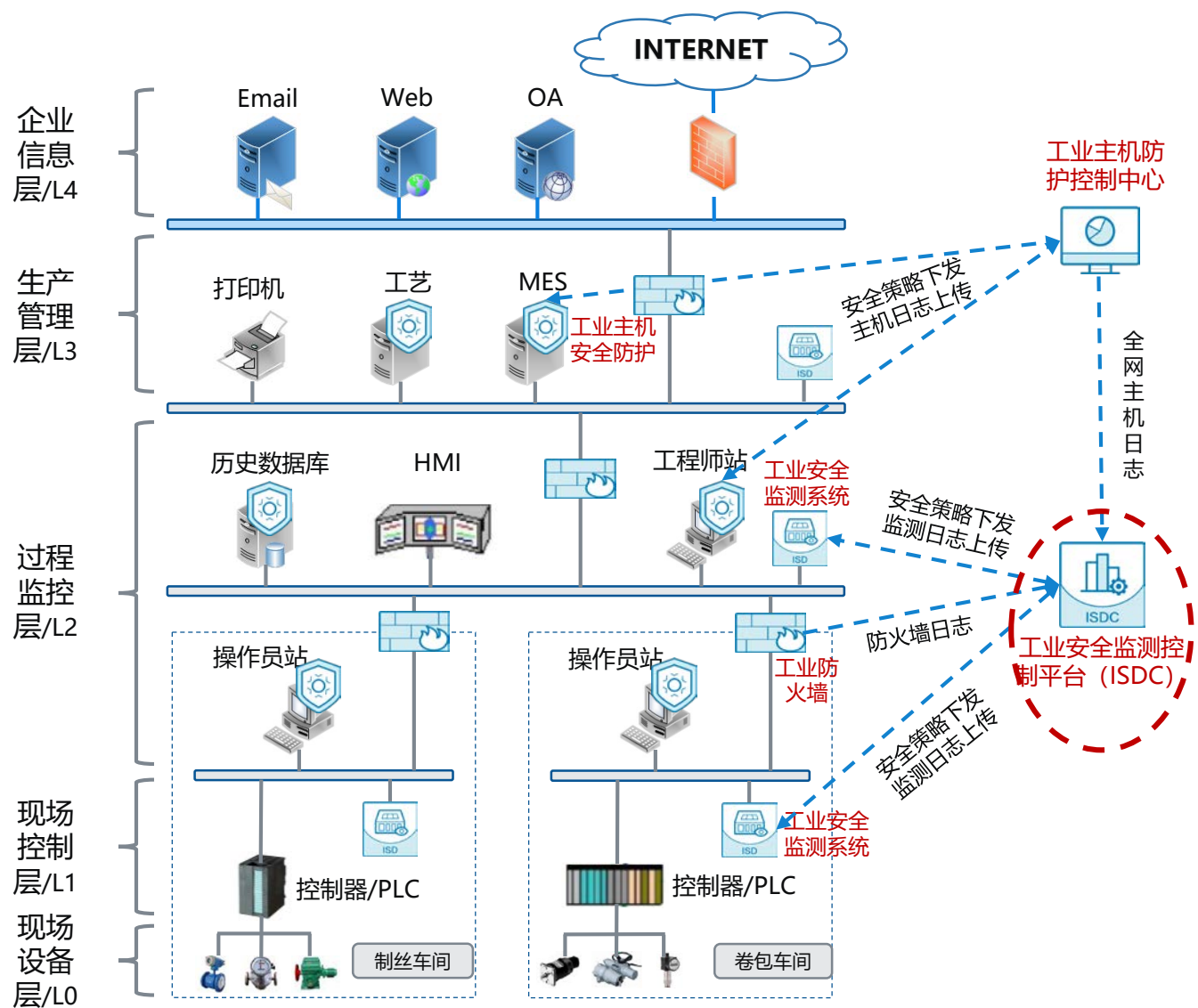
挑战三：不满足高可靠性

- ① 平均无故障时间 > 10年，使用寿命 15-20年
- ② 从IT“故障关闭”到OT“故障畅通”，处理的原则不同



挑战四：不匹配运维要求

- ① 不允许频繁升级
- ② 策略稳妥实施，不允许现网调试试错
- ③ 访问控制对时延要求更为敏感



工业资产状况

资产数量不清楚
资产类型不清楚
资产分布不清楚

工业安全威胁

谁有隐患不知道
谁被攻击不知道
攻击后果不知道

工业资产
为核心的
风险可视化

工业生产故障

设备断线难定位
设备停机难定位
异常操作难定位



恐惧源于未知，看见才能安全

“永恒之蓝”超前防御，防蓝屏



一键设置白名单, 无需升级



网络防护, 主机中毒后防止扩散



入口拦截

运行拦截

扩散拦截

U盘管控, 防止非授权外设引入病毒



三种模式一键切换, 保障生产连续性



日志审计, 溯源攻击主机和恶意程序





自动发现工控漏洞

- 资产漏洞映射，开放端口，不安全协议
- 支持3大漏洞库CVE, CNVD, CNNVD
- 覆盖220+厂商, 3300+条漏洞



IDS入侵检测

- 各种工业漏洞利用行为
- 缓冲区溢出，拒绝服务攻击
- 检测端口扫描、口令探测等渗透行为
- 5000+条规则，持续更新



检测网络病毒

- 检测病毒木马，僵尸蠕虫，及各种间谍软件，及时告警提示



识别控制器关键操作

- 控制器组态下装、上载，起动、停止、复位
- PLC程序下装、上载，文件写入，固件升级



识别工业资产，建立资产清单

- 设备类型 PLC, DCS, HMI, RTU
- 品牌型号 西门子，施耐德，罗克韦尔，和利时
- 软件系统 Win2000, Win XP, Web站点
- 设备属性 IP, MAC, 端口



