工业互联网产业联盟
Alliance of Industrial Internet

IIoT安全挑战与应对

企业工业互联网安全观察与思考

彭卓
树根互联技术有限公司 CISO
工业互联网产业联盟安全组副主席
安加互联 CEO

智 联 赋 能　　融 通 创 新

2019 工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019

目录
Contents

根云平台

安加互联 SECADDIOT

率先发展到跨行业赋能

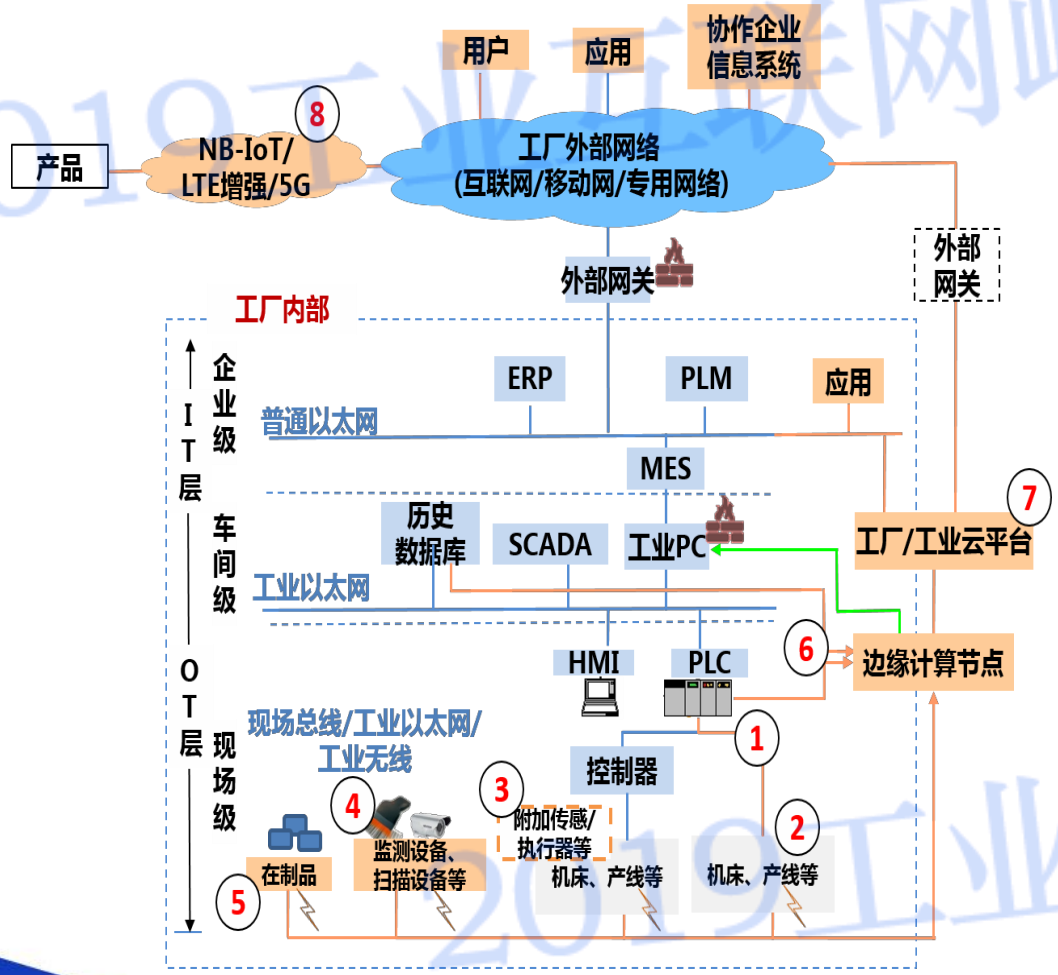
根云平台

安加互联 SECADDIOT

通过IoT实时在线运营的方式，服务超过61种不同行业

根云平台

灰场升级建设任务



1. 通信方式改造
2. 现有设备增加网络接口
3. 现有设备加装传感器等
4. 部署新的监测设备等
5. 在制品网络化
6. 边缘计算节点
7. 引入云平台、大数据
8. 产品智能化

