案例 1

华为技术有限公司

基于主动防御的电子制造基地安全方案

一、项目概况

1. 项目背景

该电子制造企业既有自己的工厂又有众多的外协工厂，且外协工厂分布式在全世界多个国家。目前该企业已经实现“云上办公”和“生产管理系统上云”，企业各园区之间采用企业专网进行通信，生产基地和外协厂基本上通过租借的专网进行通信，部分供应商采用 TLS VPN 进行通信，厂区内部还根据不同的应用场景采用不同的通信方式，除了有线通信之外，还有 WiFi 和 eLTE 等无线通信方式，工厂和外协工厂之间通过该企业的云平台实现生产协同

正是企业制造智能化和管理 IT 化的水平比较高，使其制造业务的面临安全挑战非常大，且制造业务的安全要求和公司的通用 IT 安全要求有所不同，前者重点是保障业务的连续性和可靠性，后者重点是确保数据的安全性和可控性。因此制造业务部门在基于公司通用的 IT 安全部署和安全管理之上，提出制造基地独立的安全防护体系和安全管理机制。

2. 项目简介

该电子制造基地的安全实施，以保证业务连续性为目标，采取管理约束和技术保证双管齐下的策略，根据生产实际述求，本着先改造 IT 后增强 OT 的安全实施理念，提出了被动的静态防御和主动防御相结合的安全部署方式， 通过严

格的安全隔离和访问控制机制等传统的静态防御手段，为生产基地构建独立的网络安全防护围墙；在此基础上，引入主动防御的安全工具，通过先进的安全防御工具，来弥补攻防的不对称问题，提高应对未知威胁的反应能力和预警能力，确保工控系统运行环境的安全性。

3. 项目目标

项目的安全目标是确保业务的连续性，避免因攻击事件造成生产线的停机。项目安全方案的前提条件是不对工控系统的可用性、实时性和可靠性产生任何影响，制造基地的数据安全保护已经由公司的云平台安全保护体系进行保护，不在本项目考虑之内。

目在增强传统的静态防御手段基础上，采用“先提高 IT 免疫力，后增强 OT 安全”的思想，分两期部署主动安全防御系统：第一期主要给制造基地 IT 网络和 OT 边缘区增加主动防御，建立数据交换区来隔离安全风险，车间内的数据以安全监控为主；第二期，将主动防御系统的行为建模能力扩展到 OT 网络和工业协议，实现 OT、IT 和 CT 网络的全方位监控。通过这两期的安全方案部署，加强了网络安全纵深防御和联动协防能力，建立有效应对 APT 攻击防御的全网协同的智能“自我免疫”的安全防御体系，实现对全网威胁的态势感知。实现网络安全“智能检测”、“智能处置”和“智能运维”，从被动、单点防御到主动、整网防御，从人工运维到智能运维。

二、项目实施概况

1.项目的面临的挑战和对策

- **主要挑战**
  终端安全手段难以部署，停机维护不可接受；生产线无人值守，工控设备高自动低智能；生产网络是专用的封闭系统，与外部情报共享不方便；另外面对 APT 高级持续威胁和 WannaCry 等这种新型勒索病毒，传统单点和静态防护手段常常束手无策，等到攻击事件爆发时才知道已经为时已。
- **应对策略**

采用不依赖终端的网络旁路部署方案；威胁检测不依赖威胁情报，而是基于 AI 和业务环境自适应的智能检测与响应技术；通过建立数据交换区，最大限度避免外部攻击和威胁直接进入生产网，部署诱捕网络，与智能检测与响应系统进行联动，提高对未知威胁的攻击意图分析能力和全网的动态安全响应能力。

2. 项目总体架构和主要安全部署策略

项目采用静态安全防护和主动安全防御相结合的方案，安全解决总体解决方案示意图如图 1 所示，项目采取下面的安全部署策略：

- 多层次的安全隔离措施：在企业的大专网中，划分一个生产专网，将办公网络和生产网络区分开，在生产网络中再进一步划分若干个子网；生产区根据设备和业务特点，划分不同安全区域，每个区域对应一个网络子网。通过严格的安全隔离措施，来弥补工控系统自身防护能力弱的问题。