建立工控基线，监测生产异常

- 自学习业务行为，建立基线模型
- 深度解析流量，发现异常行为



建立动态行为基线

- 设备之间通信模型相对固定
- 协议，内容，时间，频次，流量
- 偏离基线意味着发生异常



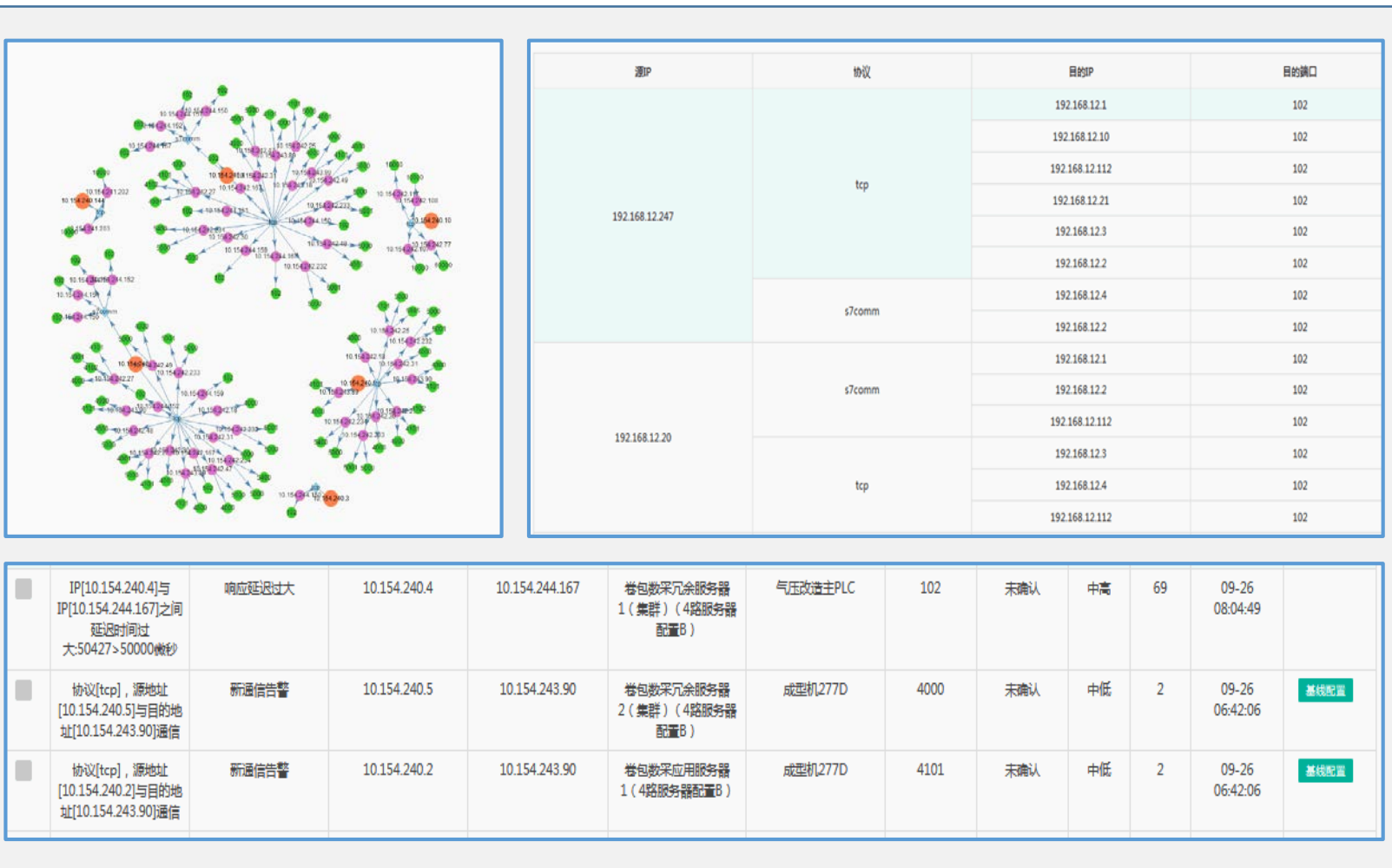
多维数据构建基线模型

- 覆盖制丝、卷包、集控、能动
- 采集解析汇聚数据资源池
- 机器学习梳理优化通讯模型



偏离基线生产异常监测预警

- 流量峰谷合规分析
- 数据上传时间频次审计
- 数据交互延迟判断PLC健康度