安全现状-根云租户

安加互联 SECADDIOT

1. 相互独立的安全治理机构和政策。
2. 安全团队对OT资产缺乏可见性。
3. 存在OT网络、资产及其安全影响，多年未被发现和管理。OT网络扁平， 各工业组件使用不同的供应商架构和安全标准，存在危险通信通道。
4. OT安全评估由IT提供商完成，不了解OT域，多不包括OT网络的过程和控制层。
5. IT安全控制在OT设置中使用，而不考虑对OT的影响。如IT安全控制主动扫描网络。工厂经理不允许主动扫描OT网络，可能导致PLC失败。另IT安全工具不会对OT协议进行深度数据包检查，例如DNP3Modbus
6. IT和OT域之间的安全责任模糊不清。
7. 控制工程师、 OT供应商或维护商具有不受控制和不安全的远程访问。
8. OT和垂直特定威胁情报既没有收集也没有使用。。
9. IT与OT响应计划之间的协调有限。OT的事件响应计划没有与关键利益相关者合作制定，如设备制造商、运营、工程、安全（如健康、Safety，Security和环境）和法律部门。
10. 由于缺乏备份和恢复机制，恢复很慢。
11. 安全意识和培训计划未扩展到OT人员，且未考虑IT和OT之间的文化差异。

安全现状-误区

安加互联 SECADDIOT

	误区	现实
1	OT系统面临与IT相同的风险，因此OT和IIoT可使用IT方法计算风险并评估威胁	具有重叠但独特的风险，且使命是不同的： 机密性，完整性和可用性 人和环境的可靠性和安全性
2	IT和OT文化太不相容，太独特，无法制定和实施单一或共同的网络安全战略	以工程为中心，“适合目的”；以信息为中心，“通用灵活”；但IT和OT文化在以资产为中心的组织中同步发展
3	套用IT网络安全设计和管理方法来保护OT、IIOT的计划，满足其需求	一种尺寸不适合所有需求。OT系统实时、事件驱动、逐个检测和响应、被动控制网络、隔离策略等，还可能涉及人员和环境安全的特定行业合规性。
4	OT和IIoT系统过于专业化和独特，无法使用现成的解决方案，需要定制来保护OT系统	不排除使用标准的IT网络安全系统，但须遵守OT治理和设计，以满足特殊需求。以信息为中心且对功能的物理影响越小，使用主流IT解决方案的可能性越大
5	OT网络隔离的保护手段已经消亡	如军事和情报或高风险金融系统，仍然采用隔离 公用事业，石油和、天然气以及航空航天等行业中，存在单向数据流
6	基于云的网络安全解决方案和网络安全响应自动化，对OT和IIoT系统不现实	基于云的能分析全球生产流量，区分系统中的正常与异常行为。如对事件驱动系统的连续测井进行实时密集处理，需使用此方法来区分可能是威胁因素造成的特定异常与机械故障，还是意外配置导致的简单异常？