- 严格的网络访问控制：每个子网分配私有 IP 地址段，子网之间通信需要通过网关进行访问控制；设备接入生产大专网时，采用设备和用户的双因子鉴权机制，设备需要先通过云的合规性和杀毒检测等常规性健康检查之外，进入生产区还需要进行未知威胁的检测；各生产子网的访问权限由云平台统一管理，实现全局访问监控。

- 定义数据交换的专门安全隔离区域：在生产大网前面，专门设计一个安全隔离区，作为 OT 网络和 IT 网络之间的数据交换的唯一场所，也是新来的设备和文件进入 OT 网络前的健康检查区域，设立该安全隔离区目的是尽量将外部攻击阻止在该隔离区，避免其进入 OT 网络。

- 部署主动防御系统：在保留原有的防火墙和 IDS 的安全能力上，叠加一个动态的安全防护系统，来提高安全检测和响应能力，并在安全隔离区专门设立一个诱捕网络，通过诱捕网络来分析攻击意图

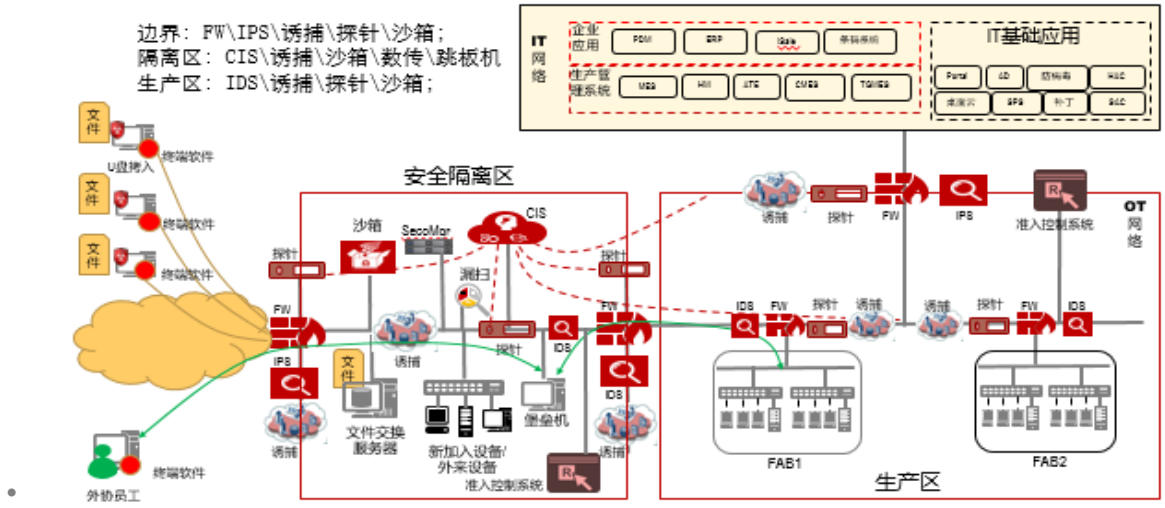

图 1 主动防御系统的部署总体示意图

. 3 方案的关键组件

该项目的主动安全防御方案均采用华为的安全产品进行部署，关键组件之间的关系如图 2 所示：

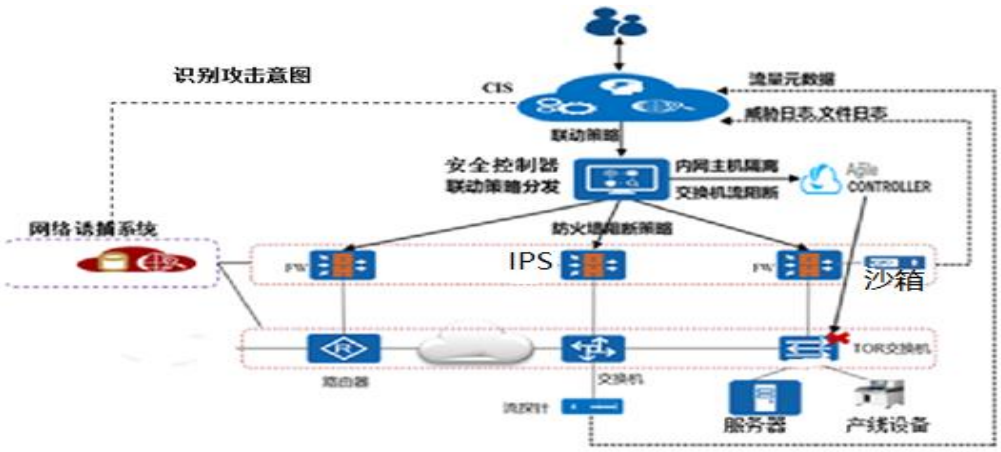

图 1 主动防御系统各组件之间关系图

- CIS：基于 AI 技术的智能安全分析器，通过检测探针上报的流量特征和日志、终端行为等数据分析，识别未知威胁，并联动安全控制器下发安全策略
- SecoManager：智能的安全控制，实现安全设备和网络设备的统一调度，提高全网联动能力，安全控制器接受安全分析器的安全处置措施，编排成为设备可执行的策略，并自动下发给安全执行器进行执行，是全网的主动防御系统的安全资源调配中心。
- 安全执行器，包含防火墙和 IPS，一方面向分析器提供安全分析的数据输入，另一方面接收控制器下发的具体指令，执行安全策略的实施，实现安全处置闭环，同时对接 CIS，实现本地信誉升级。
- 探针：流量探针部署在各子网关口处和网络边界处，探测流量的行为特征和用户行为，日志探针采集交换机、防火墙和 IPS 的安全日志，并上报 CIS。