专有硬件防火墙

- 工业网络环境，宽温，无风扇，导轨/机架
- 工业控制协议



部署位置

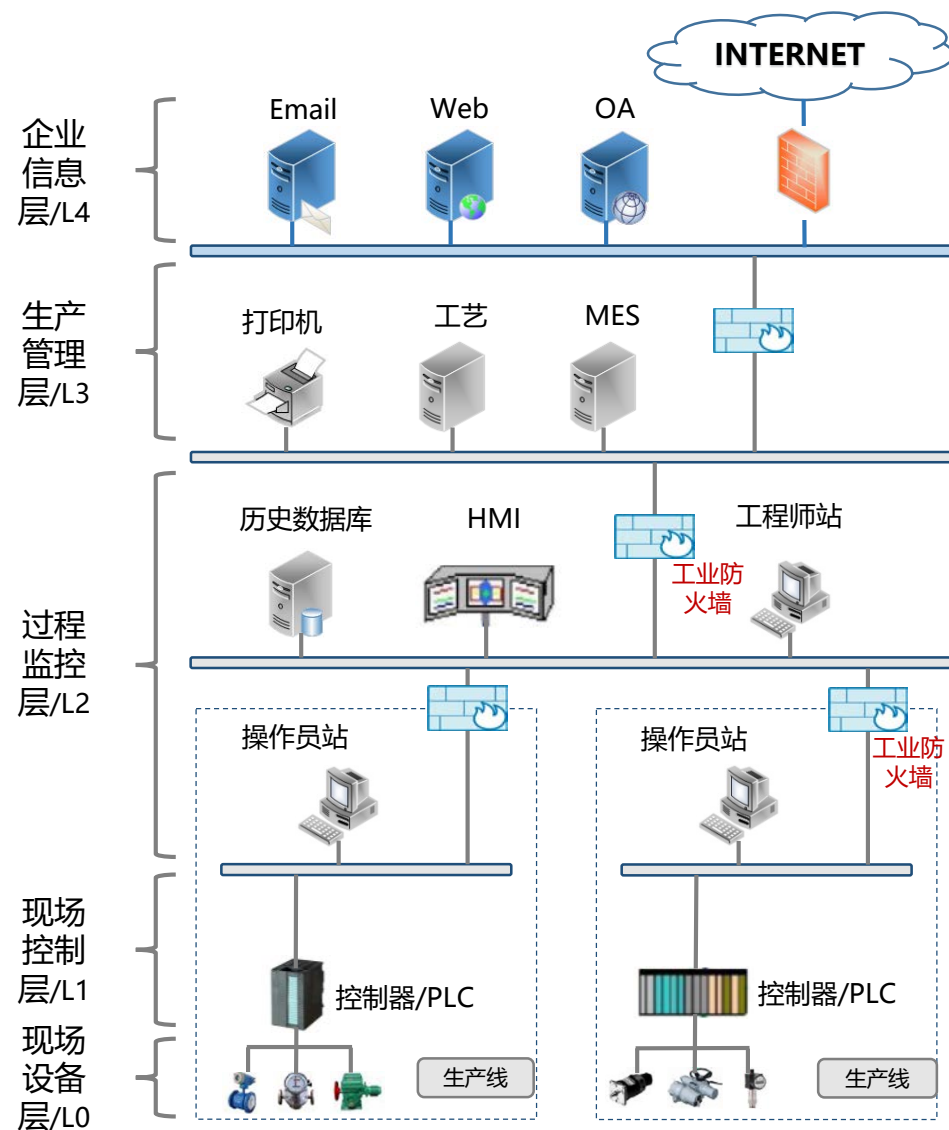
- 监控网与控制网之间
- 生产线上位机与控制设备之间



导轨式
适用控制现场



机架式
适用机房环境

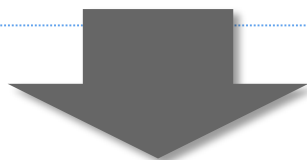
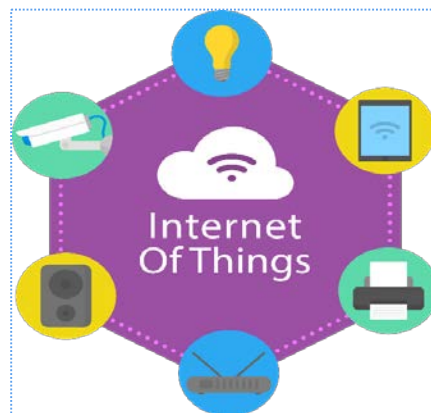
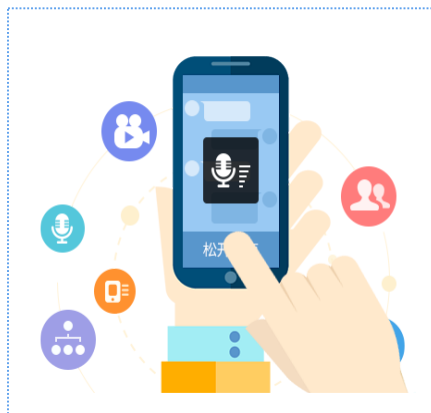