安全现状

安加互联 SECADDIOT

传统IT和OT环境之间的安全功能差异

摘自NCCIC和ICS-CERT

安全功能	IT	OT
防病毒和移动代码	易于部署和更新。用户可以自定义控制，可以基于资产或基于企业	内存要求会对ICS产生影响; 组织只能通过售后解决方案保护遗留系统; 通常需要“排除”文件夹以避免程序隔离关键文件
补丁管理	容易定义; 企业范围内; 远程和自动化	成功安装补丁的时间表很长; OEM专用; 可能“破坏”ICS功能; 资产所有者需要定义可接受的风险
技术支持终身	一生两到三年; 多个供应商; 无处不在的升级	10至20年; 通常是同一个供应商 产品报废产生了新安全问题
测试和审计	使用现代方法; 系统通常具有弹性和健壮性来处理评估方法	调整系统测试; 现代方法可能不合适; 设备在测试过程中可能容易失效
更新与替换	定期和有计划的，与最小使用周期一致	战略调度，影响生产的重要过程
资产分类	常见且每年进行一次; 结果推动了支出	仅在有义务时执行; 难见非实质资产的准确库存; 资产价值与适当对策之间的脱节
事件响应和取证	易于开发和部署; 一些监管要求; 嵌入技术	专注于系统恢复活动; 取证程序不成熟（超过事件重建）; 需良好的IT / ICS关系
物理和环境安全	范围从差（办公系统）到好（关键IT运营系统）	通常对关键区域非常好; 成熟度因场地设施而异
安全系统开发	整个开发过程的一部分	不是开发过程的组成部分; 供应商正在成熟但速度比IT慢; 核心/主打ICS解决方案难以安全性进行改造
安全合规性	取决于部门的最终监管监督	具体监管指导取决于行业

框架对标

框架/规则	评价
欧洲议会和欧盟委员会2016年7月6日2016年版第1148号指令（EU）	此框架不论是在欧盟内外运营的组织都必须参考，尤其是对于提供重要服务并严重依赖信息通信技术（ICTs）的行业而言，例如能源、交通运输、水力、银行业、金融市场基础设施、医疗保健和数字基础设施等行业。
Industrial Internet of Things Volume G4: Security Framework	当制定安全策略并将其扩展为更广泛的IoT时推荐此框架，为如何制定符合IoT / OT计划的安全策略提供了详细的架构建议。
SCADA Cybersecurity Framework 国际信息系统审计协会ISACA发布	该框架利用了OT领域主要行业供应商的合作，十分详细。希望专注于OT安全领域而非更广泛的IoT的SRM领导者应考虑该框架。
ISA/IEC 62443(ISA-99) 国际自动化协会ISA	ISA/IEC 62443是OT组织工业控制系统安全性方面公认的全球标准之一。帮助OT组织提高其数字安全性以及其流程和SCADA环境的安全性。
Cybersecurity Framework NIST	CSF为OT组织提供了共同的分类和机制： 描述当前的网络安全态势、描述网络安全目标状态、在持续和可重复的过程中确定并优先考虑改进机会、评估目标状态的进度、就网络安全风险问题在内部和外部的利益相关者之间进行沟通
Securing Your SCADA and Industrial Control Systems 美国Technical Support Working Group	该标准对工业控制系统进行概述，旨在为安全从业人员提供指导，包括管理控制、架构设计和安全控制等方面。

To-Be

1. IT/OT一体化安全治理
2. IT/OT一体化安全政策框架的构建与加强
3. 根据重要程度识别和管理OT资产
4. 保证OT访问控制和数据安全
5. 持续监控OT安全、预警和事件监测、有效性验证
6. 检测方法的维护和测试
7. 响应和恢复计划充分考虑到OT特异性
8. 定期OT风险评估

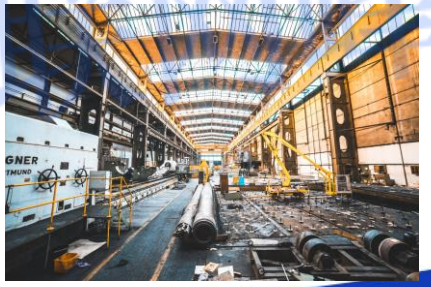
差距分析

安加互联 SECADDIOT

1. 缺乏适当的OT安全治理、运营模型，以及工程、IT和安全部门之间角色和职责的明确定义。
2. 缺乏对OT系统、组件（资产）及其配置和连接模式的正确识别和管理。
3. 生产控制和自动化领域缺乏业务连续性和灾难恢复。且涉及备份和恢复过程以及事件管理。
4. 缺乏安全架构以防止关键资产轻易渗透。如网络分段、OT基础设施访问管理和漏洞补丁管理等。
5. 有限的检测和监控机制。OT人员被用来对生产环境中的异常情况（而非安全）进行警报和反应。
6. 缺乏安全管控的第三方管理和治理，如维保OT设备（PLC、RTU）的第三方后台审计和远程访问。