- 沙箱：检测未知的恶意代码，与防火墙和 IPS 具备联动功能，防火墙和 IPS 从流量中提取可疑文件，送到沙箱检测。 所有新文件和新设备都需要进行沙箱检测。
- 网络诱捕系统：向攻击者呈现虚假资源，诱导攻击，把攻击引入蜜罐，与攻击者交互，通过某些技术手段，确认攻击意图，以便采取对应措施。
- 堡垒机：对各种资源的帐号、认证、授权和审计的集中管理和控制，部署在安全隔离区，所有对生产区的设备运维，都需要堡垒机进行集中管控。

4.方案部署的关键要点

1.对原有的防火墙和 IPS 进行升级，在保留原有的安全防护能力基础上，使其能支持与安全分析器、安全控制器和沙箱等进行联动，成为安全执行器。

2、所有子网的边界处部署流量探针，防火墙、IPS、路由器和交换机部署日志探针。

3. 在安全隔离区安全部署一台 CIS 和 SecoManager，CIS 和生产区内外的探针进行对接，并和 SecoManager 进行联动，由 SecoManager 来统一调配安全隔离区和边界处的安全资源。

4.在安全隔离区部署专门的诱捕网络，禁止在生产网络的系统中安装 TeamViewer 等远程控制软件，所有生产网络和外部网络的数据和文件都需要经过诱捕网络。

4.在安全隔离区专门部署文件交换服务器，同时部署沙箱，所有文件进入生产网络之前，需要先经过常规 IT 检测、诱捕网络和沙箱的检测，然后才能上载在文件交换服务器，只有经过安全检测的设备才能在文件交换服务器进行下载。

5. 在安全隔离区部署堡垒机和跳板机，通过跳板实现，外部的运维方对生产区进行运维时，需要先经过跳板机，登录到堡垒机进行用户行为审计，然后才能运维生产设备。

5.方案的应用

- 场景 1：U 盘管理/文件传输时的安全保障

如图 3 所示，U 盘拷入文件服务器的文件需经过主机病毒扫描，网络防火墙病毒扫描，沙箱未知病毒、木马程序扫描，同时经过漏洞扫描系统漏扫测试。在文件传输过程还要经过诱捕系统进行诱捕异常扫描、嗅探侦测网络行为的检测。