目录

- 等保2.0工控安全要求
- 工控网络安全解决方案
- 烟草行业工控安全建设思考

思考一：迎接技术变革，必先夯实基础

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

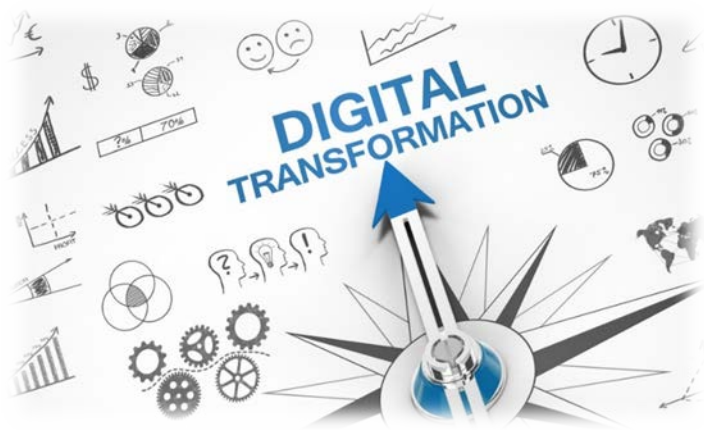


互联网+

卷烟智能工厂

CPS工业互联网平台

融合创新与产业升级