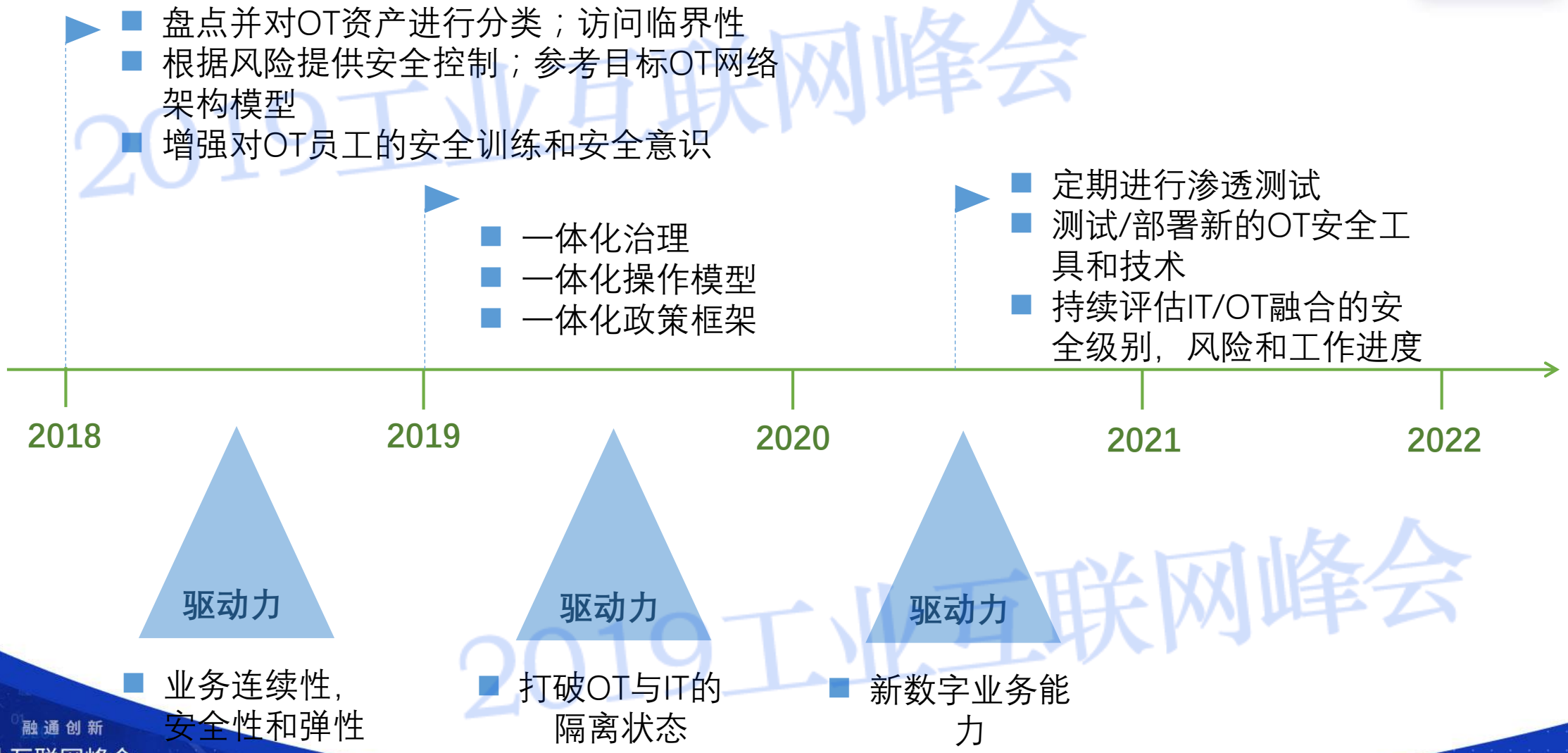
常用策略

问题	建议
缺乏对安全状态和资产的可见性，对管理和优先处理哪些资产，以及如何执行操作认知不清。	• 绘制出IIoT体系结构，并制定全面且记录完整的资产清单，以便在系统操作中进行资产安全优先级排序和风险分析。
对IIoT安全性的特定要求不确定，所以不去解决这些要求，或者采取不适合IIoT要求的IT安全措施。	• 通过使用有效、高回报的安全对策（如白名单和远程访问控制），基于风险资产优先级采取安全控制。
解决合规问题十分复杂且要求大量人力。如果解决问题缺乏充分准备，以无组织、临时的方式进行，可能会破坏和干扰业务。	• 引入政府和标准的外部指导，制定合规的安全实践，不断审计，保持公司政策、行业协会和最佳实践的内部合规性
许多旧的工业协议是专有的，未考虑到现代威胁和安全架构，造成了互操作性和安全性方面的挑战。	• 采用与技术无关并能跨异构系统部署的安全控制，以获得对支持协议集成的系统活动统一视角。