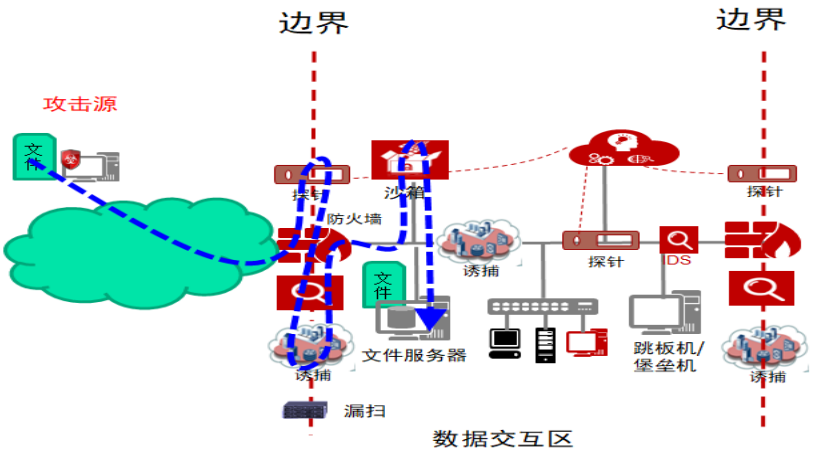

图 3　U 盘和文件的传输管理时的安全保障

- 场景 2：外来供应商运维管理或者外来电脑管理

如图 4 所示，外来厂家的运维管理，首先要登录到数据交互区的跳板机，通过跳板机再登录堡垒机，运维人员行为经过堡垒机审计，对于非法远程控制软件行为进行禁止。

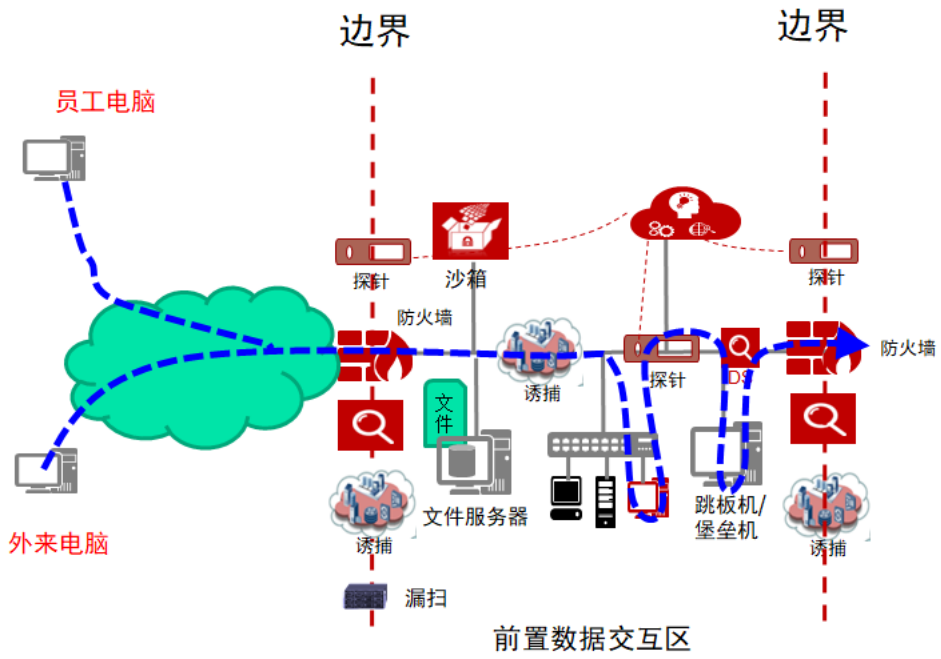

图 4　设备运维时的安全保障

- 场景 3，新机台接入网络的安全保障

如图 5 所示，新机台接入生产区之前需要先接入数据交互区，机台潜伏的病毒经过数据交换区的异常流量检测模型，诱捕系统识别并控制在数据交换区；在数据交互区 48 小时后，检测异常或者学习到正常基线，无风险的机台正式接入生产网络区。