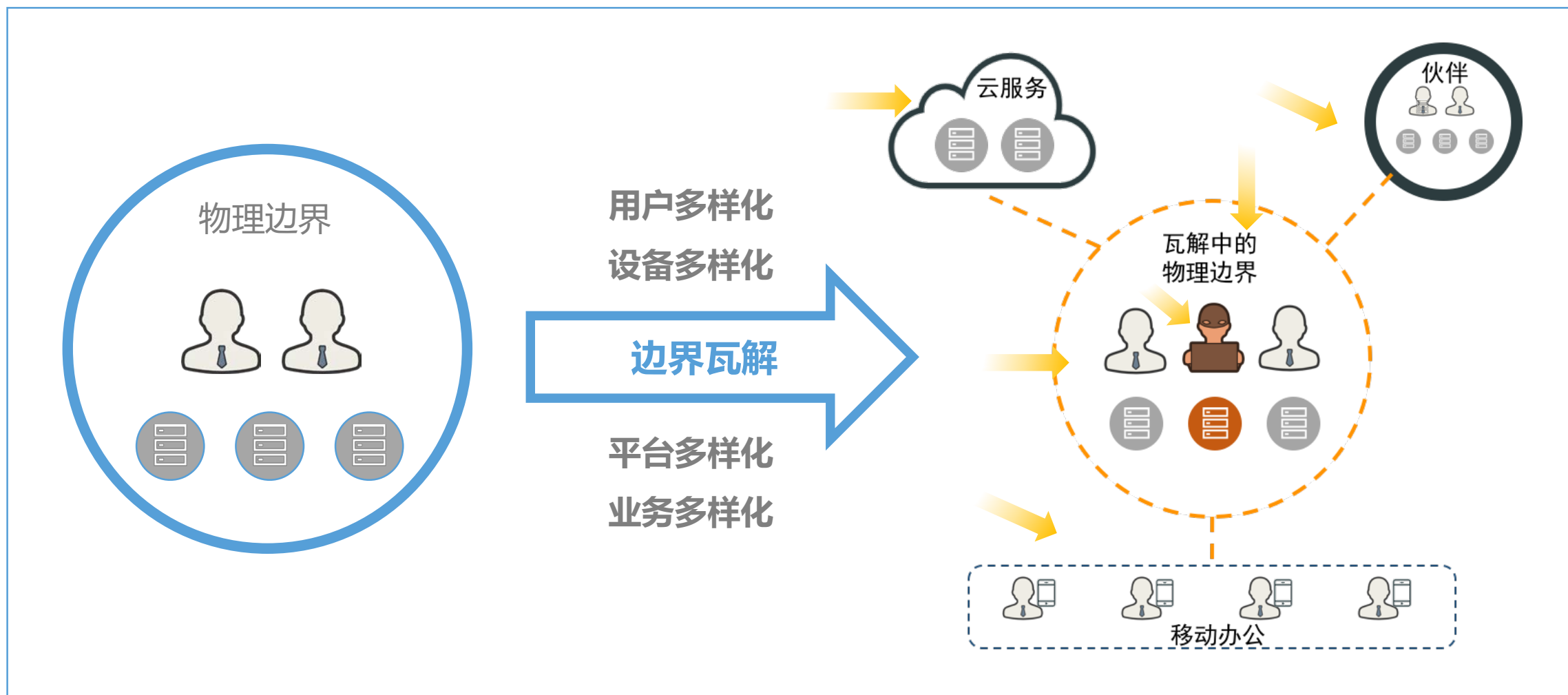


数字化转型



工业互联网

边界瓦解，设备联网，工业上云，数据流动，老问题没有消失，又迎来新挑战

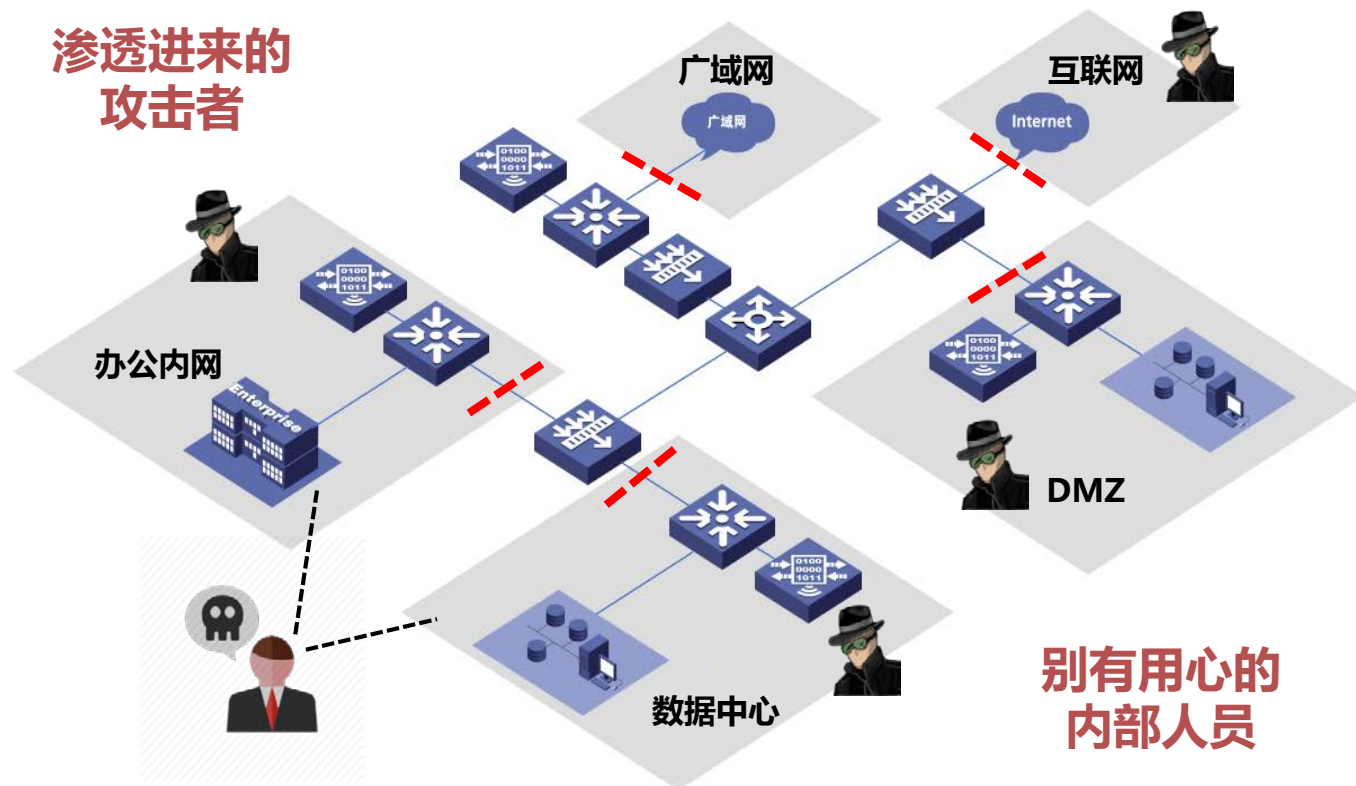


数据分散在不同的业务应用中并持续流动，流动加剧了大数据的风险

安全意识?

安全投入?

安全措施?