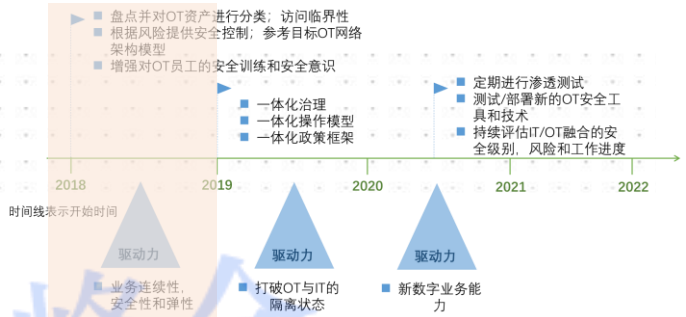


实施路径

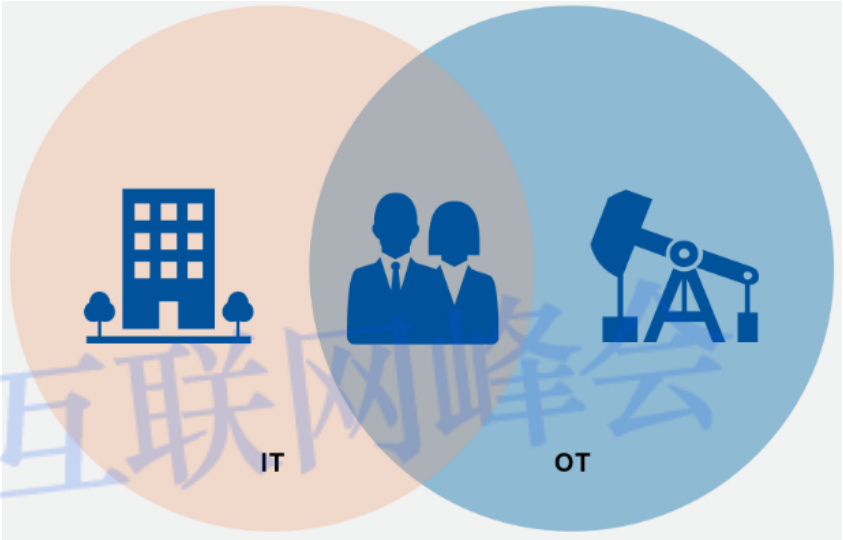
SANY 集成IT和OT安全和风险管理战略路线图



实施路径-短期

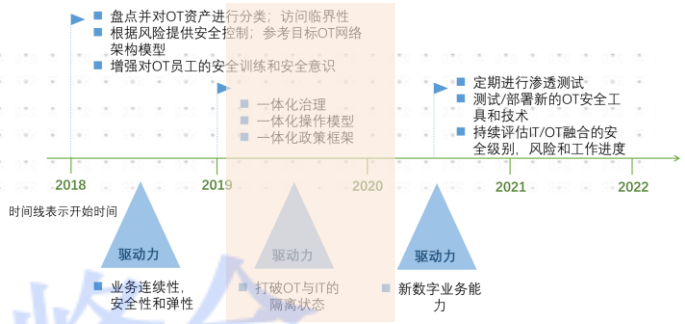


1. 提供安全意识和培训。
2. 组建统一的IT / OT安全治理机构。
3. 对OT资产进行盘点和分类，包括设备，操作，软件，网络和人员。分析这些资产之间的互连和依赖关系。
4. 定义各类OT资产的安全要求，及所需的安全服务。
5. 定义目标OT网络架构参考模型，包含：网络细分、身份和访问管理、应急计划备份等、漏洞管理、远程访问（包括特权和普通访问）、安全监控、第三方管理、补丁管理、事件响应
6. 针对目标架构模型进行安全评估、差距分析，确定补救计划并启动执行。检查：
    1. 不安全的远程访问实现
    2. 虚拟局域网（VLAN）使用不当（应在网络分段中检查）
    3. 弱网络接入点自带设备（BYOD）安全策略
    4. 不受信任的云托管环境和SLA的强化不足以实现关键的ICS功能
    5. 作为分层式深度防御战略的一部分，OT网络监控的采用不足
    6. 故障后有效OT系统恢复到安全状态的能力有限
    7. 不正确的物理访问和闪存驱动器的使用
7. 实施风险监控方法和工具，以确保安全计划进度的可见性。
8. 根据优先级对OT进行快速实用的安全控制，以查看即时结果