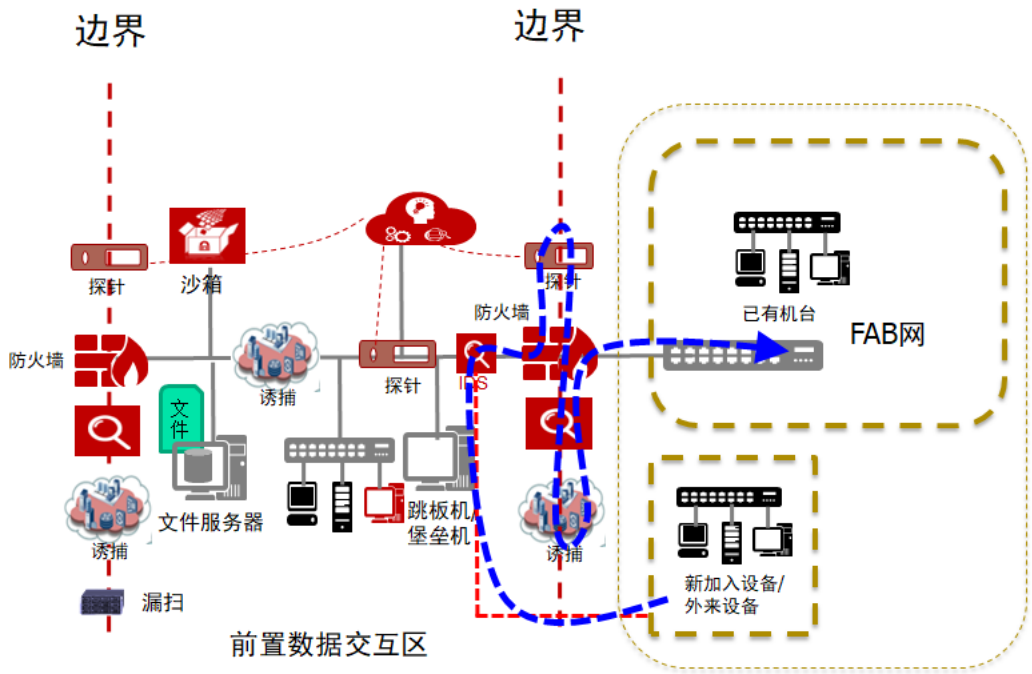

图 5，新设备加入生产区的安全保障

- 场景 4，机台和设备的准入控制

为了防止假冒机台和设备接入网络，或者为经过健康检查的设备和机台非法接入网络，需要进行准入控制，新设备在数据隔离区 48 小时后，需要经过准入控制检查后才能接入生产区。

如图 6 所示，部署网络安全准入系统做终端和机台的准入控制，终端、机台接入前的健康度检查、补丁安装巡检、合规检测等。各设备接入准入系统时，需要强制进行漏洞修复，对于特定终端，如哑终端，无法进行正常的健康检查，由准入系统进行白名单检查。