边界安全架构：为内网中的人和设备预设了过多的信任

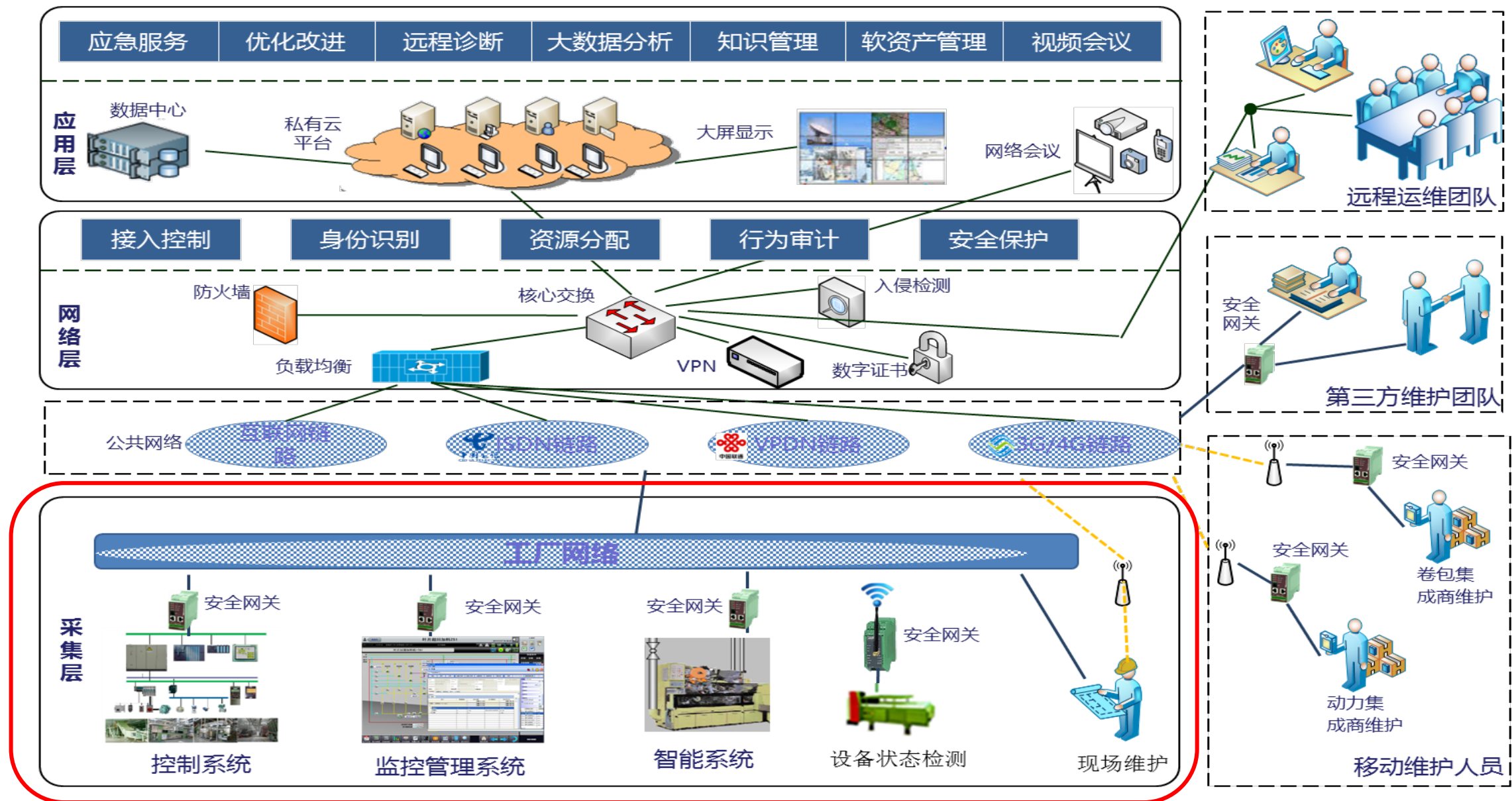


每一次数据泄露“黑天鹅”事件背后，都隐藏着“灰犀牛”式的危机。

工业互联网安全建设，基础不牢，地动山摇

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



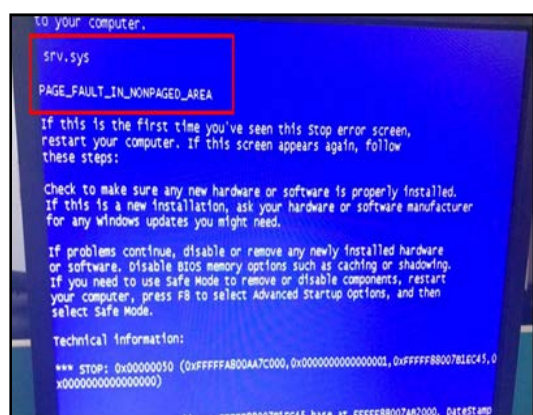
思考二：工控安全建设，重在落实执行

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

近几年与合作伙伴一起应急服务过上百起工业网络攻击事件，包括多家烟草企业，