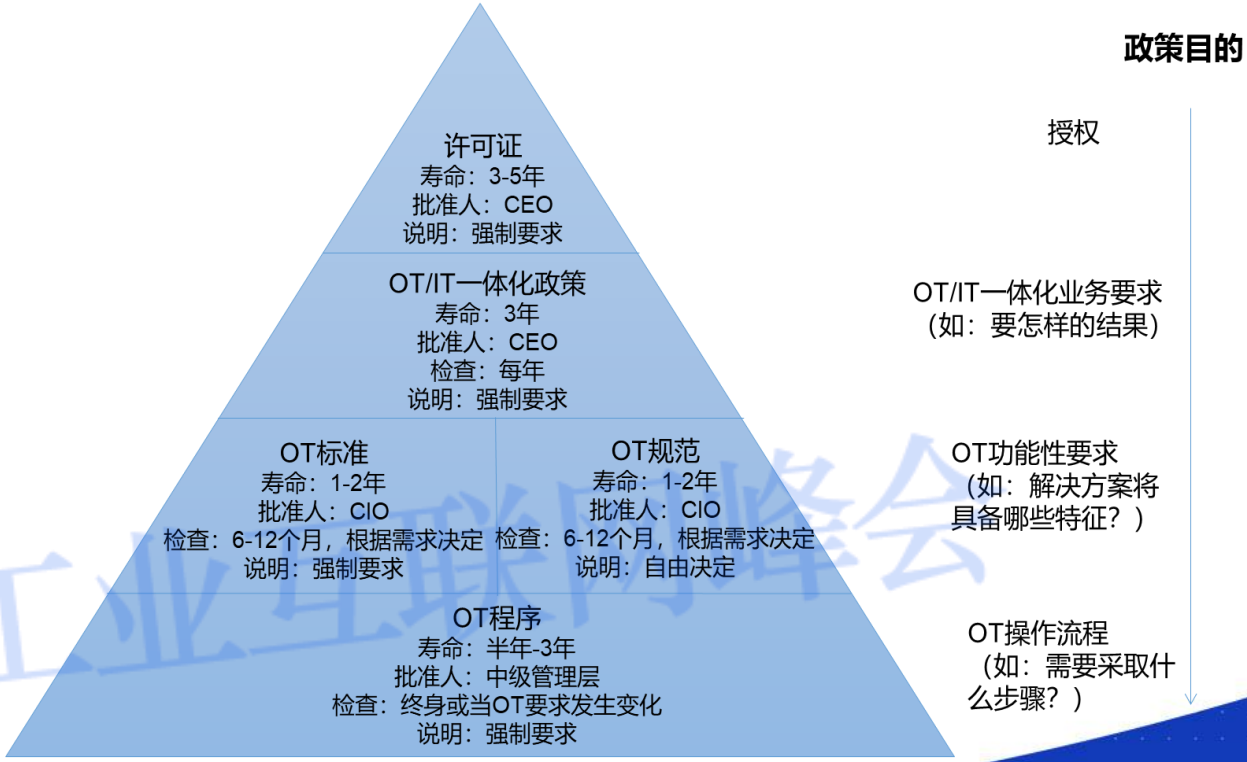
IT和OT的统一安全治理主体

实施路径-中期

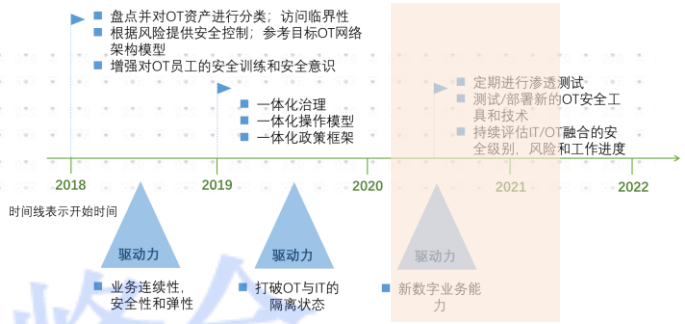


1. 根据关键战略问题选择适当的治理模型：
   1. OT安全功能的范围应该是什么？
   2. 该模型将提供什么流程？
   3. 什么技能至关重要？
   4. 需要哪些技术变更？
2. 定义通用的IT / OT安全操作模型，建立联合角色，职责，流程和系统，以支持日常OT和安全操作。描述如何创建和提供价值。支持更灵活，更灵敏的运营模式。
3. 定义现有安全策略框架以包括OT安全性细节。通过利用通用IT / OT安全操作模型并确保策略易于访问和组织，自定义和适应现有的针对IT和OT角色和职责的安全策略。
4. 通过下一代防火墙实施IT / OT网络分段和逻辑分离计划。OT设置中存在许多架构约束，可能需要重新设计以优化网络分段。
5. 提高OT安全流程的成熟度级别，例如变更管理，访问管理和事件管理。
6. 利用新工具和新的OT安全产品，来增加OT环境的可见性和控制，以帮助识别新OT资产变化。