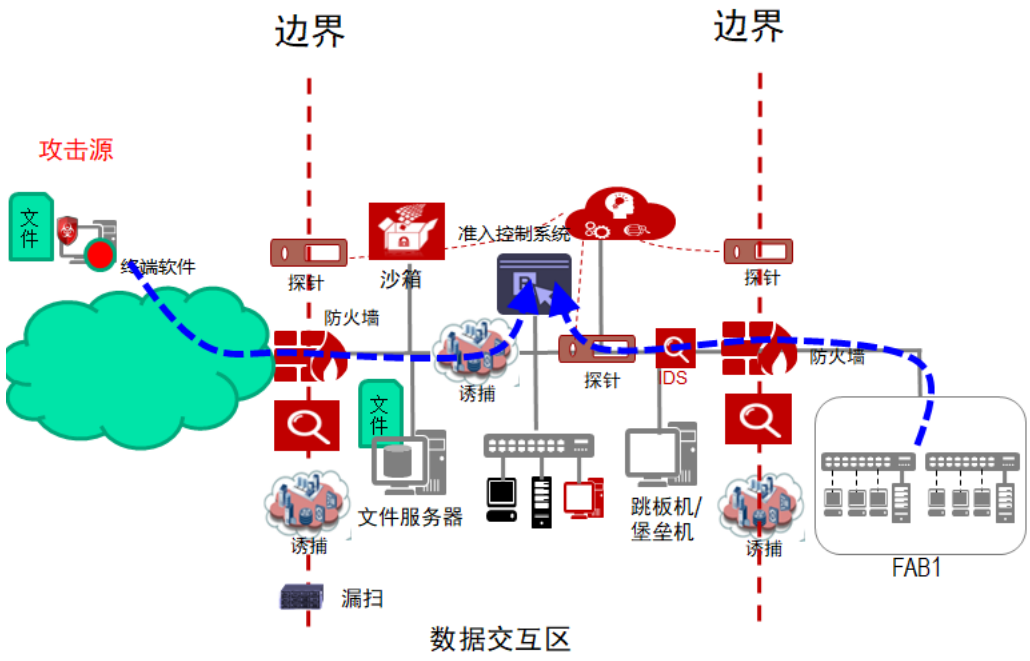

图 6，设备的准入安全控制。

- 场景 5，生产区间的行为检查和隔离措施

新机台之间有相互感染风险，一台机台感染病毒，会传播到其他机台，攻击者会利用机台已知漏洞进行攻击。

如图 7 所示，机台之间通过交换机 Muxvlan 技术进行隔离，不需要传输数据的机台之间进行隔离；需要进行交互的机台交互数据通过防火墙进行隔离，通过漏洞检测和防护，过滤已知漏洞。

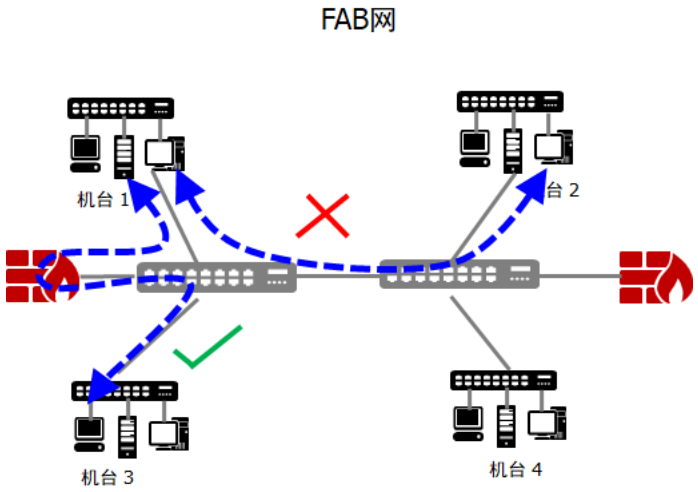

图 7，生产区的设备的隔离措施

三、下一步实施计划

1. 将主动防御系统进一步延伸到 OT 网络中，主动防御系统的行为建模能力扩展到 OT 网络和工业协议。

2.推广该安全实践经验和解决方案，将方案推广到其他行业的制造基地，目前已经和某芯片先进制造企业进行联合研究，将方案部署到其芯片制造基地

四、项目创新点和实施效果

1. 项目先进性及创新点

- 首创提出安全隔离区是新文件和新设备进入生产区 OT 网络的唯一通道。
- 基于 AI 建立行为基线，检测未知攻击，通过构建安全威胁态势感知、安全策略智能管理和网络诱捕系统，形成“三位一体”的主动防御体系，提高未知威胁感知能力和响应能力；
- 无需对现有网络和设备进行大规模改造，主动防御体系不影响现有生产网数据通信，项目方案可以复制性强，可以复制到其他行业的生产基地。