多数发生**工业主机蓝屏**，**反复重启**，**勒索加密**，甚至**生产停工**



某烟厂制丝车间，集控服务器反复蓝屏重启，停产



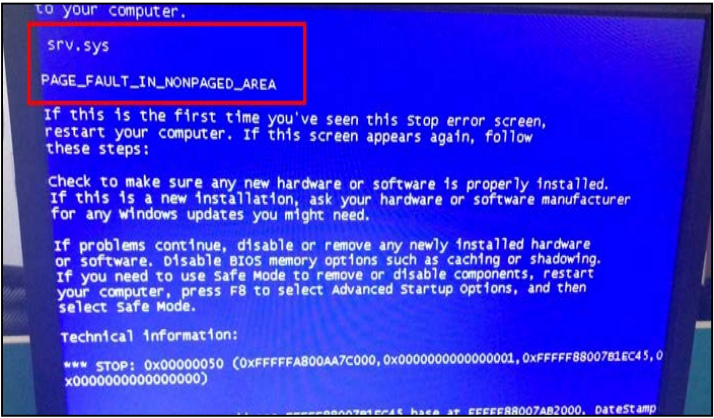
某烟厂卷包车间，U盘导致数采主机中毒，批次无法跟踪



某烟厂数据中心，错误配置导致直连互联网，遭勒索攻击

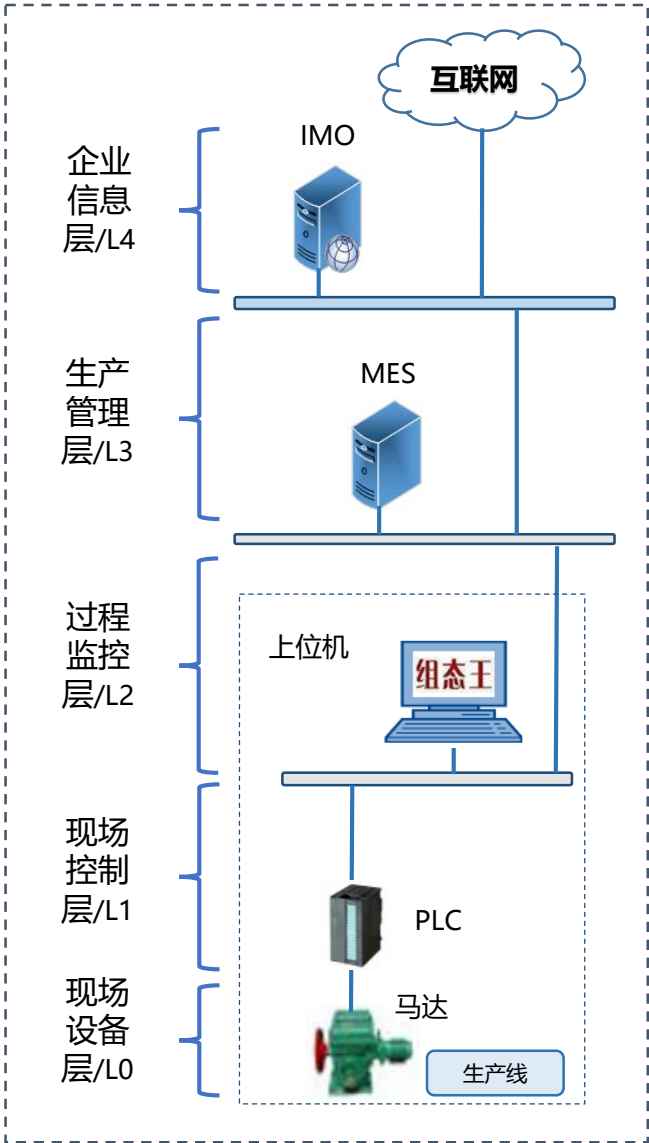
事件过程

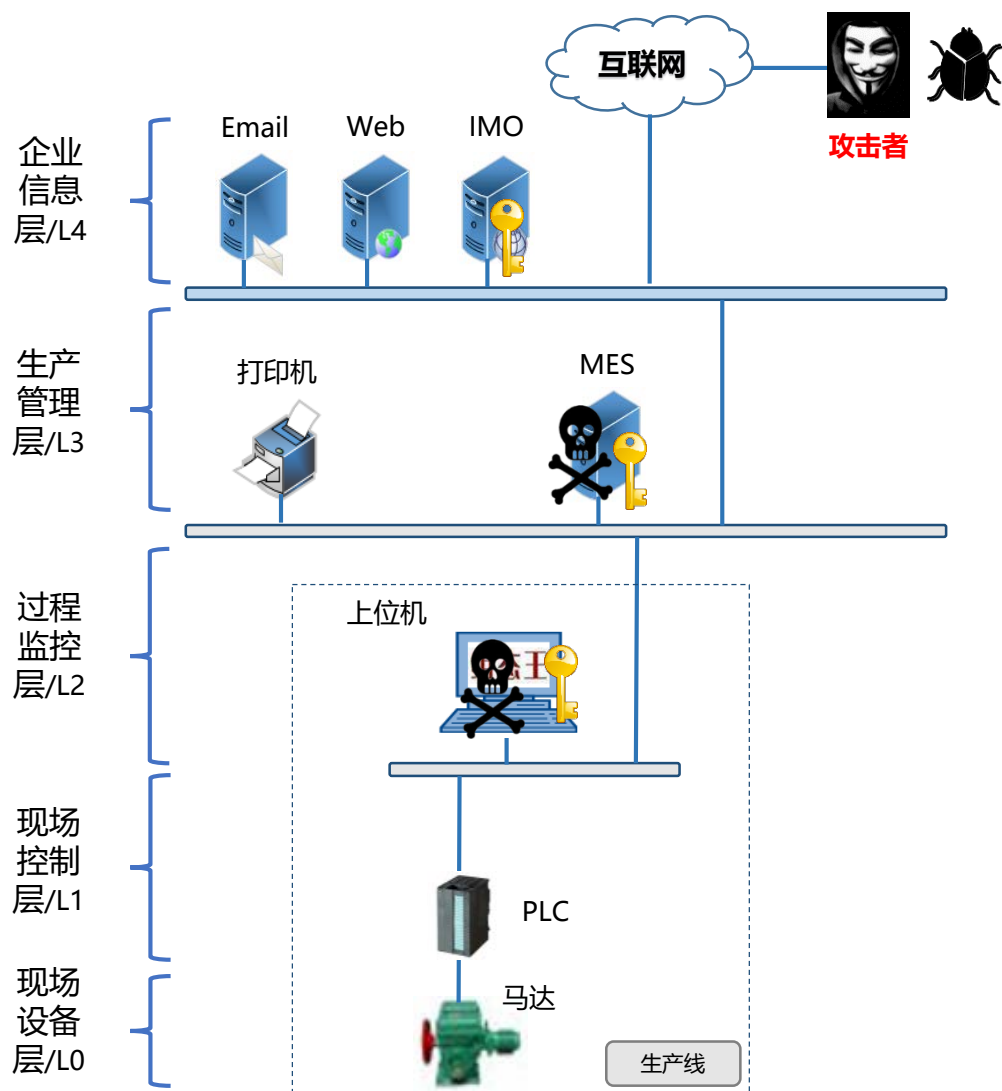
2018年9月，某大型智能制造企业遭勒索病毒攻击，数十台工业主机蓝屏重启，多条生产线停产，损失严重。工业安全团队提供紧急安服响应，帮助快速恢复生产。通过对现场网络安全风险评估，发现多个安全漏洞。