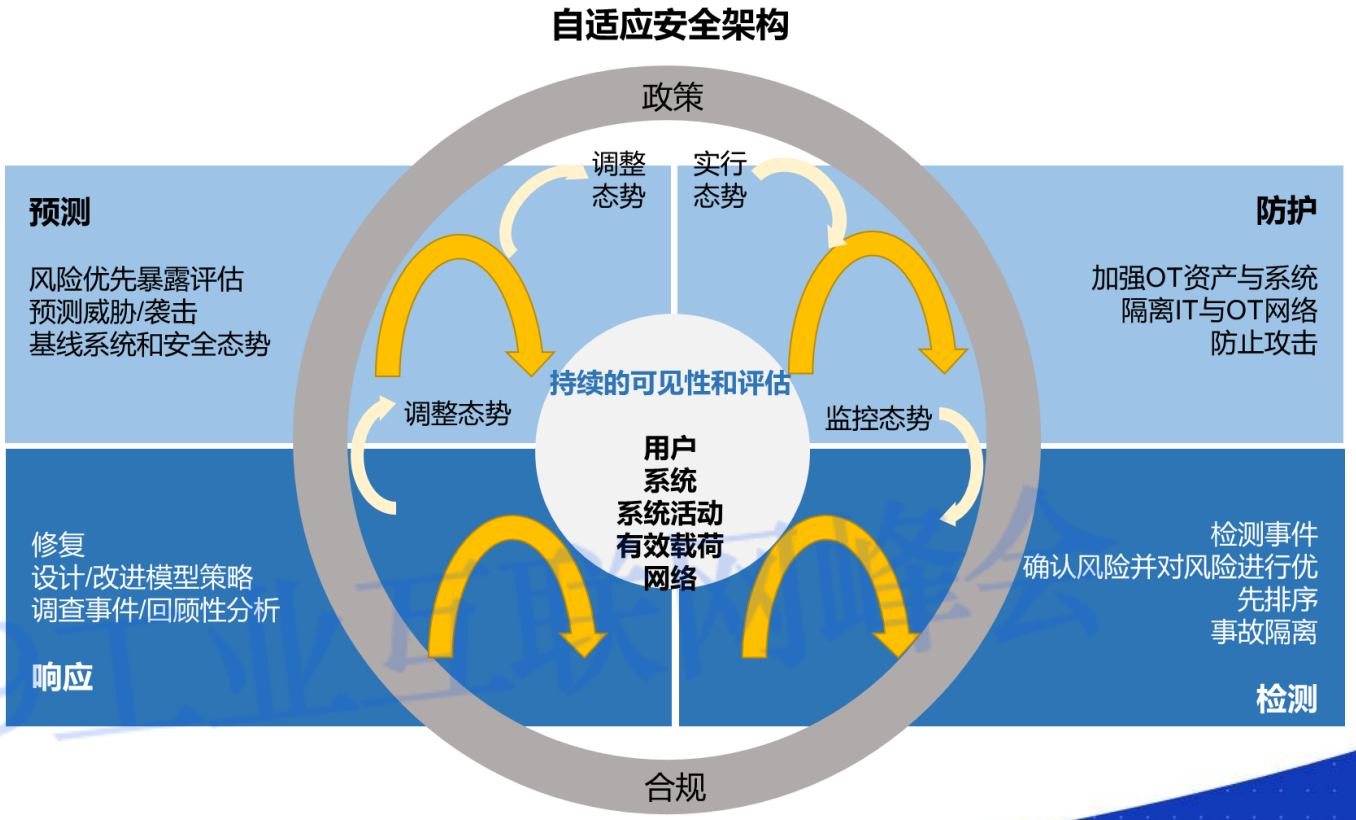
IT/OT一体化安全政策框架



实施路径-长期



1. 定期测试（外部渗透测试，内部测试，OT漏洞评估）。
2. 进行概念验证和测试新的OT安全工具和技术，并在有意义的时候部署这些工具。
3. 重新配置系统
4. 测量和监控OT安全流程及其有效性。
5. 持续评估实施计划范围内的集成IT / OT安全级别，风险和工作进度。
6. 根据需要修改人员配置。
7. 确定可能影响OT功能的基础架构和系统的潜在变化。
8. 持续解决威胁形势的变化。



工作进展

- **成立专业公司**
  - 投资成立安加互联，专注工业互联网安全领域发展
  - 应急团队：突发事件应急管理规范、平台事件应急演练实施方案

- **参与项目课题**
  - 数据驱动的工业互联网安全保障体系建设与应用示范；
  - 工业互联网可信服务关键技术标准试验验证；
  - 工业互联网安全监测与态势感知技术手段建设；
  - 工业互联网突发事件应急协作指挥手段建设和应用；
  - 工业互联网安全标准体系与试验验证环境建设；
  - 面向中小企业的工业互联网安全公共服务能力建设等。

- **标准制订**
  - 牵头拟订GB/T-工业物联网平台安全要求及评估规范--//TC260-SWG-BDS组

关键技术研究（自主可控+边缘计算、人工智能、区块链等）

- 合作成立物联网网络安全应急技术国家工程实验室
- 边缘侧漏洞挖掘
- 标识解析安全，如网联标识防伪造，地址解析返回可信等
- APP应用安全
- 事件应急、共享与通报

工业互联网产业联盟
Alliance of Industrial Internet

Thanks

彭卓

2019年2月22日

智联赋能　融通创新

2019 工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019