2. 实施效果

安全方案全面覆盖了工业互联网 TOP10 安全风险，具体风险处置应对措施如下：

No.	安全风险	应对方案	残余风险
1	外来 U 盘带入病毒风险，供应商或者员工使用 U 盘拷贝文件，容易遭受病毒或摆渡攻击，将威胁带入 IT 或 OT 网络。	所有U盘数据只能先拷贝到安全隔离区，通过沙箱对已知和未知威胁检测通过后才能传入 IT 或 OT 网络	有病毒漏报风险，如有漏报，还有事中检测的方案

No.	安全风险	应对方案	残余风险
2	外来电脑带入病毒风险，供应商或者第三方运维人员通过外来便携电脑直接接入网络，将威胁带入 IT 或 OT 网络。	所有外来电脑只能接入安全隔离区，通过安全健康检查后才能使用	有病毒漏报风险，如有漏报，还有事中检测的方案
3	新机台带入病毒风险，供应商新机台存在病毒，接入 OT 网络后扩散到整个网络。	供应商的新机台需要接入安全隔离区运行规定时间（通常建议三个月），确认安全无毒之后才能正式切换到直接接入 OT 网络	可能存在长时间潜伏的威胁，还有事中检测的方案
4	双网卡办公电脑风险，办公人员为了方便，同一台电脑同时接入 IT 和 OT 网络，容易成为跳板攻击 OT 网络。	禁止采用双网卡同时接入 IT 和 OT 网络，应通过远程桌面连接到部署在 IT 网络的桌面云进行日常办公操作	可能存在漏网之鱼，还有事中检测的方案
5	工控操作系统老旧风险，工控计算机所使用的系统多为 Windows 或 Linux 的早期版本，存在漏洞容易被攻击。	在网关防火墙处针对 OS 已知漏洞部署 IPS 规则（虚拟补丁），防范跨防火墙针对已知漏洞发动的网络攻击	可能 IPS 规则库更新不及时，如条件允许可考虑及时升级补丁
6	工控软件系统老旧风险，现网多数工控软件系统版本老旧，存在漏洞容易被攻击	在网关防火墙处针对 OS 已知漏洞部署 IPS 规则（虚拟补丁），防范跨防火墙针对已知漏洞发动的网络攻击	可能 IPS 规则库更新不及时，如条件允许可考虑及时升级补丁
7	运维人员特权操作风险，运维人员误操作、违规操作或恶意操作易导致系统异常或敏感信息泄露等问题，难回溯。	在特定区域接入安全隔离区，通过登录部署在安全隔离区的堡垒机对 OT 网络设备进行运维操作	可能存在无需登录堡垒机也能运维的情况，如果存在需要优化安全策略
8	装远程控制软件风险，在系统中安装 TeamViewer 等远程控制软件，容易绕过边界安全防护措施，带来安全风险。	原则上禁止在 OT 网络的系统中安装 TeamViewer 等远程控制软件，避免绕过边界安全防护措施，带来安全风险；如需远程运维，建议采用 VPN 接入安全隔离区，通过登录堡垒机对网内设备进行运维操作	可能存在漏网之鱼，可以可考虑在相应边界防火墙设置策略阻断相关远程连接端口
9	缺乏合理安全区域风险，生产区网络没有划分合理的安全区域并实施边界保护，病毒一旦爆发波及整个网络。	将安全区域划分为最小单位（推荐以一个车间为单位），有病毒入侵时将威胁控制在特定区域，防止整网扩散	区域划分最小颗粒但还是扩散风险，但还有事中检测方案
10	来自外部网络攻击风险，合作伙伴网络受攻击	在与合作伙伴外部网络互联的边界部署防火墙、IPS、网络探针和诱捕系统实现该区域边界保护	可能存在安全策略配置不到位风

No.	安全风险	应对方案	残余风险
	后，做为跳板攻击 IT 或者 OT 网络。		险，建议定期评估安全策略有效性