在实验室仿真客户环境，还原攻击过程。

设备	用途	系统配置	存在漏洞
IMO	OA服务器	CentOS	任意命令执行漏洞
MES	生产管理服务器	Win7 64位	“永恒之蓝”漏洞
上位机	控制PLC	WinXP SP3，组态王，双网卡配置	远程堆溢出漏洞
PLC	控制器	西门子300	拒绝服务漏洞





1. 攻陷IMO服务器

攻击者利用办公网IMO服务器的任意执行漏洞，发起攻击获得服务器权限。



2. 攻陷MES服务器

搜索内网发现MES主机，利用MES存在的“永恒之蓝”漏洞，获取权限；将勒索病毒样本上传至MES主机运行，病毒在内网中蔓延传播。



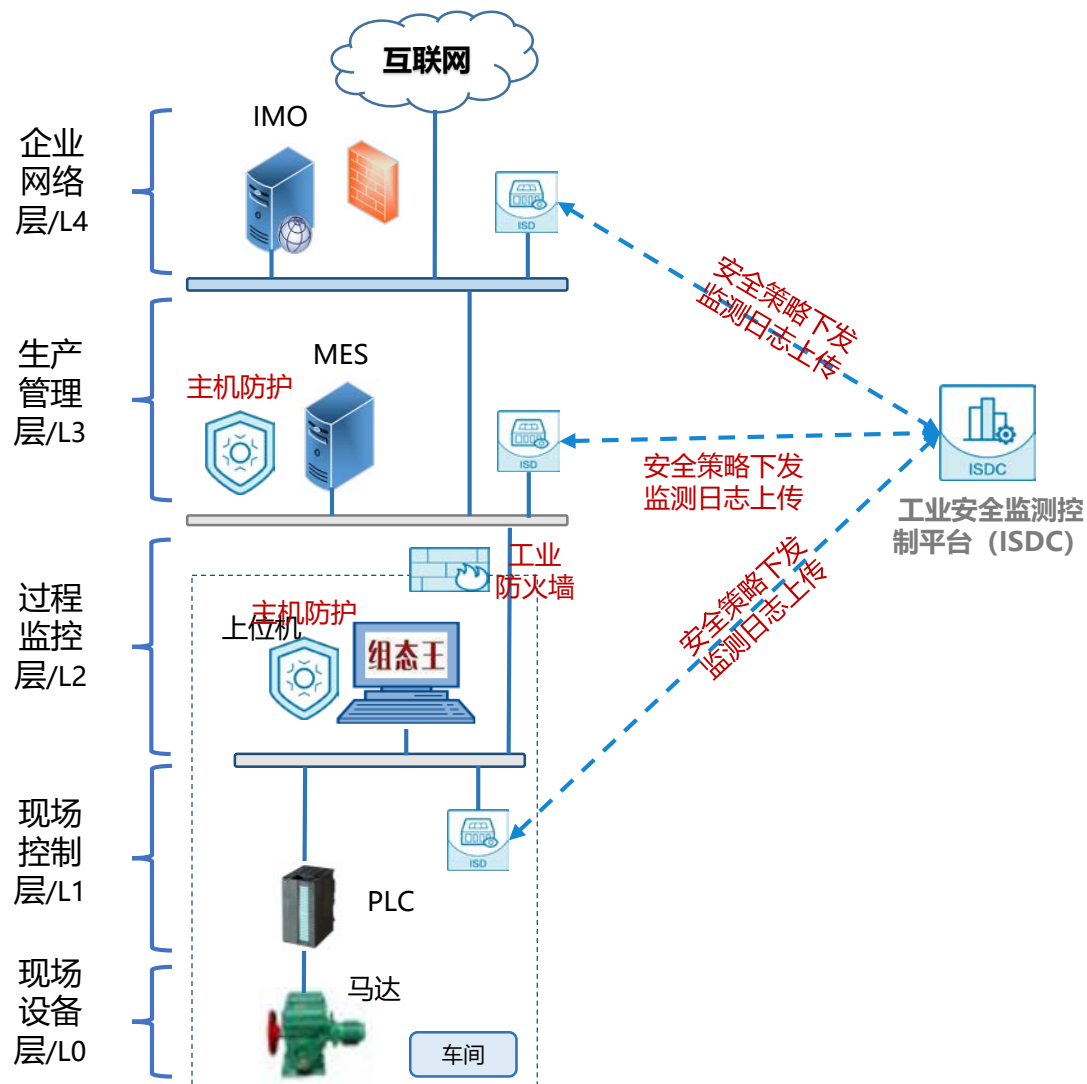
3. 攻陷上位机

搜索内网发现双网卡配置的XPSP3上位机，利用上位机组态软件的远程堆溢出漏洞，获取上位机权限。



4. 攻击PLC

继续搜索发现西门子300控制器，向上位机投递PLC攻击软件，程序运行后向PLC发送特制攻击报文，致使PLC进入Defeat状态，其控制的马达（生产线）停转。



加强安全监测

- L2、L3、L4层旁路部署工业安全监测设备，监测网络攻击与控制器异常操作
- 告警/事件实时上传安全监测控制平台




部署主机防护

- MES主机和上位机安装主机防护软件
- 白名单管控，拦截病毒攻击



加强边界防护

- 办公网出口部署防火墙，阻止互联网攻击
- L3与L2之间部署工业防火墙，阻止办公网攻击进入控制网

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE