工业安全一站式解决方案（基于等保2.0）

Moxa & 威努特

张杰，Moxa 工业安全产品经理

杨璐，威努特产品总监

工业安全部署遇到的两个主要挑战：

1. 懂安全的厂商不懂工业控制系统，不敢使用
2. 安全相关厂商各执一词，难以抉择

我们致力于提供工业安全一站式解决方案

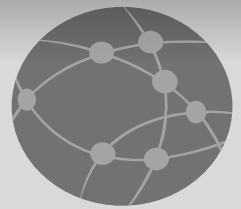
Source: Gartner, Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 29 December 2016

Moxa经营成就

Moxa 是边缘连网、工业计算机及工业网络基础建设解决方案的领导品牌，致力于**工业互联网的共同推动与实践**。

连接全球

50+Million 工业设备



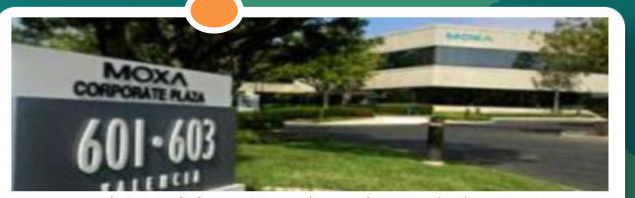
市场领先地位

串口设备连网服务器全球 **第一名**领导品牌

工业级以太网交换机亚太 **第一名**领导品牌

全球性奖项

全球布局



销售和行销总部
Brea, California USA

设计和研发总部
Taipei, Taiwan

2
企业总部

12
营运分公司

120+
经销商

34%
研发人员占比

威努特公司介绍

北京（全国总部及研发中心）
电话：010-62977816
地址：北京市海淀区上地三街9号金隅嘉华大厦F座701室/901室/906室/907室

天津（制造&研发中心）
电话： 022-25282873
地址：天津市滨海新区北塘中关村科技园大唐总部基地东区1号楼4单元201室

西安（服务中心）
电话：17782836657
地址：陕西省西安市雁塔区沣惠南路与科技二路交汇处泰华·金茂国际7号楼1203室

上海（技术&业务中心）
电话： 021-64150586
地址：上海市钦州北路1122弄89号D座10楼

广州（业务中心）
电话： 18922772413
地址：广州市越秀区东风东路836号2座2505室

成都（业务中心）
电话： 028-86529251
地址：四川省成都市高新区吉瑞三路99号1栋5单元B座1607室

北京威努特技术有限公司（以下简称“威努特”），成立于2014年，是国内专注于工控安全领域的国家高新技术企业，全球仅六家荣获国际自动化协会安全合规学会安全认证的企业之一。

威努特以率先独创的“白环境”整体解决方案为核心，研发了覆盖工控网络安全的5大类20款自主可控产品，并提供全生命周期工控安全服务。以领先的核心技术及市场优势，成功为电力、轨道交通、烟草、石油石化、市政、智能制造、冶金及军工等国家重点行业五百余家客户提供了有效的安全保障，多次受邀为中共十九大、两会、一带一路、G20等重大活动进行网络安保工作，广泛参与工控安全领域的国家和行业标准制定，得到了国家多个政府部门和客户的高度认可。

威努特始终以保护我国关键信息基础设施网络空间安全为己任，为“中国制造2025”保驾护航，为建设网络强国添砖加瓦！

威努特——专注工控，捍卫安全！

权威资质荣誉

历经五年，已通过多项体系认证，已是国内专注于工控安全领域的领军企业。

ISASecure CRT Tool 认证

公安部等保建设服务机构

信息安全风险评估服务资质

信息系统安全集成服务资质

ISO9001质量管理体系认证

ISO27001信息安全管理体系认证

ISO20000技术服务管理体系认证

中国IT产品信息安全认证证书

国家高新技术企业

国家网络与信息安全技术支撑单位

国家信息安全漏洞库技术支撑单位

工信部网络安全试点示范项目

工业信息安全信息报送与通报试点工作优秀单位

国家重大活动网络安保技术支持单位

工业信息安全应急服务支撑单位

国家工业信息安全产业发展联盟会员单位

工业安全一站式解决方案

工业网络安全的认知误区

等保2.0简介

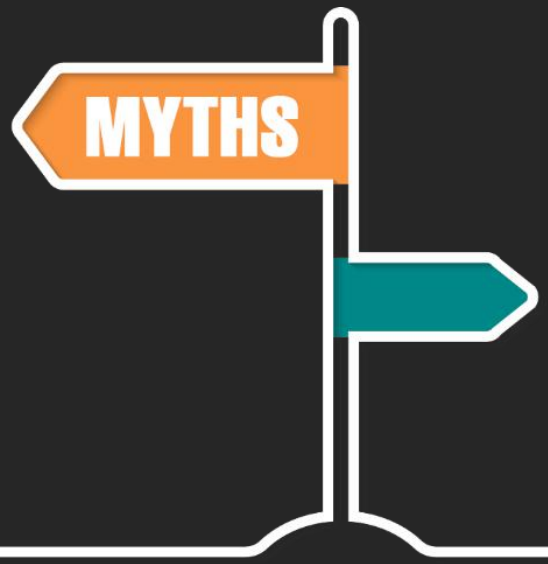
工业安全一站式解决方案

工业防火墙交换机介绍

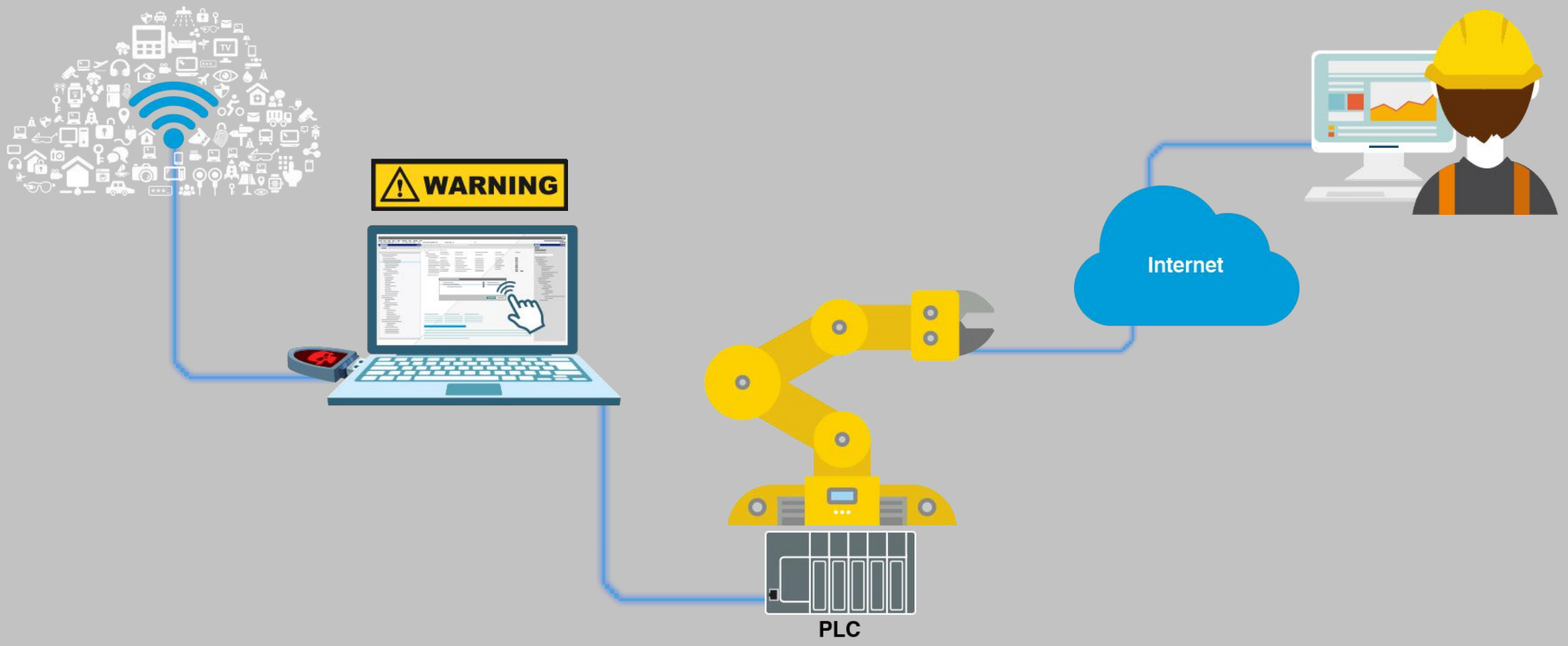
工业网络安全的认知误区

工业系统安全认知误区1

我们的系统是物理隔离的，所以，我们的网络没有信息安全的风险，很安全……

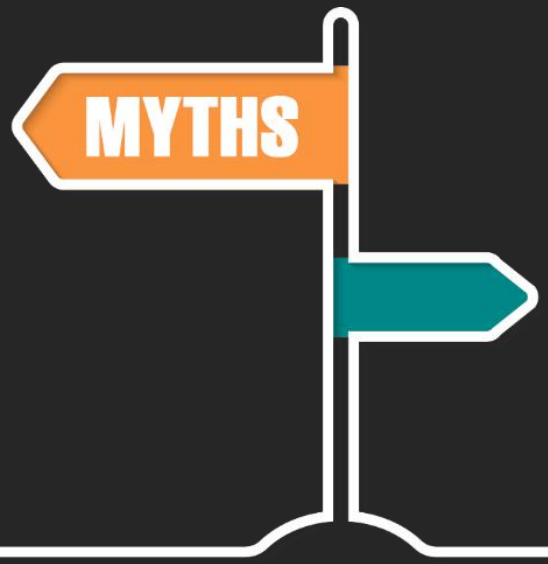


即使系统没有链接外网，也存在被侵入的风险，比如第三方的维护工程师带入的病毒和恶意程序，或者新加入系统中的设备本身就存在安全隐患（如:台积电事件）



工业系统安全认知误区 2

黑客不懂ICS，PLCs， 和 SCADA 系统。
所以，我们是安全的……



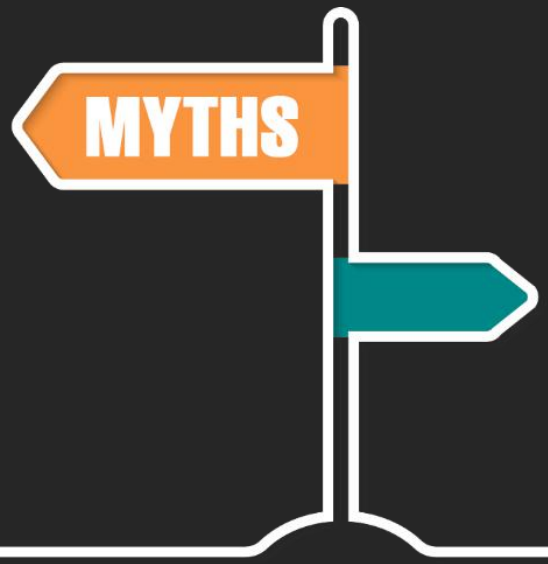
MOXA®

工控安全时间和攻击目标

年份	攻击事件	攻击目标	
2010	Stuxnet	**PLC**	(Nuclear Power Plant in Iran)
2011	Duqu	Computer/Server	(Public Utility in Multiple Countries)
2012	Disttrack/Shamoon	Computer/Server	(Oil Company in Saudi Arabia)
2014	Sandworm	**SCADA/HMI**	(Factory Floor in Multiple Countries)
2015	BlackEnergy / Killdisk	**HMI**/ Serial Device	(Power Grid in Ukraine)
2016	Industroyer	Circuit Breaker	(Power Substation in Ukraine)
2017	Dragonfly	Computer/Server	(Public Utility in US/EU)
2018	WannaCry	Computer/Server	(Factory Machines in Asia)

工业系统安全认知误区 3

就算黑客工业系统, 我们这样的小系统，不会是攻击目标的
我们是安全的.....

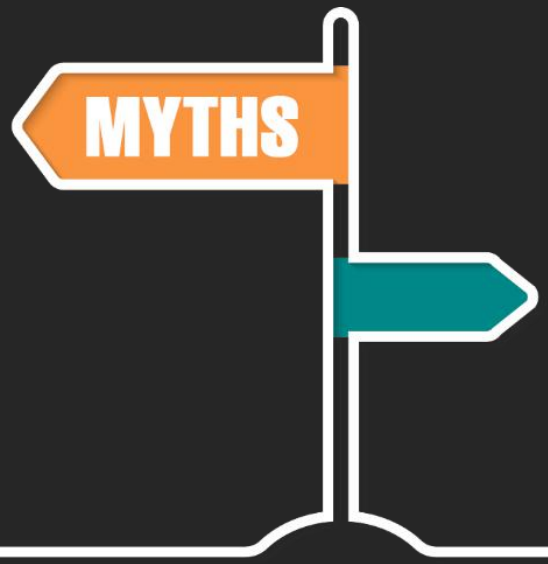


很多病毒和恶意程序针对的是通用服务器，或常用的特定产品系列，即使不愿意，也会被动成为受害者

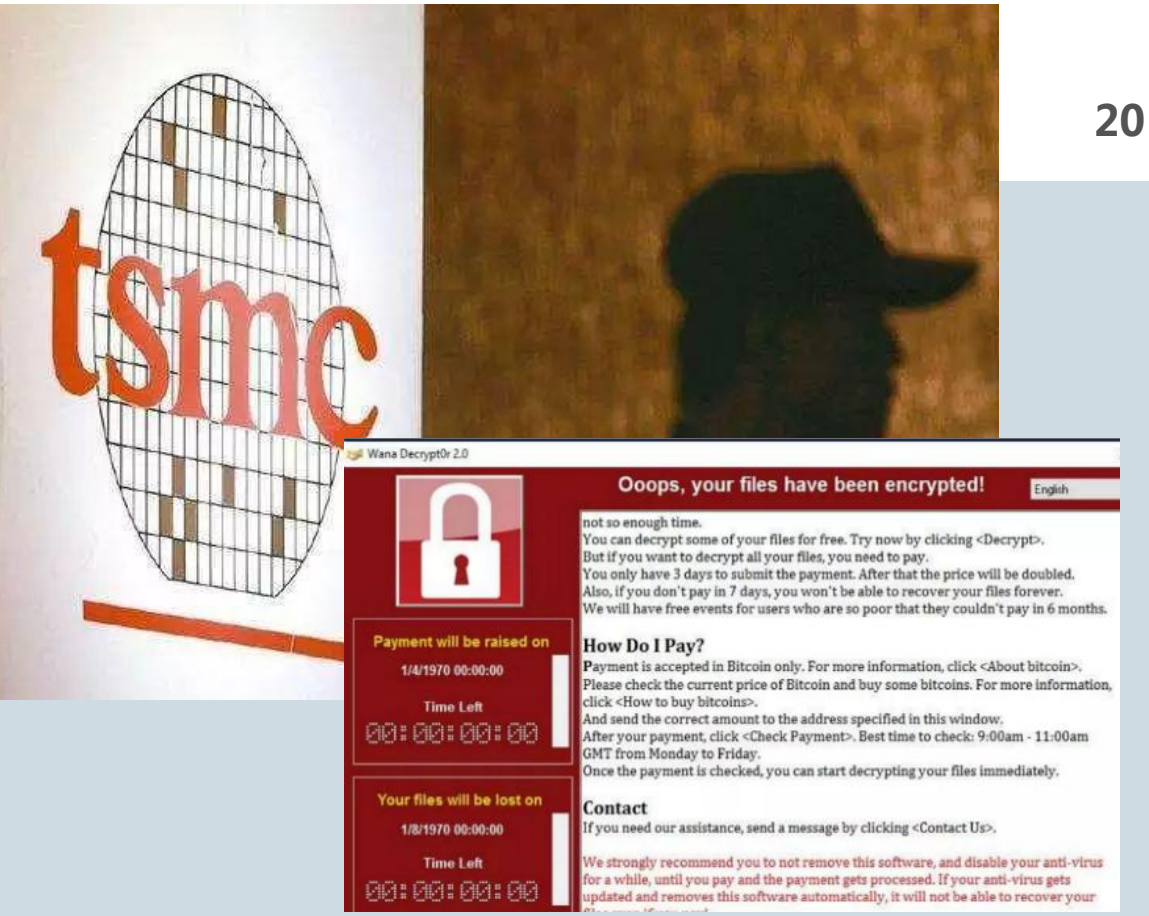
Source: 5 Myths of ICS Cyber Security – 2017, KIACS Cyber Security Conference

工业系统安全认知误区4

我们已经上了系统级的安全解决方案，我的工业系统是安全的.....



制造业工控安全事件-台积电事件



2018年8月3日，台积电中了勒索病毒WannaCry（“想哭”）的变种病毒

病毒影响范围：

- 感染的厂区包括竹科Fab 12、中科Fab 15、南科Fab 14等；

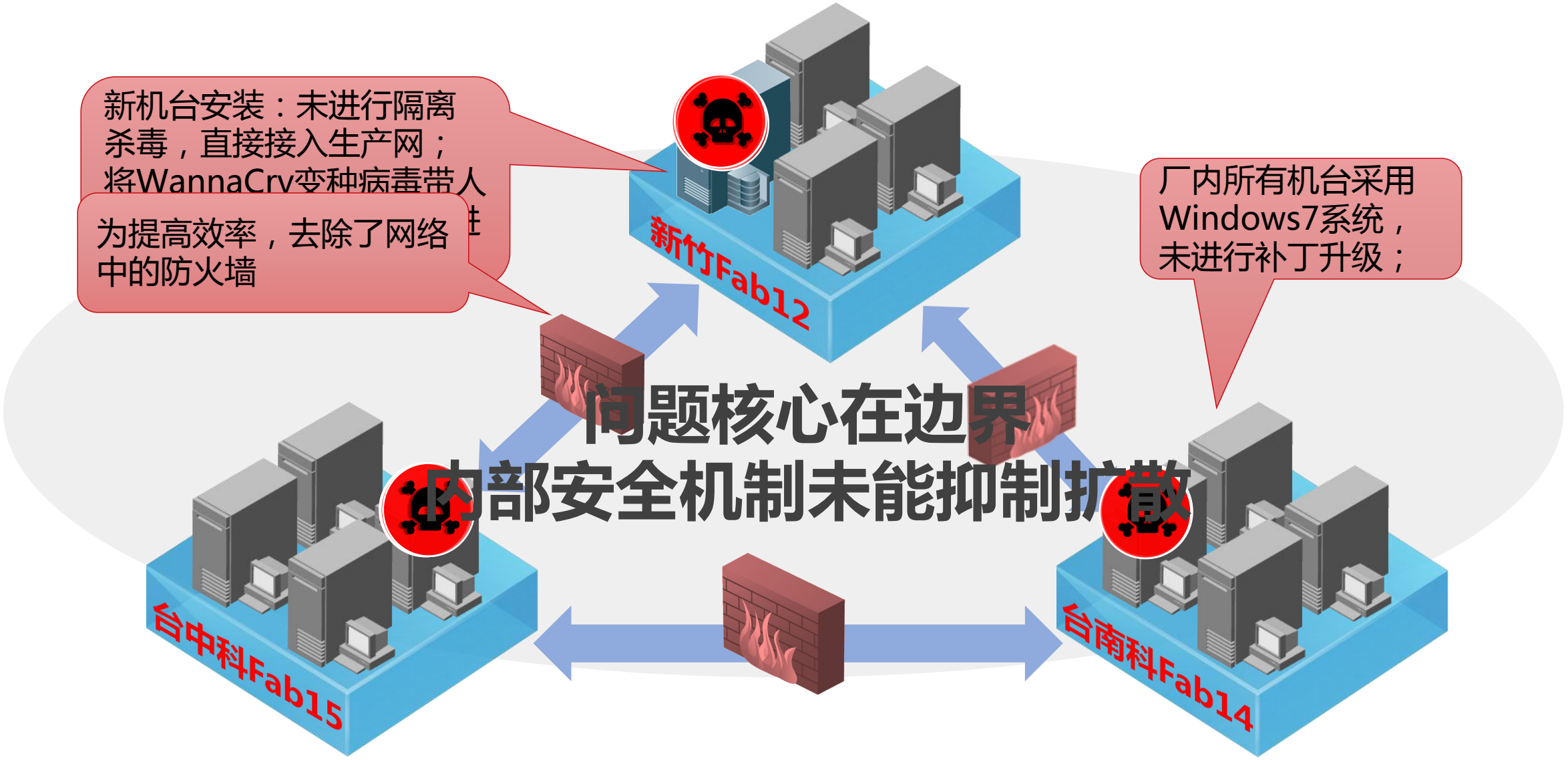
病毒特征及传播：

- WannaCry变种病毒通过445端口进行传输；
- 将word，excel，ppt，rar，pdf，txt等进行加密，无法打开；
- 电脑主机出现宕机或不断的重新启动。

感染病毒原因：

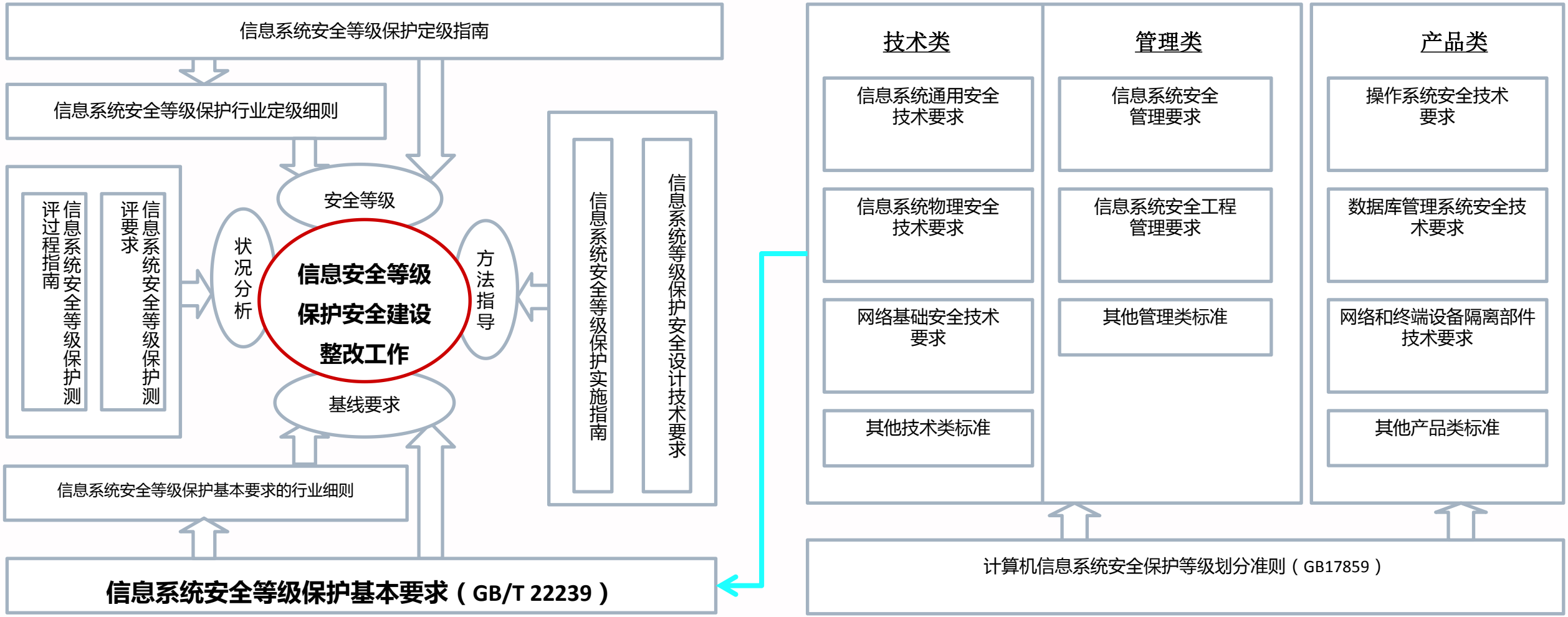
- 新台机接入时，未进行隔离，确认无病毒，直接联网；
- 所有机台生产程序放在云端，每次生产需要重新下发安装；为提高效率，取消了各厂区的防火墙；
- 设备及系统过于陈旧，未进行升级，未安装防病毒软件。

台积电中毒过程简述


新机台安装：未进行隔离杀毒，直接接入生产网；
将WannaCry变种病毒带入
为提高效率，去除了网络中的防火墙
厂内所有机台采用Windows7系统，未进行补丁升级；
新竹Fab12
台中科Fab15
台南科Fab14
问题核心在边界
内部安全机制未能抑制扩散

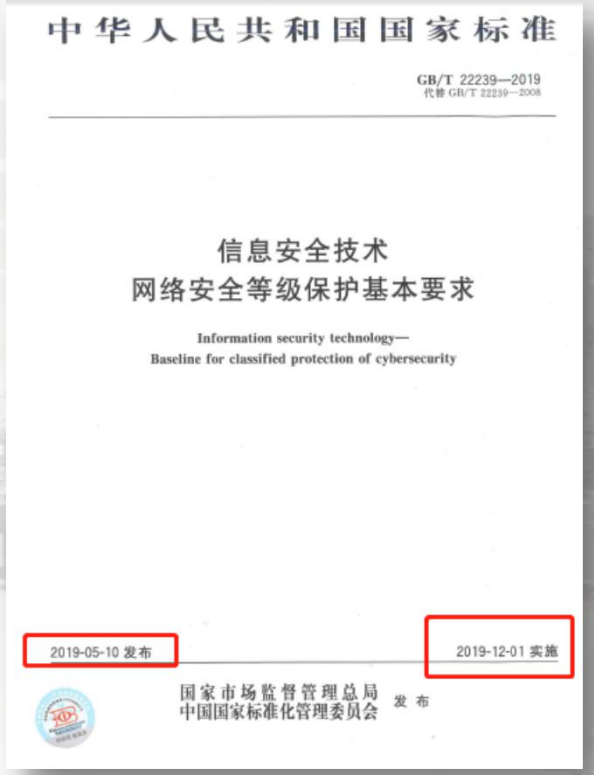
等保2.0简介

等级保护主要工作内容


信息系统安全等级保护定级指南
信息系统安全等级保护行业定级细则
安全等级
信息系统安全等级保护测评过程指南
信息系统安全等级保护测评要求
状况分析
信息安全等级保护安全建设整改工作
方法指导
基线要求
信息系统安全等级保护实施指南
信息系统等级保护安全设计技术要求
信息系统安全等级保护基本要求的行业细则
信息系统安全等级保护基本要求（GB/T 22239）
技术类
信息系统通用安全技术要求
信息系统物理安全技术要求
网络基础安全技术要求
其他技术类标准
管理类
信息系统安全管理要求
信息系统安全工程管理要求
其他管理类标准
产品类
操作系统安全技术要求
数据库管理系统安全技术要求
网络和终端设备隔离部件技术要求
其他产品类标准
计算机信息系统安全保护等级划分准则（GB17859）

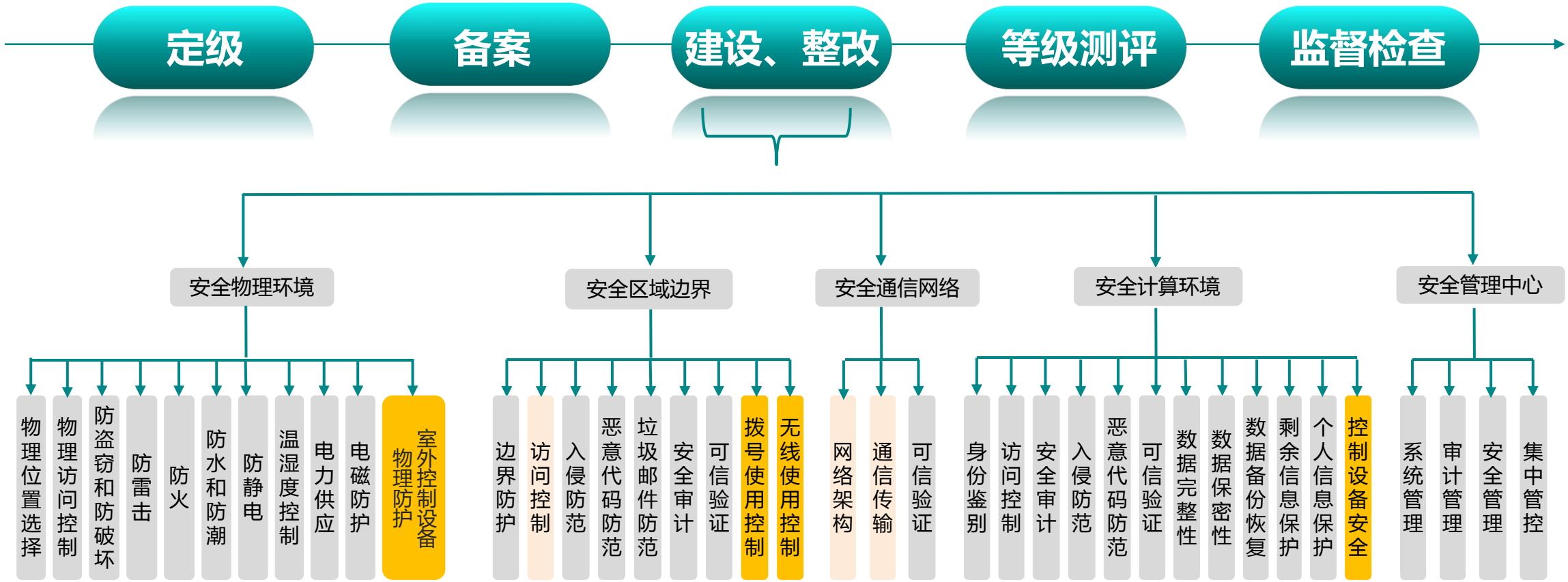
网络安全国家立法-依据《等保》建设网络安全

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，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在**网络安全等级保护制度**的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。



- **2019年5月10 号正式发布**

信息安全技术 网络安全等级保护基本要求



网络安全国家立法-依据《等保》建设网络安全

等级保护上升为法律

《中华人民共和国网络安全法》第21条规定“国家实行网络安全等级保护制度”，要求“网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”。

保护对象不断拓展

随着云计算、移动互联、物联网、工业控制、大数据等新技术不断涌现，计算机信息系统的概念已经不能涵盖全部，特别是互联网快速发展带来大数据价值的凸显，等保保护对象的外延将不断拓展。

工作内容持续扩展

在规定动作基础上，将风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等这些与网络安全密切相关的措施都将全部纳入等级保护制度并加以实施。

保护体系重大升级

在现有体系基础上，建立完善等级保护政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等。

等级保护2.0时代，将根据信息技术发展应用和网络安全态势，不断丰富制度内涵、拓展保护范围、完善监管措施，逐步健全网络安全等级保护制度政策、标准和支撑体系。

工业安全一站式解决方案

方案设计依据

整体方案设计主要解决政策、法规要求中的核心问题。

工业控制系统安全解决方案设计依据

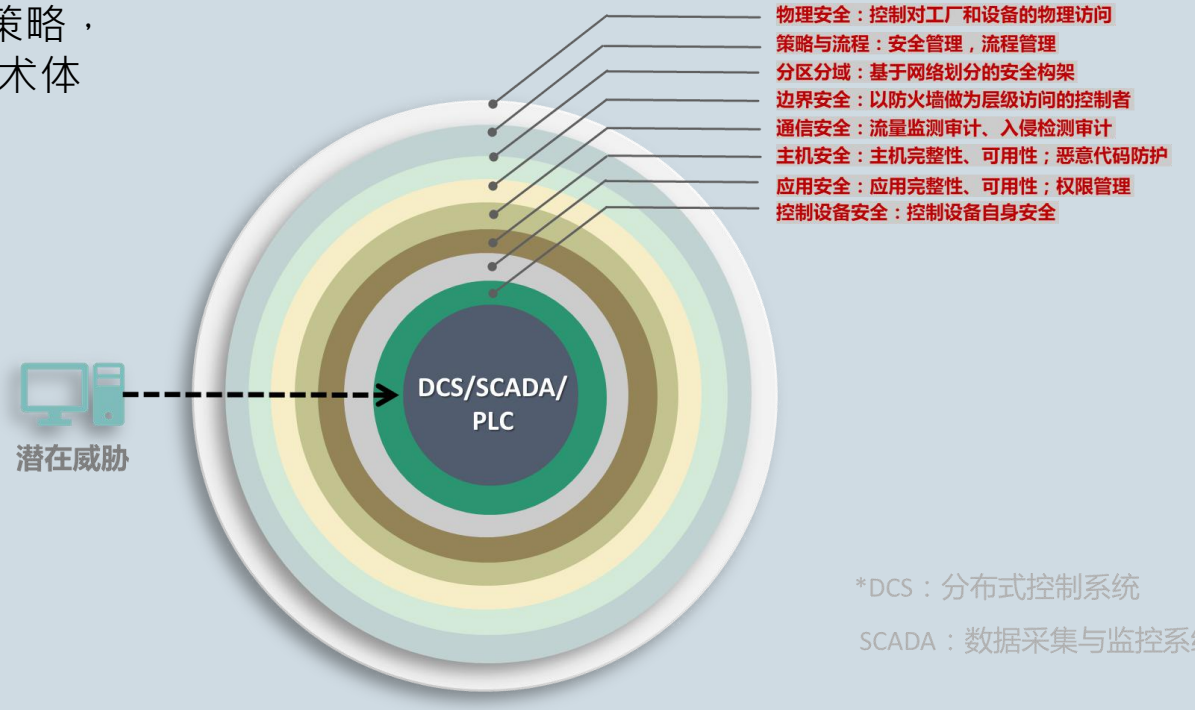
- 《信息安全技术 网络安全等级保护基本要求》
- 《信息安全技术 网络安全等级保护测评要求》
- 《信息安全技术 网络安全等级保护安全设计技术要求》
- 《工业控制系统信息安全防护指南》
- 《GB / T26333-2010 工业控制网络安全风险评估规范》

解决方案技术体系设计

以“分区分域、整体保护 、积极预防、动态管理”为总体策略，围绕“纵深防御+白环境”,打造企业工业控制系统安全技术体系。

以“分区分域、整体保护 、积极预防、动态管理”为总体策略，围绕“纵深防御+白环境”,打造企业工业控制系统安全技术体系。

- 以风险为核心，先了解风险，再分步规划实施；
- 网络区域划分，纵向分区，横向分域；
- 技术，管理双管齐下；
- 纵深防御，适度防护；
- 白环境；
- 集中管控、监测预警。



纵深防御技术体系

安全区域边界-边界防护

解决方案

解决方案

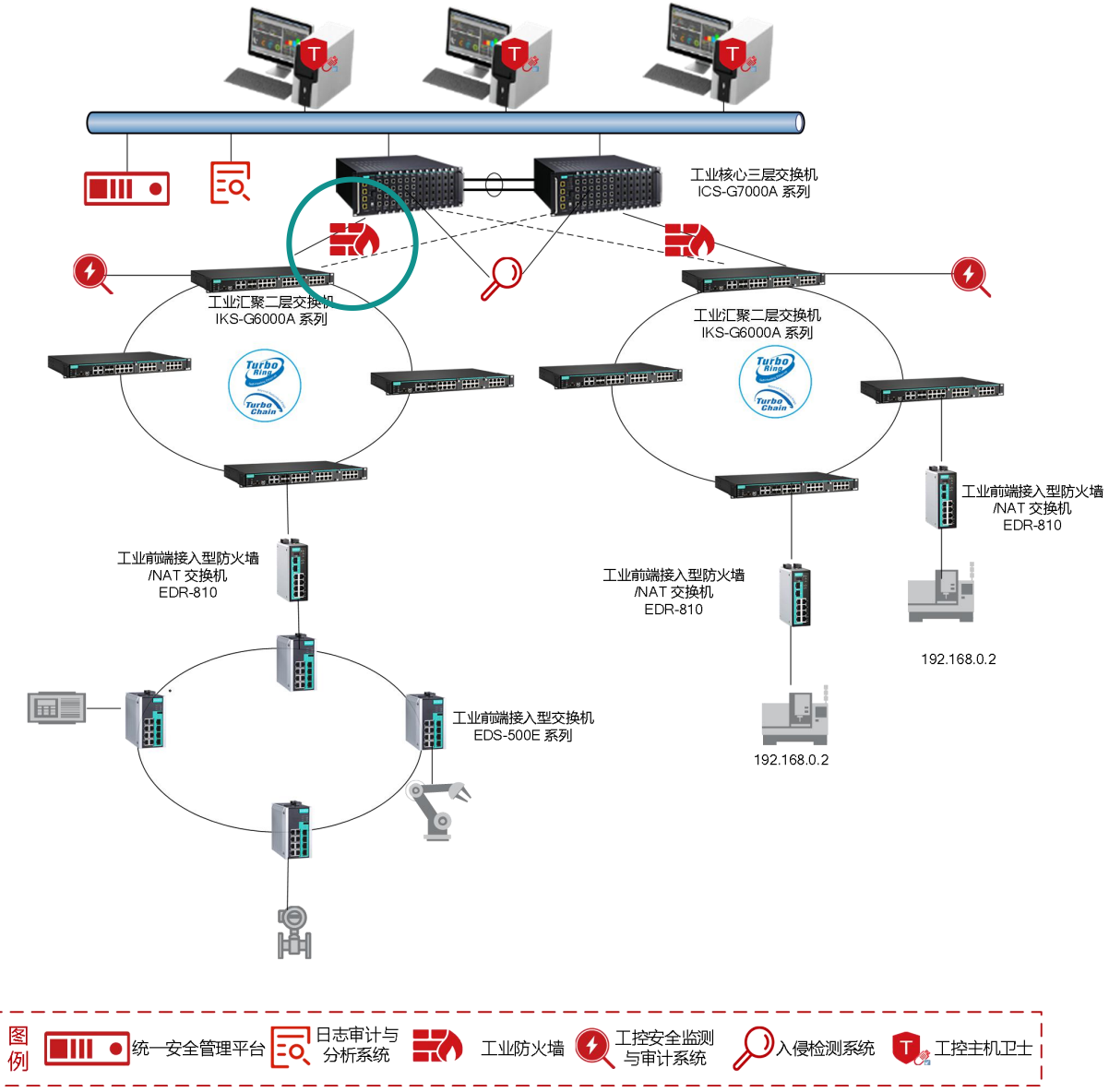
在工程师站、操作员站与生产线的控制环网之间部署工业防火墙。

解决的问题

1) 阻止来自外部系统攻击行为；
2) 阻止不同系统之间的越权访问行为；
3) 阻止病毒、蠕虫恶意软件扩散和入侵攻击，保护控制系统安全运行；
4) 阻止非授权设备的接入。

产品特点

1) 工业级的硬件品质，无风扇设计，延续设备使用寿命，减低故障；
2) 内置bypass功能，杜绝因安全设备损坏而导致的业务中断；
3) 集中管理，无需在终端调试；



安全通讯网络-安全审计

解决方案

解决方案

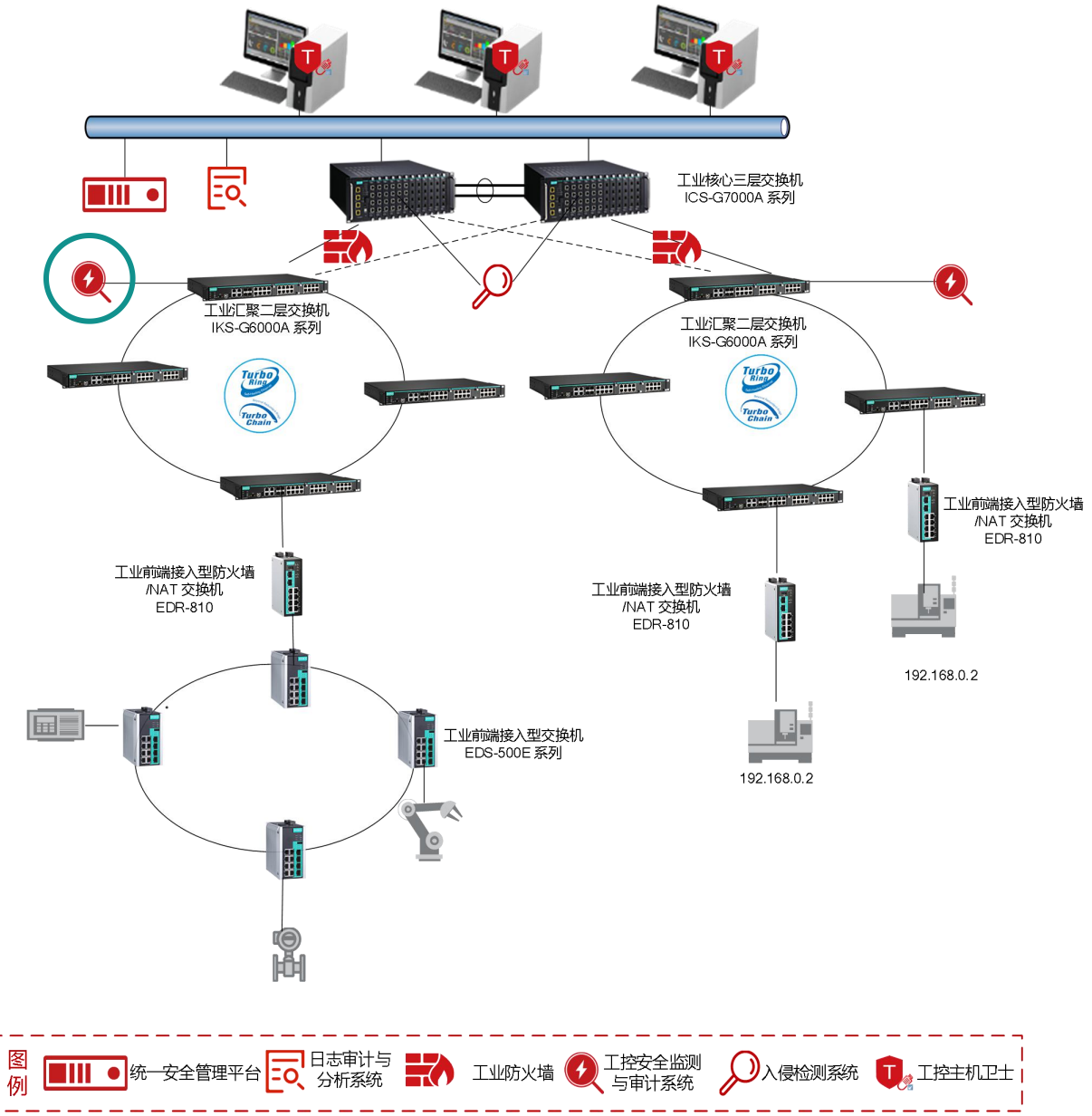
在生产线各控制环网关键节点旁路部署工控安全监测与审计系统。

解决的问题

1) 实时监测工控网络中的恶意攻击、误操作、违规行为、非法设备接入以及蠕虫、病毒等恶意软件的传播，帮助客户及时采取应对措施，避免发生安全事故；
2) 详实记录一切网络通信流量，包括网络连接、网络协议、网络会话、工控协议指令等，为安全事故调查取证提供技术支撑。

产品特点

1) 采用旁路部署方式，对生产过程“零影响”；
2) 集中管理，无需在终端调试；
3) 私有协议的自定义。



安全通讯网络-入侵检测

解决方案

解决方案

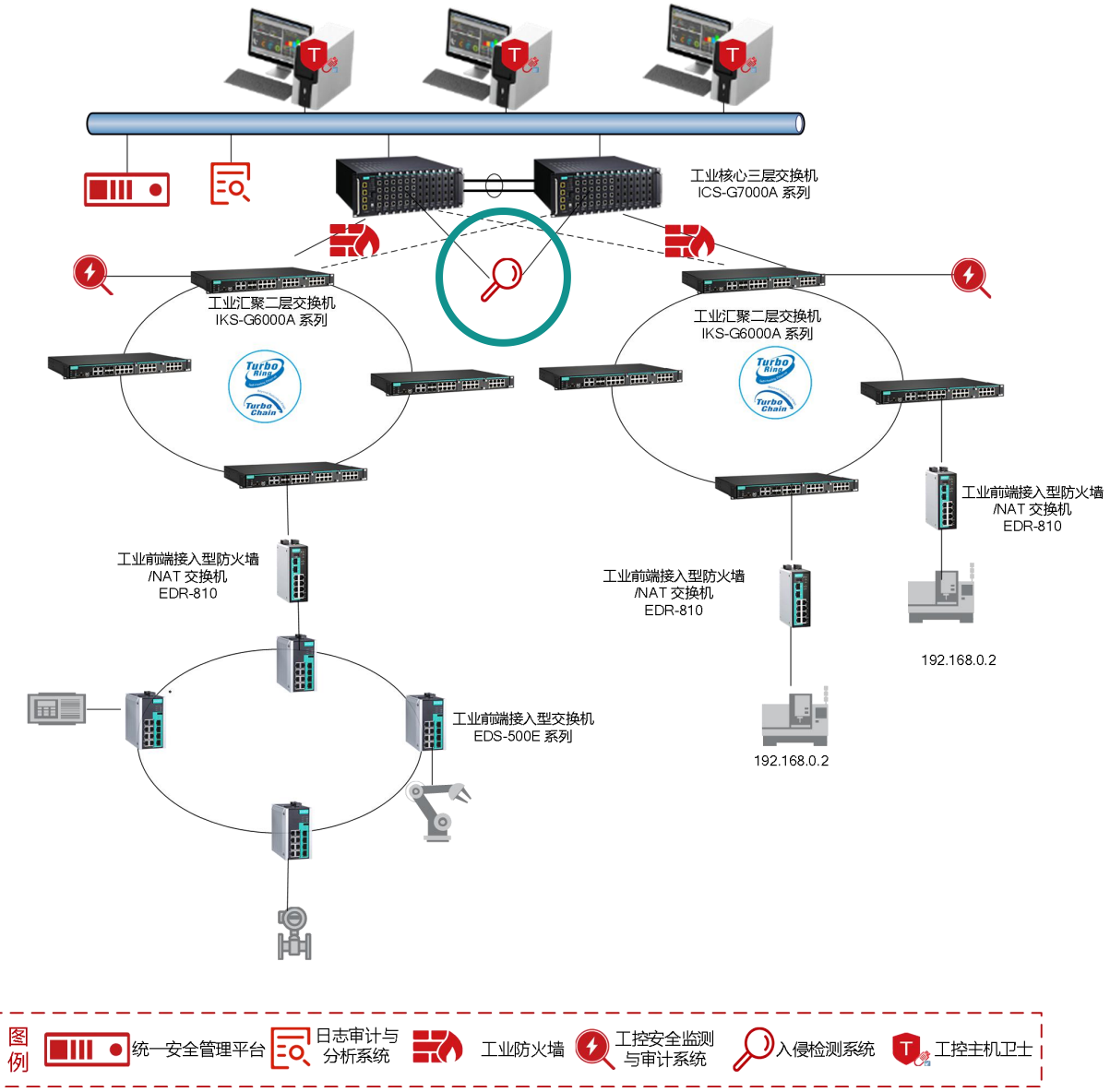
在生产线各控制环网关键节点旁路部署入侵检测系统。

解决的问题

1) 实时检测来自各车间网络中的恶意行为，以及蠕虫、病毒等恶意软件的的入侵，帮助客户及时采取应对措施，避免发生安全事故；
2) 通过网络入侵检测分析，并形成图形化的日志报表，帮助安全管理员实时展现工控网络中潜在的安全威胁和安全级别。

产品特点

1) 对工业网络、系统的运行状态进行监视，检测非法操作或异常访问行为；
2) 及时发现来自生产网络外部或内部违反安全策略的网络行为，避免恶意攻击行为的蔓延。



安全计算环境-主机防护

解决方案

解决方案

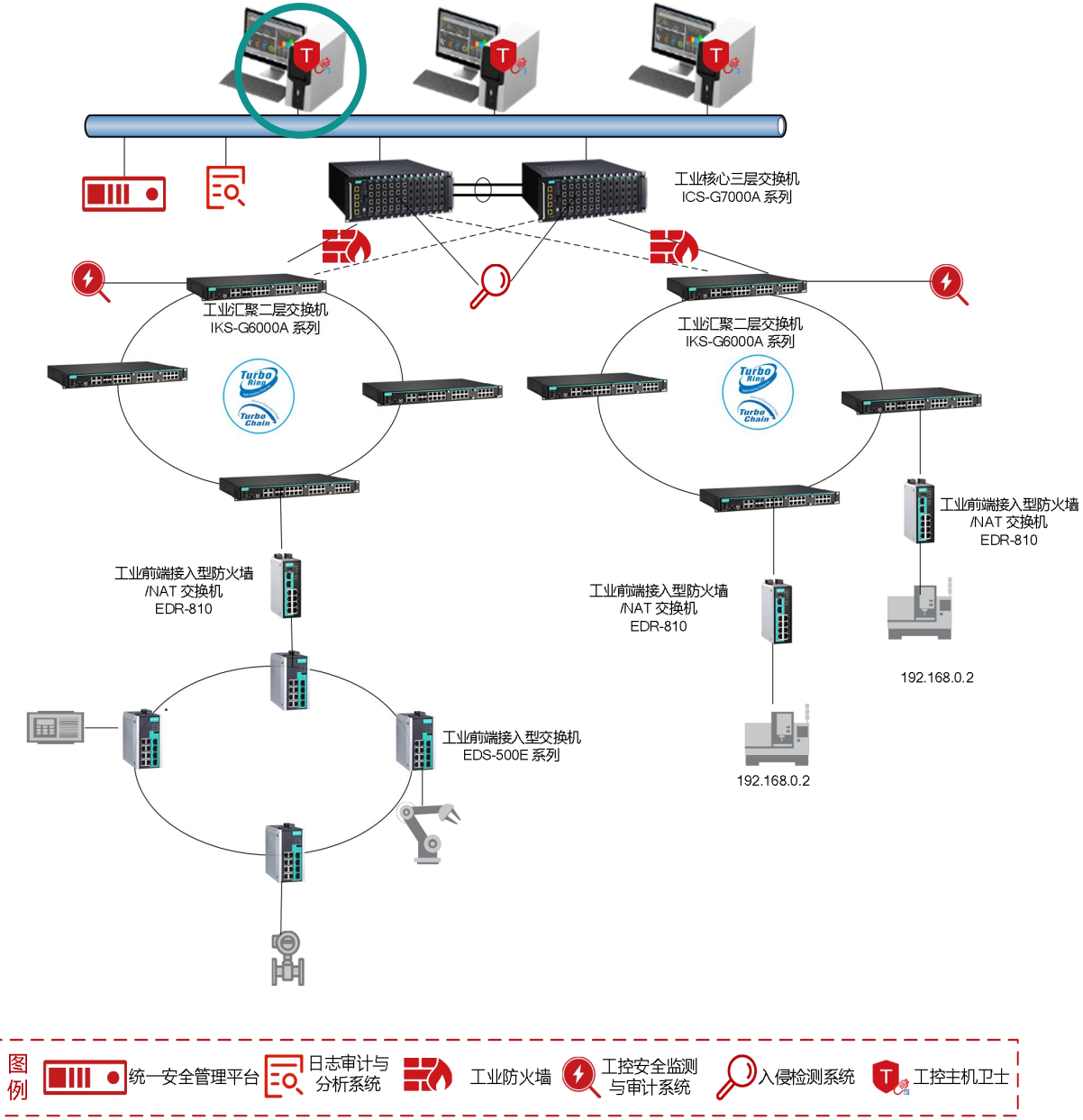
在操作员站、工程师站等关键控制设备安装工控主机卫士。

解决的问题

1) 采用强化口令鉴别（USBKEY）加用户名密码鉴别，实行强制访问控制，对所有主机、服务器被操作的日志、事件日志等信息进行记录；
2) 阻止非授权软件或进程的安装和运行，防止恶意代码攻击“0-day” 漏洞的利用；避免升级病毒库，变被动为主动；防止操作员使用移动介质带入病毒在业务网中扩散。

产品特点

1) 自学习的构建“文件级”白名单基线库；
2) 避免因传统杀毒软件带来的安全隐患；
3) 一键完成操作系统安全策略优化；



日志统一收集分析

解决方案

解决方案

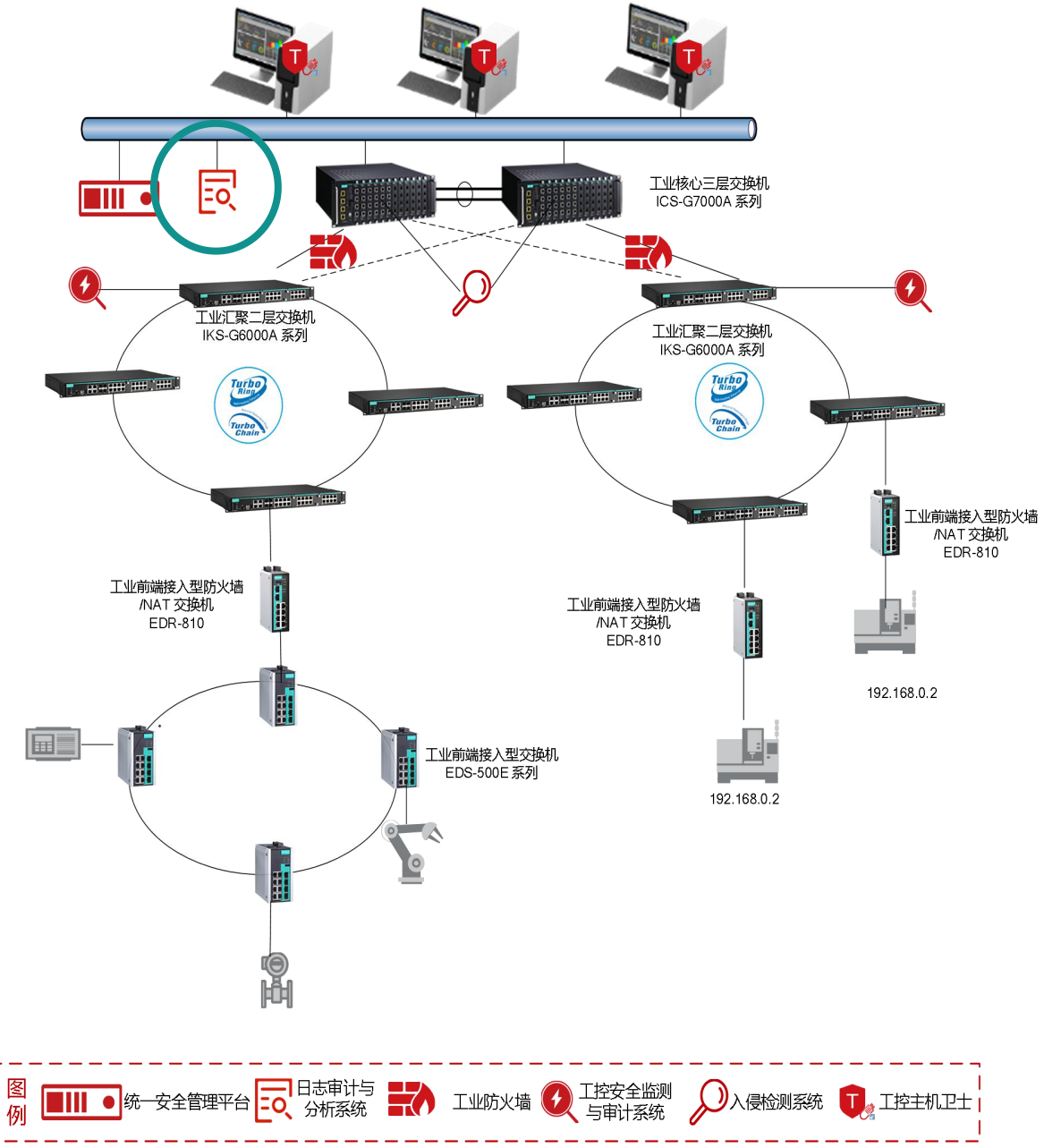
在生产线控制网部署日志审计与分析系统。

解决的问题

1) 对整个系统中的设备（网络设备、服务器、数据库、应用、中间件等）运行日志进行集中收集、存储，与管理平台联动对日志进行关联分析；
2) 满足网络安全法、等级保护对日志审计的要求。

产品特点

1) 实时采集网络中不同厂商的网络设备、安全设备、服务器、操作员站、数据库系统的日志信息，关联分析，精准识别安全事件，满足国家及行业标准规范中关于日志审计的相关要求；
2) 内置的丰富关联分析场景，通过不同规则构建复杂关联分析模型，实时发现网络攻击和违规行为。



安全管理中心-集中管理

解决方案

解决方案

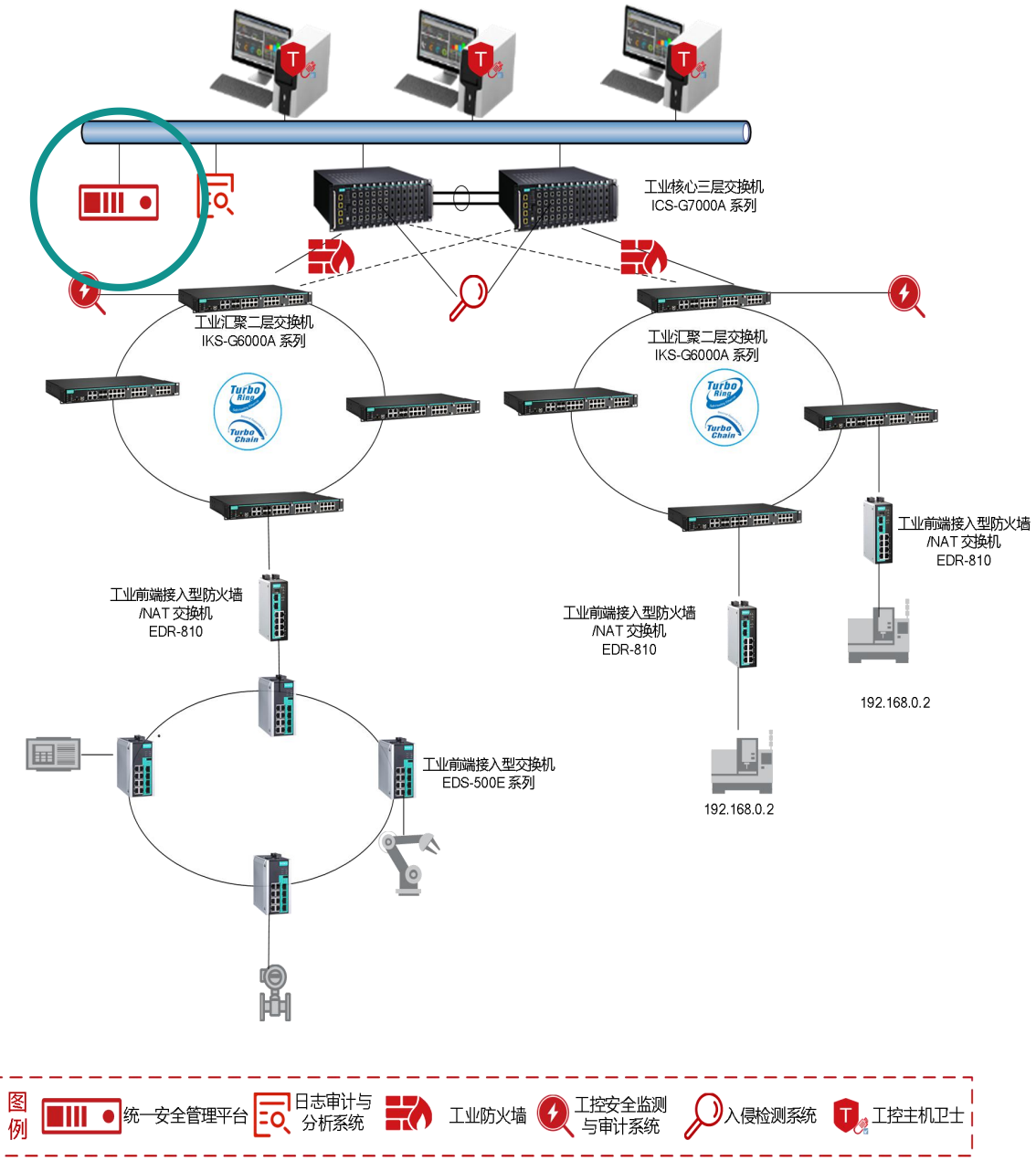
在生产线控制网部署统一安全管理平台。

解决的问题

1) 统一管理安全设备，如策略制定、下发等；
2) 对安全日志进行关联分析，并通过图形、报表方式对当前安全状态进行可视化展示；
3) 便于上级级维护人员进行维护管理，实现安全事件报警管理。

产品特点

1) 统一配置，降低日常管理工作量、提高工作效率；
2) 集中日志管理，统一收集和展示系统内各业务单元的日志信息，满足等保要求；
3) 全面监控、实时告警，从而降低运维成本、提升事件响应效率。



工业内网安全建设方案

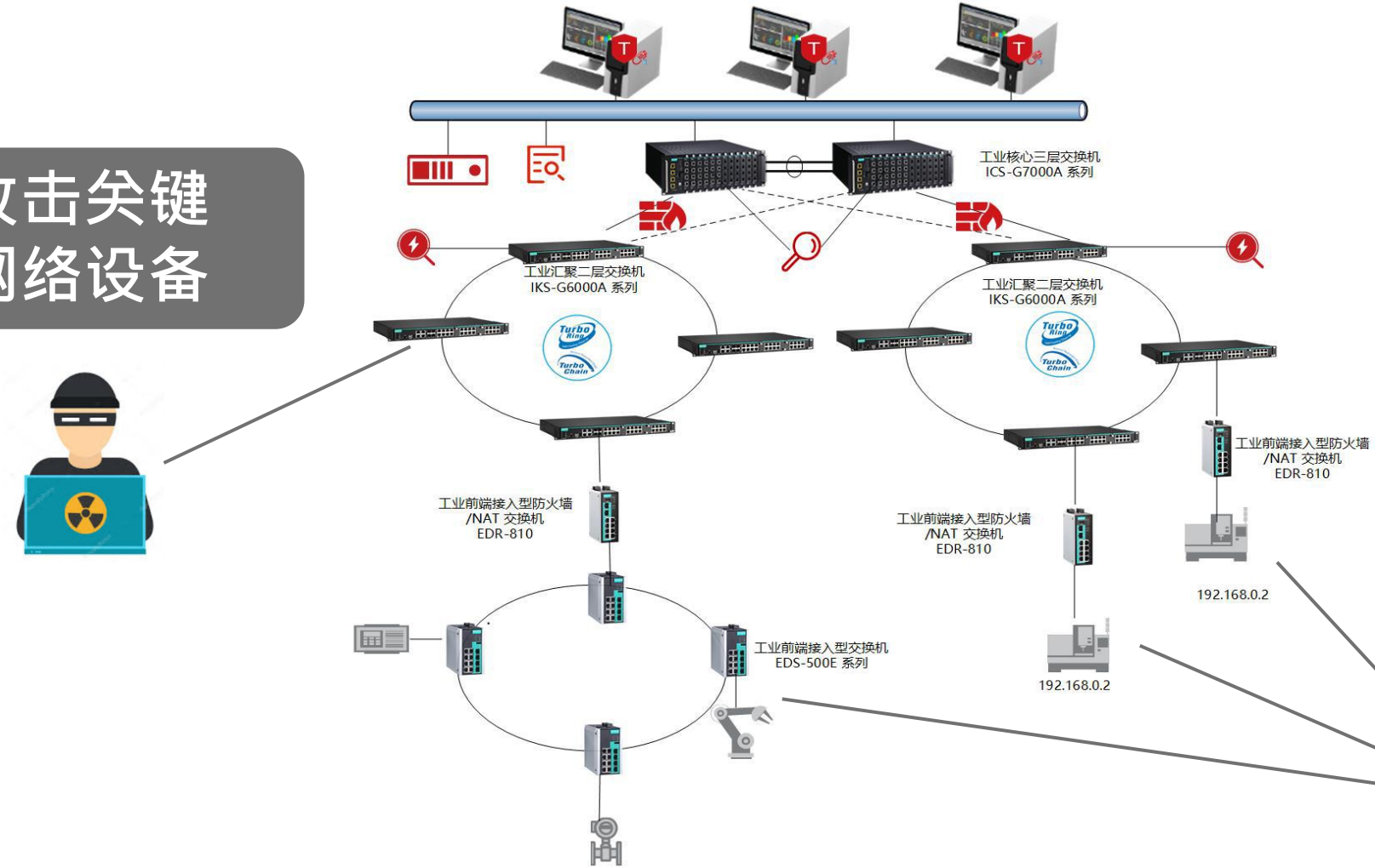
张杰，Moxa产品经理

若安全威胁来自工业系统内部，或者已经在系统内部发生？

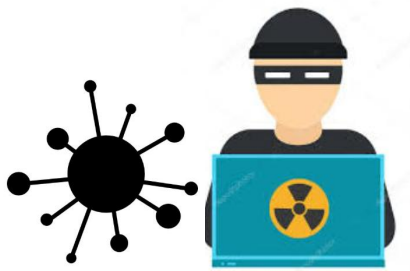
工业系统网络安全加固建议

恶意程序/人员的攻击目标（关键资产设备）

攻击关键
网络设备



攻击关键
终端设备



图例 统一安全管理平台 日志审计与分析系统 工业防火墙 工控安全监测与审计系统 入侵检测系统 工控主机卫士

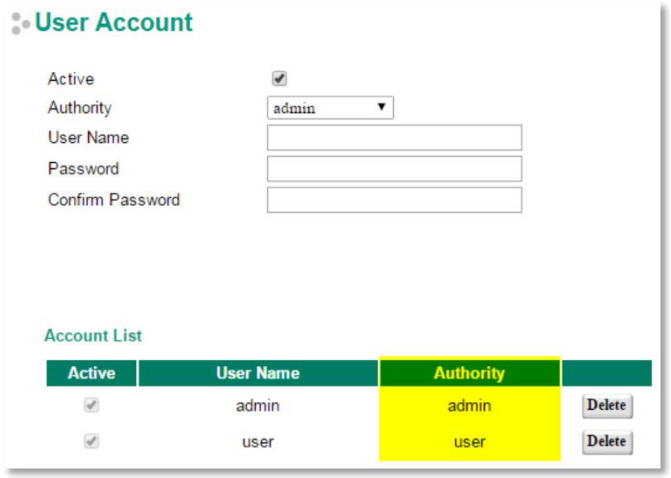
防止攻击关键网络设备

阻止侵入网络设备—**密码策略和管理**

Step 1
避免统一管理账户，
提升密码复杂度

Step 2
账户连续登录失效处理

Step 3
定期批量修改密码



功能：账户管理设定
作用：增加破解复杂度

功能：账户锁定
作用：阻止暴力破解

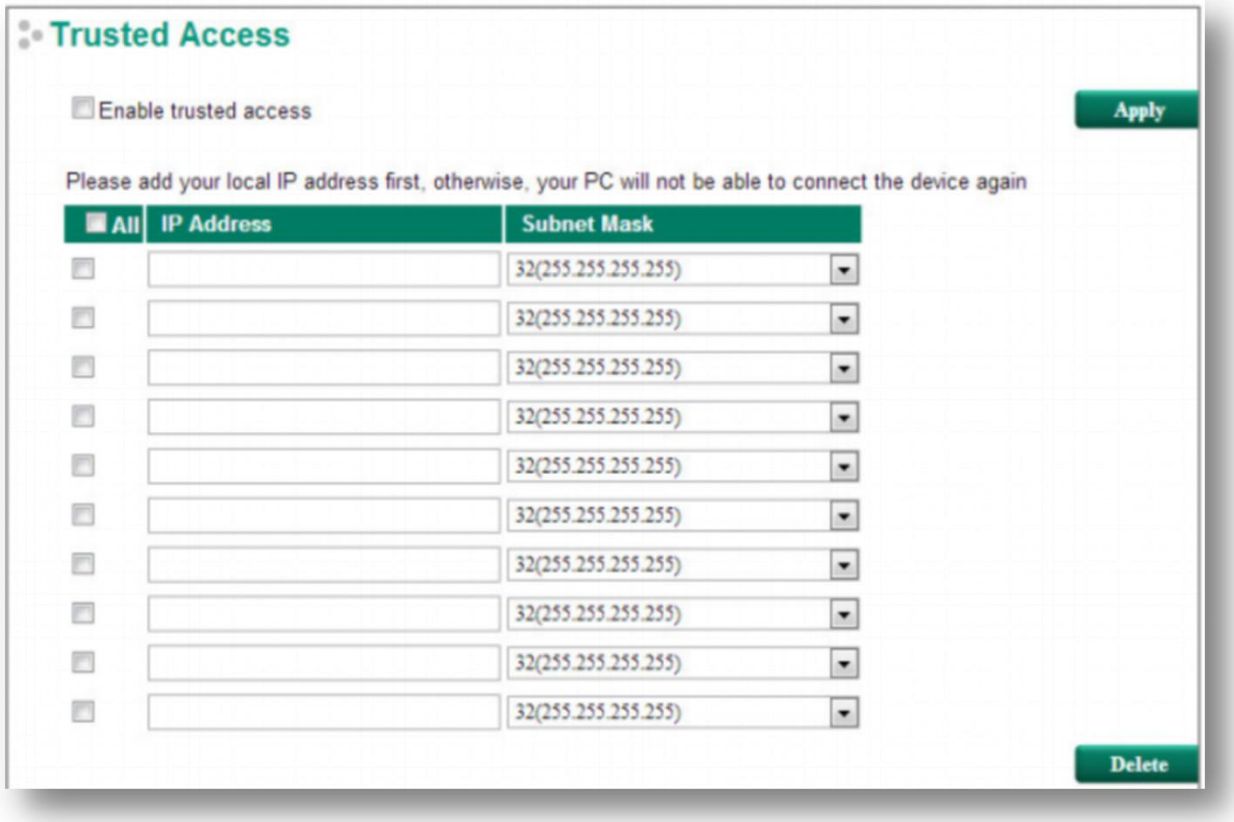
功能：**RADIUS**
作用：防止离职员工恶意破坏

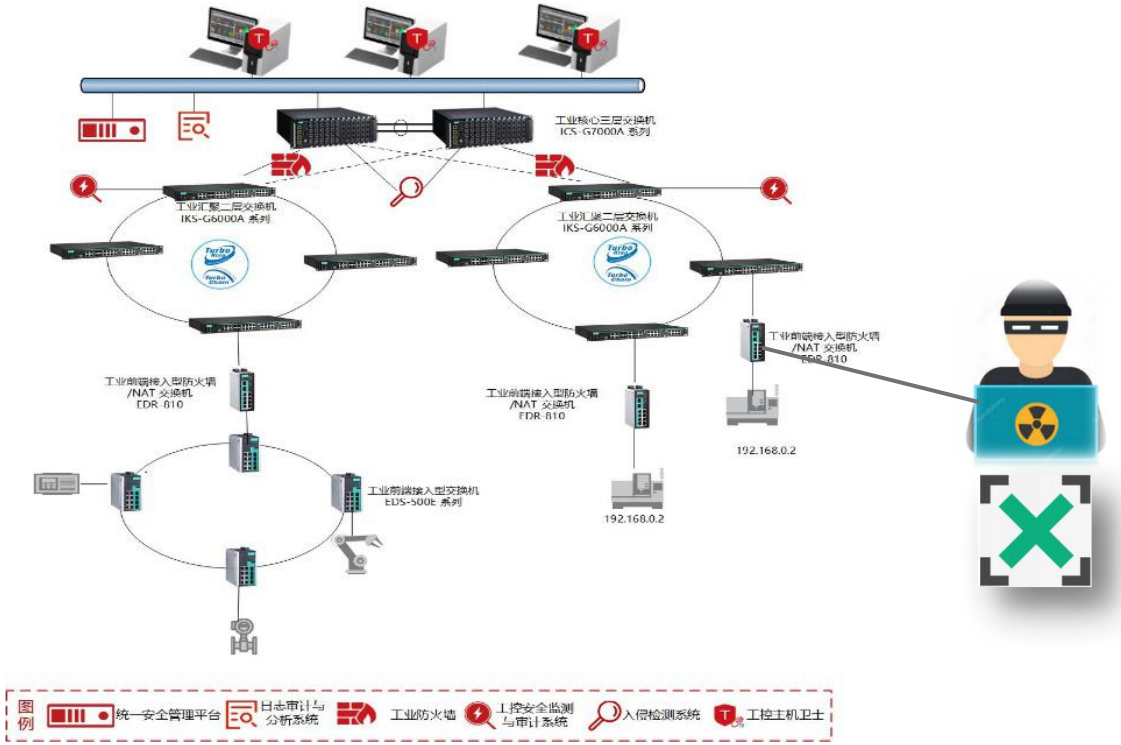
防止攻击
关键网络设备

阻止侵入网络设备—
禁止非授权设备进行网络管理

场景列举

非授权用户即使获取账户密码，也需要在特定的设备上登录网络设备的管理界面



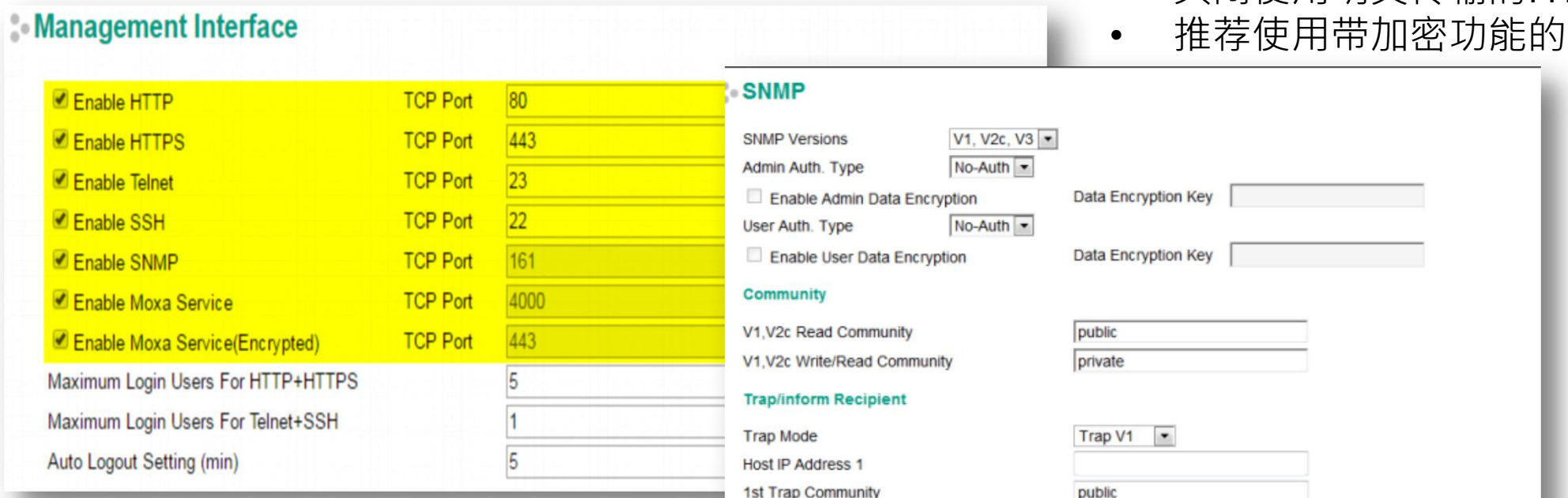


防止攻击关键网络设备

阻止侵入网络设备—**关闭不安全的服务**

场景列举

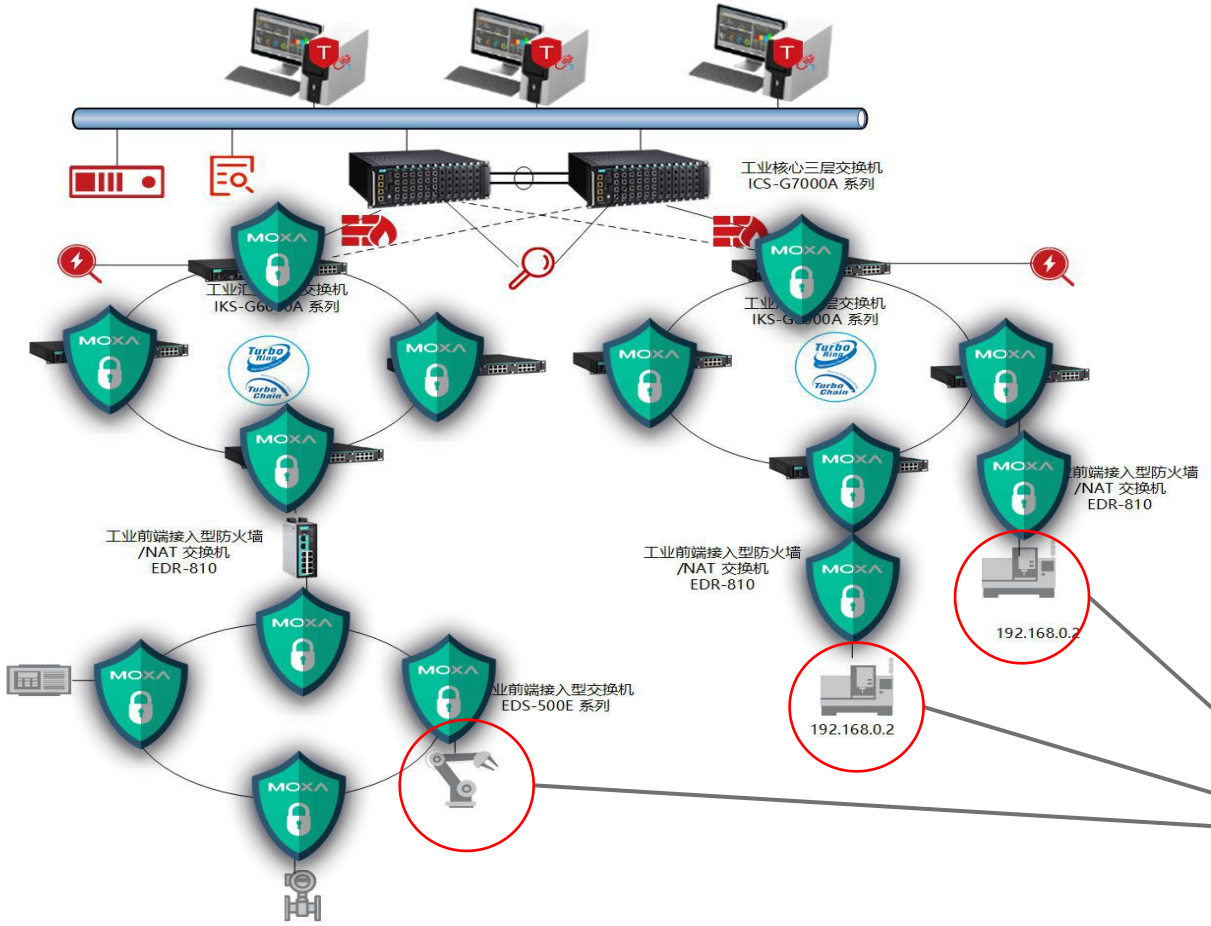
解析数据包，获取管理的用户名和密码



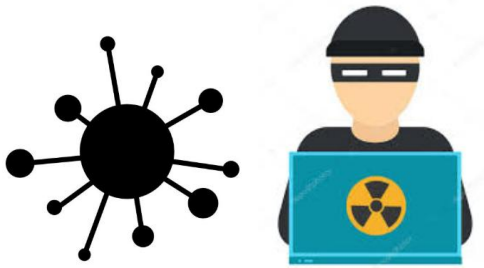
建议操作

- 关闭使用明文传输的HTTP，SSH管理接口
- 推荐使用带加密功能的SNMP V3

如何通通过网络保护关键的终端设备



攻击关键终端设备



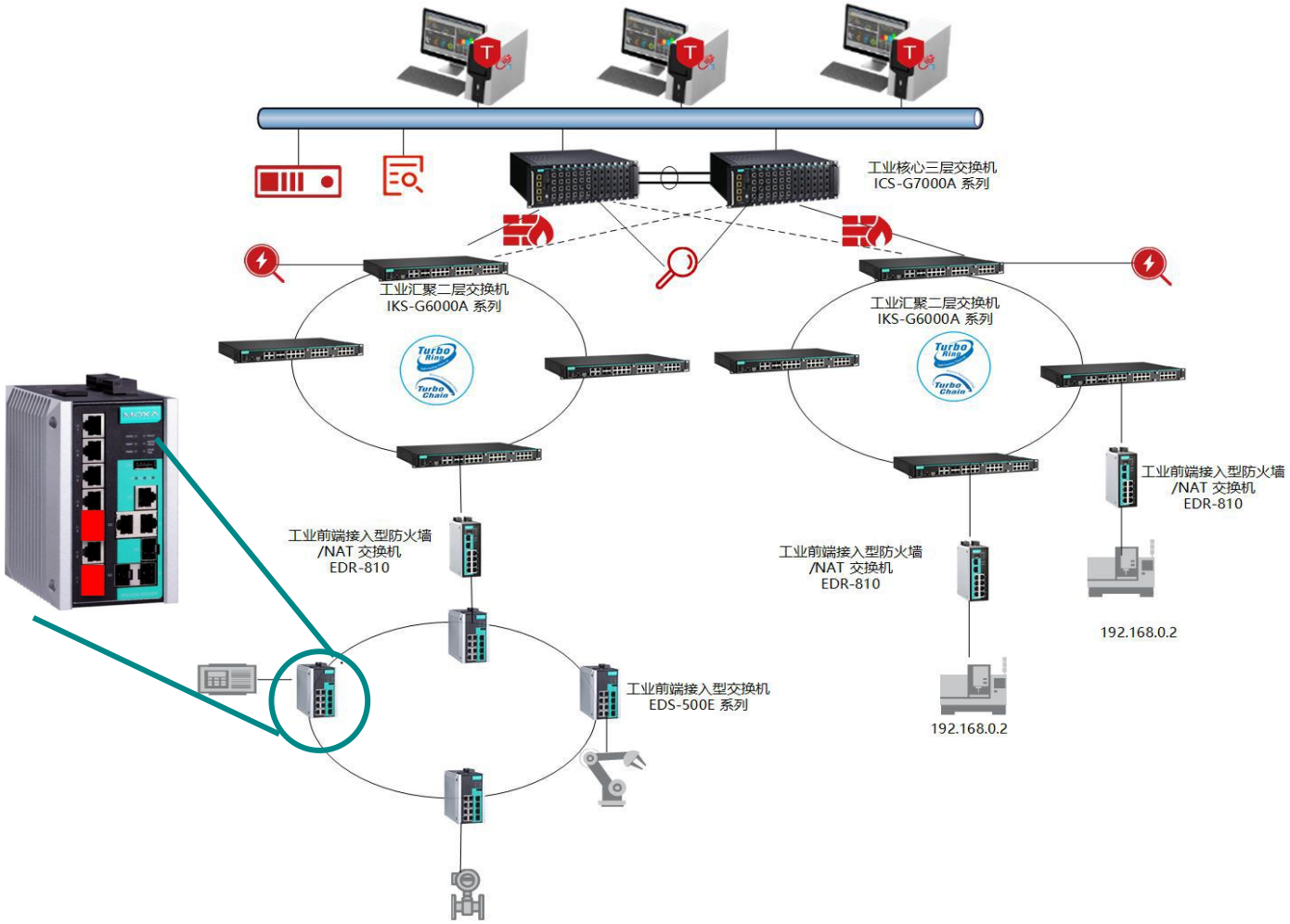
防止攻击
关键终端设备

阻止入侵者使用网络资源–
阻止恶意人员的接入

1
- 功能：禁用不使用端口
- 作用：禁止非法接入网络

2
- 功能：Mac/IP 地址绑定
- 作用：传输白环境

3
- 功能：RADIUS/TACACS+
- 作用：防止身份伪造



防止攻击
关键终端设备

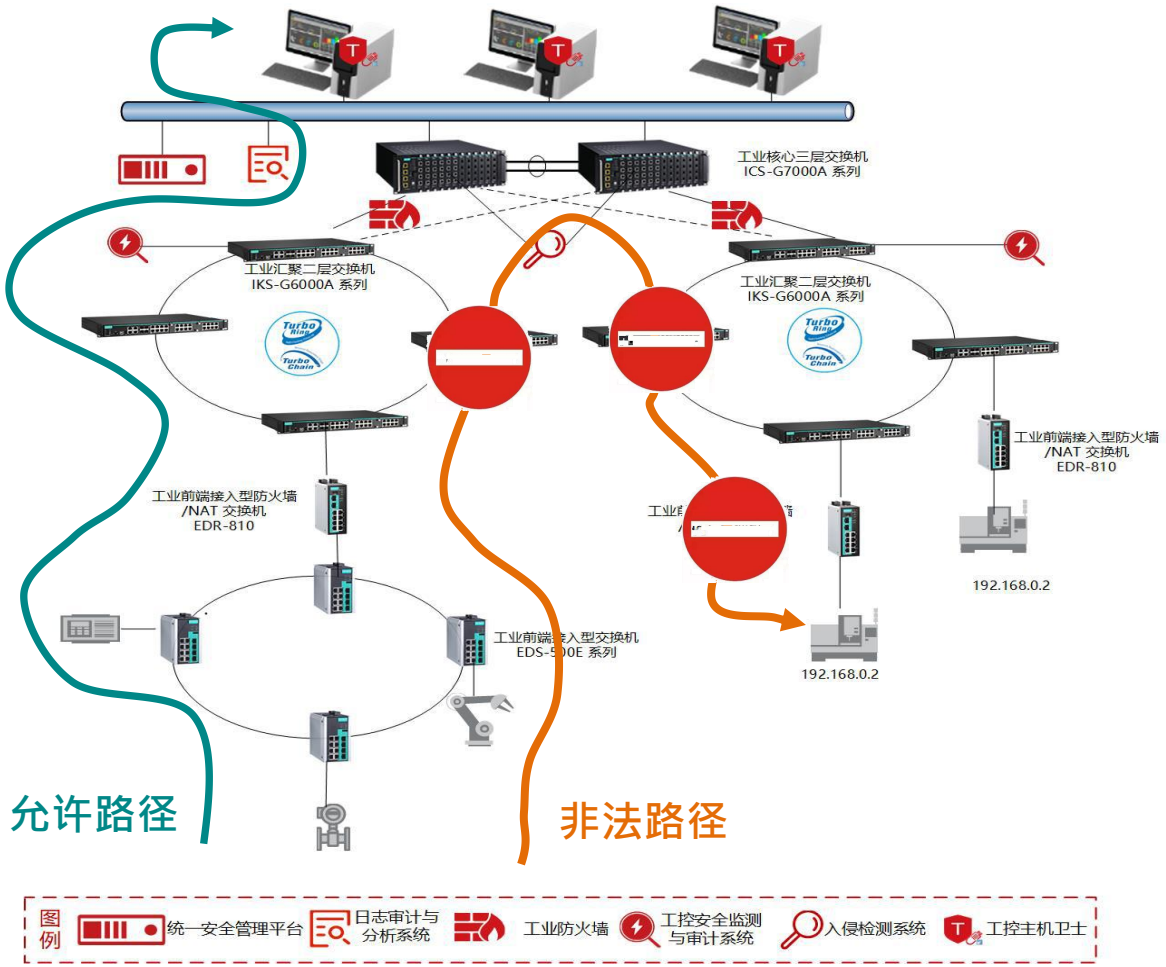
阻止入侵者使用网络资源—
阻止恶意数据横向传播

场景列举

限制目标IP/限定源IP，仅允许访问授权网段

- **Traffic filter for ingress and egress packets**

IP address	MAC address	IP protocol	Ether type
• Source • Destination	• Source • Destination	• ICMP • IGMP • IP over IP • TCP/UDP • User Define	• ARP / RARP • IEEE802.1Q • IPv4 / IPv6 • IEEE802.3 • PROFINET • LLDP • IEEE1588 • User Define



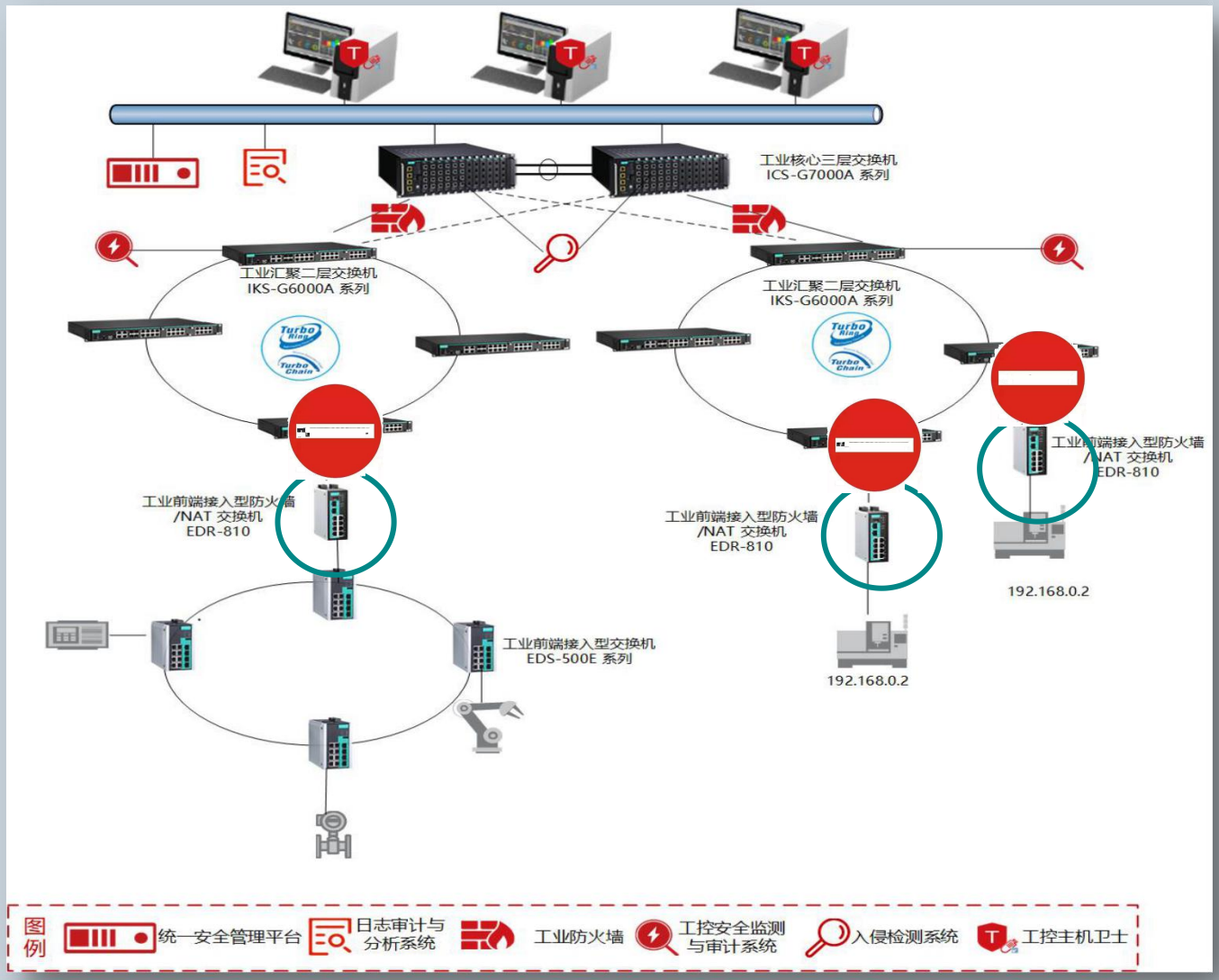
功能：访问控制列表ACL（Access Control List）

防止攻击
关键终端设备

阻止入侵者使用网络资源—
阻断恶意数据

EDR-810 Series
工业级安全路由器

- 工业协议白名单
- 支持现场级工业环境
- 支持二层交换机功能
- 支持NAT 功能



安全信息管理

安全审计和监控的可视化管理

资产管理
自动网络拓扑 & 实时报告设备状态

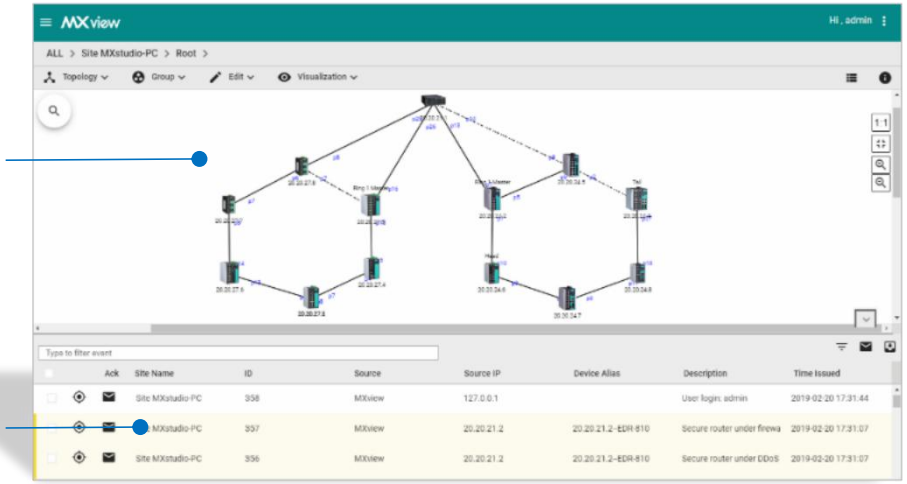
配置管理
备份和恢复设备配置

设备安全状态显示
检查设备的设置是否满足安全政策要求

安全事件侦测& 记录
日志记录安全攻击事件

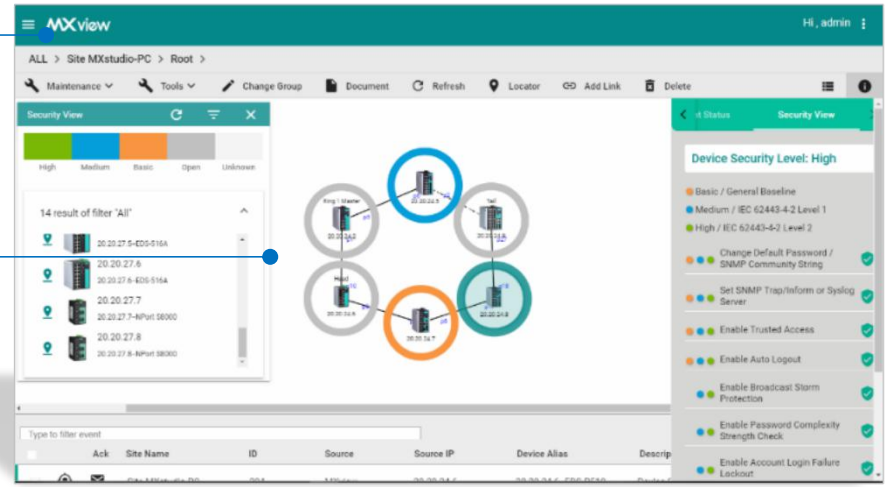
资产管理

安全事件
侦测&记录



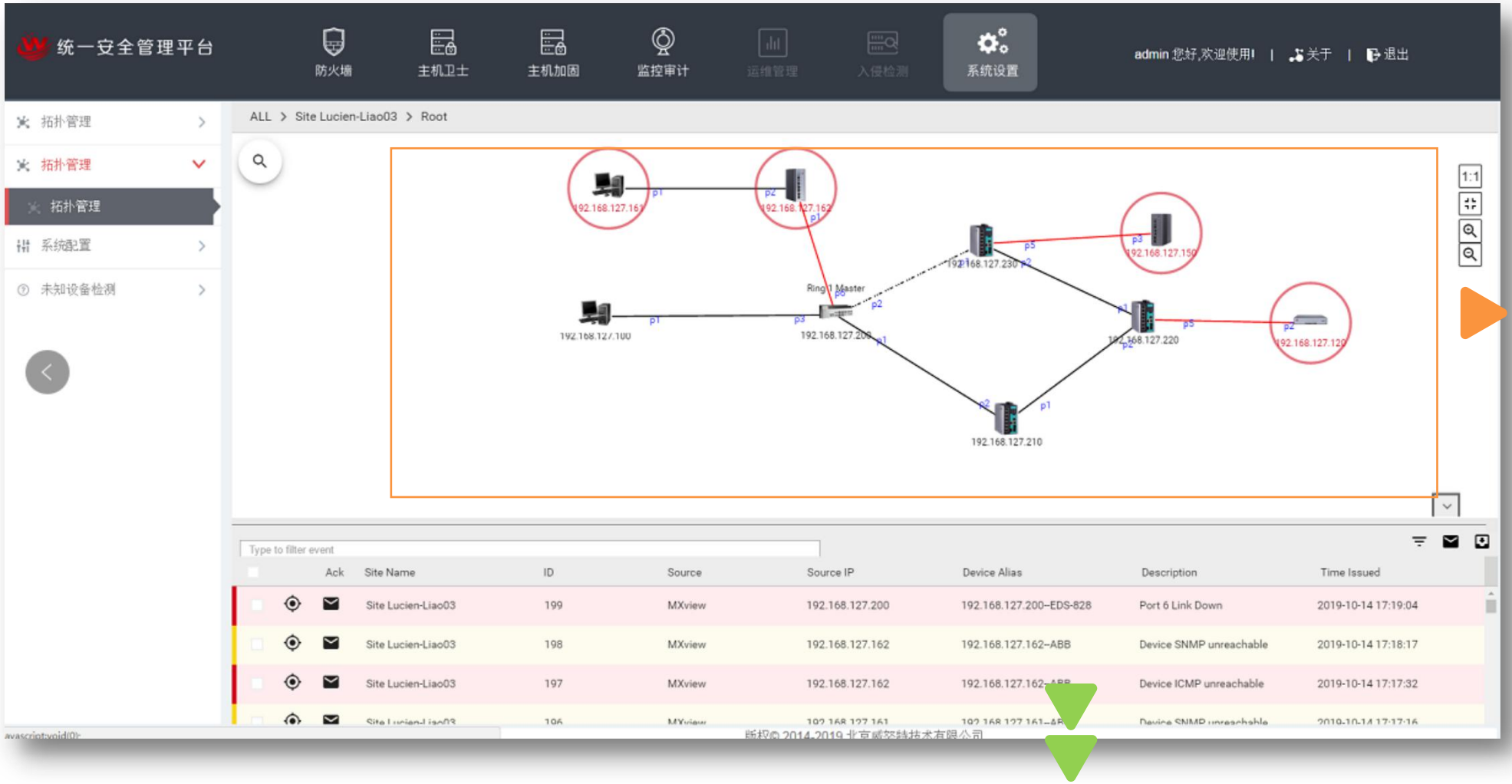
配置管理

设备安全
状态显示



安全信息管理

通过威努特统一管理平台同时管理网络和安全

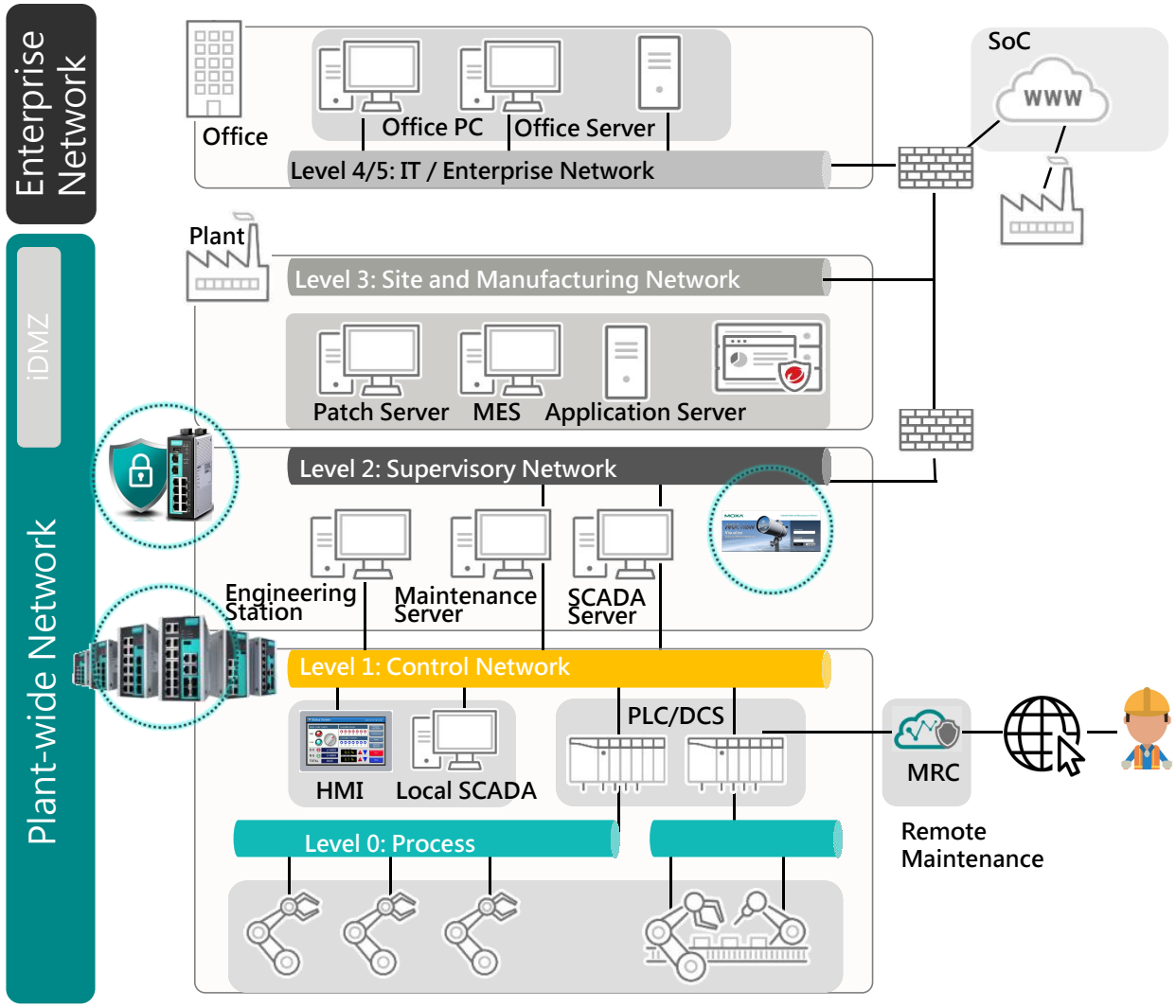


Moxa
网管软件嵌入

威努特安全统一管理平台界面

提供工业安全一站式解决方案

工控网络典型架构 (普渡模型)



工业内网安全方案

MOXA

工业交换机（安全增强型）

工业内网防火墙

工业管理软件

远程连接

工业系统安全方案

威努特 WINICSSEC

安全审计

入侵检测

主机防护

日志分析

统一管理平台

工业防火墙交换机

支持NAT/防火墙功能的安全交换机

EDR-810

- 1-对-1 、 1-对-N NAT，支持NAPT
- 支持防火墙功能，识别Modbus ，PROFINET ，EIP等工业协议
- 支持2千兆SFP，8个百兆电口
- 支持Turbo Ring ，Turbo Chain 环网冗余协议，冗余时间 < 50ms （ 250 台满载 ）

Perfect for

Secure Network Infrastructure

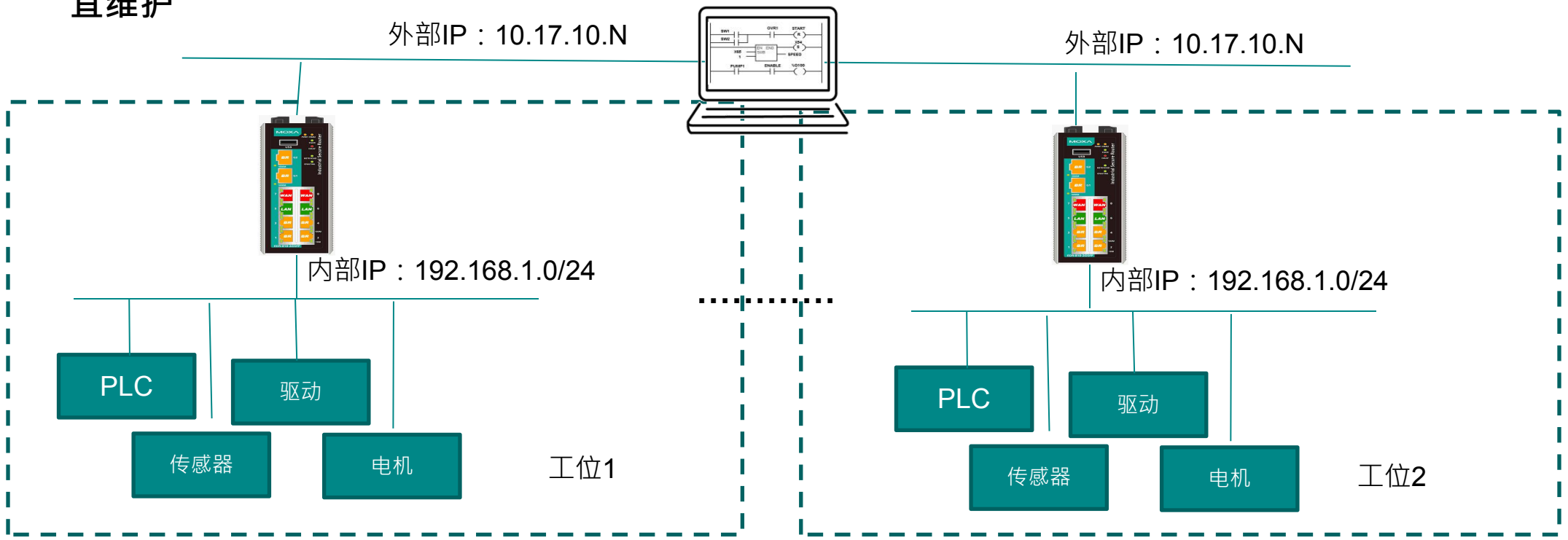
Secure Remote Access

Device Security

应用: 工厂中的NAT功能所带来的优势

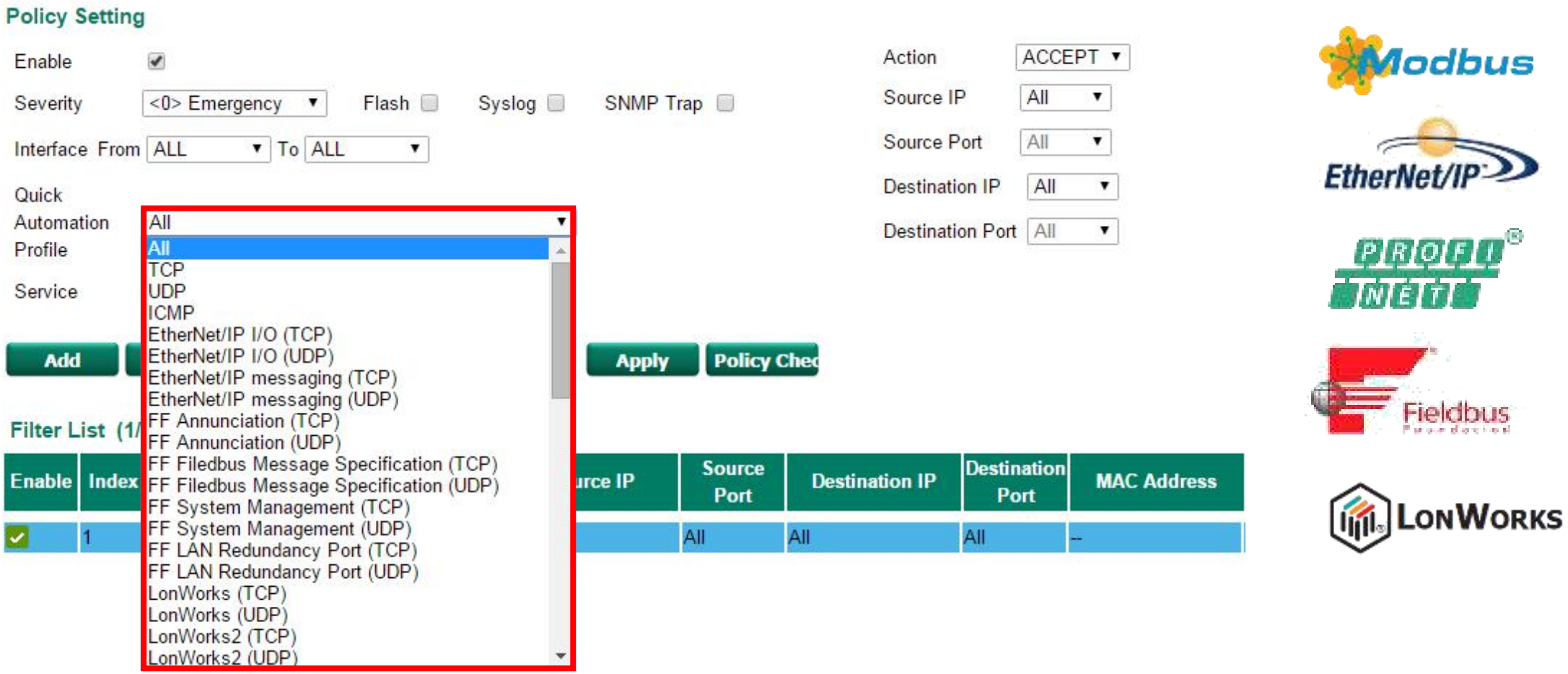
目标应用情景

- 自动化设备（如机床中关键IP设备），更改设备IP会破坏原系统运行， 组网困难
- 系统改造时（如设备监控），由于IP 已经跟业务相关，原系统的IP 地址可能造成系统运作异常
- 标准化产线中（如总装），有多个工位，每个工位上为同一套IP设备，单独规划IP 工作量大，不宜维护

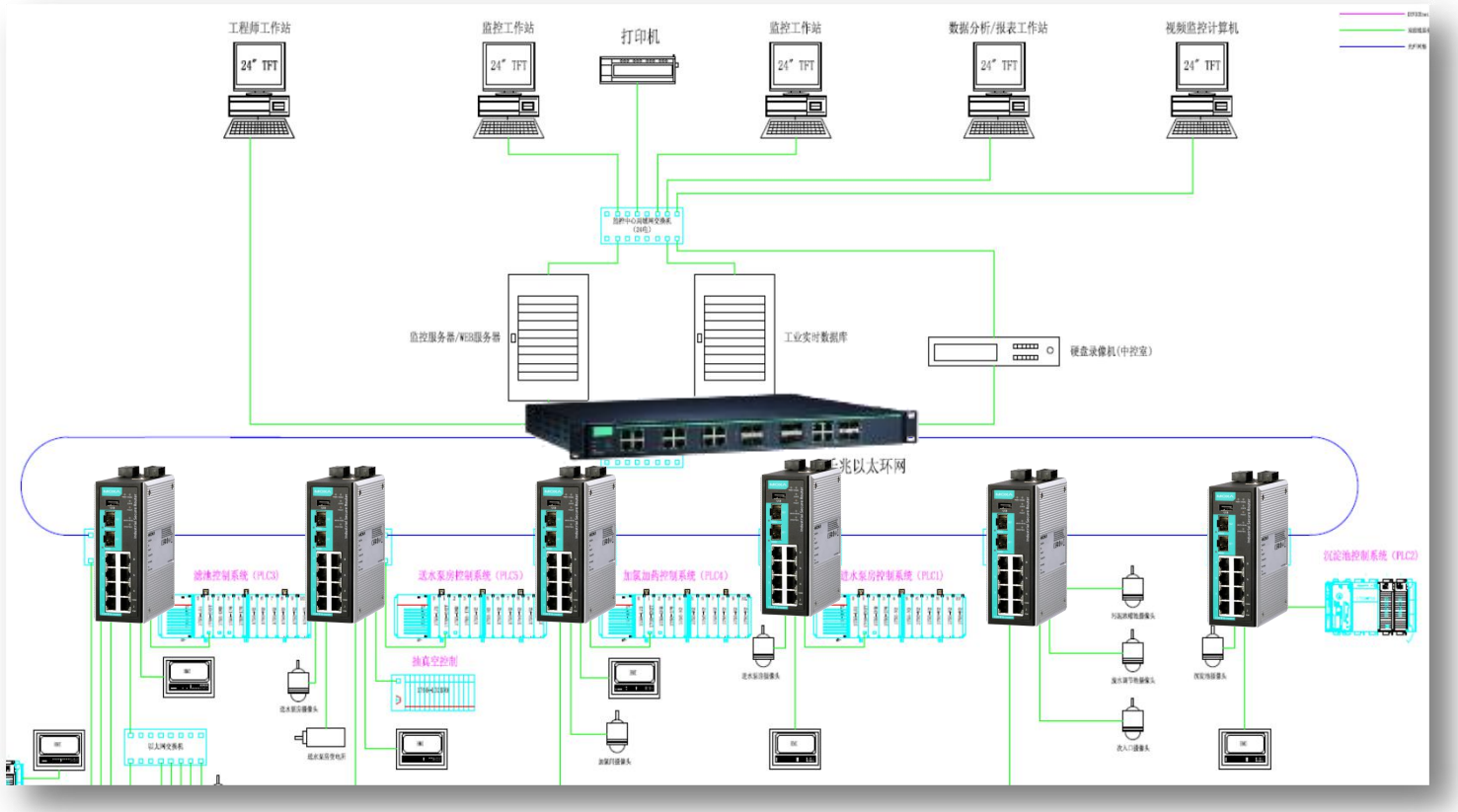


防火墙功能：工业协议识别和深度解析

[Industrial protocols]



作为支持安全增强的的工业环网交换机使用



污水处理应用结构

背景

- 客户为集成商，以往批量使用二层网管交换机，发生过一次现场故障，去终端客户现场排查2天左右才找到故障原因，损失很大

Why EDR-810?

- 每个车间相互隔离，彼此不受影响
- 通过NAT地址转换防止外部入侵，更加安全可靠
- 可开启防火墙功能，提升网络安全

支持NAT/防火墙功能的安全交换机

EDR-810

- 1-对-1 、 1-对-N NAT，支持NAPT
- 支持防火墙功能，识别Modbus ，PROFINET ，EIP等工业协议
- 支持2千兆SFP，8个百兆电口
- 支持Turbo Ring 环网冗余协议，冗余时间 < 50ms（250 台满载）

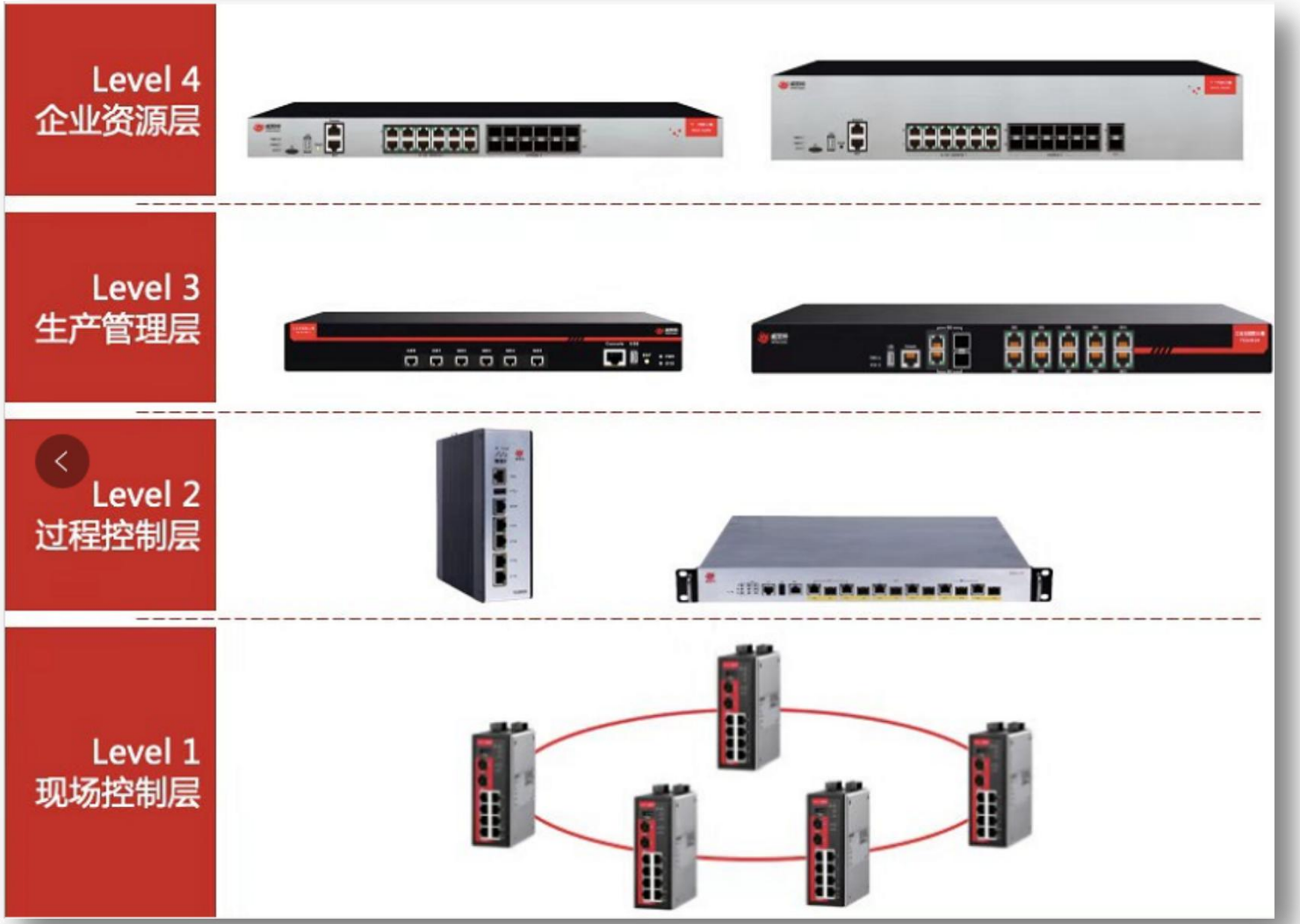
Perfect for

Secure Network Infrastructure

Secure Remote Access

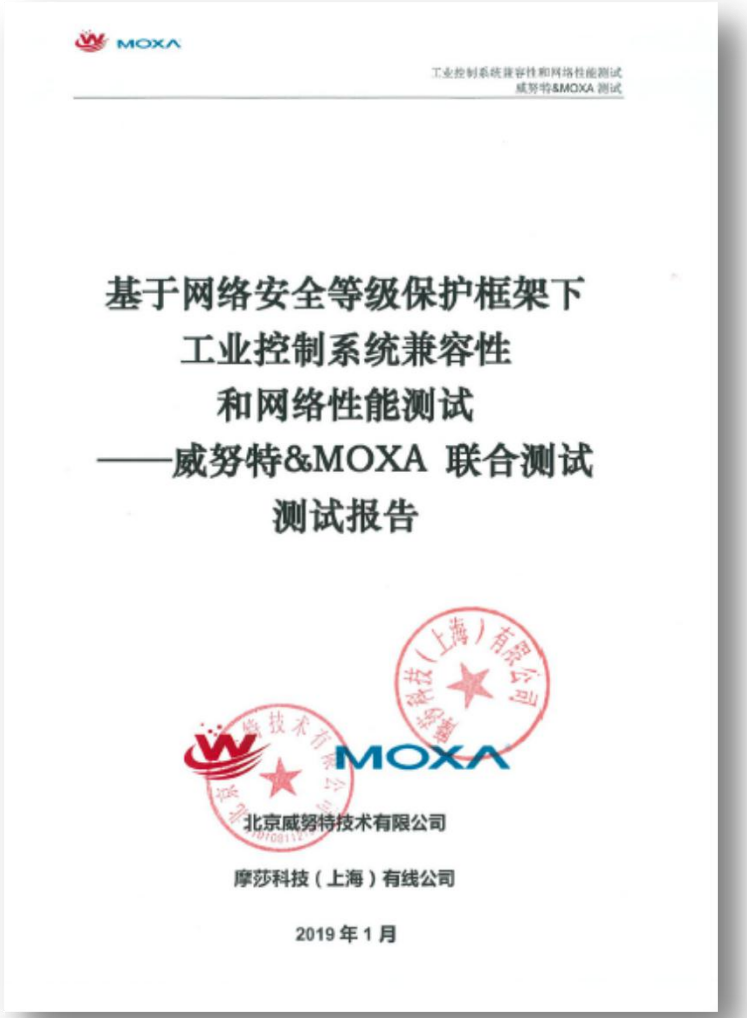
Device Security

史上最“墙”工业防火墙家族介绍



- 防火墙：
  - 状态检测
  - 透明防火墙
  - 包过滤
  - 工业协议深度检测
- 交换机：
  - 支持2千兆SFP，8个百兆电口
  - 支持Turbo Ring ,20ms 快速恢复

Moxa & 威努特产品联合测试



MOXA

工业控制系统兼容性和网络性能测试
威努特&MOXA 测试

基于网络安全等级保护框架下
工业控制系统兼容性
和网络性能测试
——威努特&MOXA 联合测试
测试报告

北京威努特技术有限公司

摩莎科技（上海）有线公司

2019 年 1 月

联合性能测试报告

兼容性声明

本报告由摩莎科技（上海）有限公司与北京威努特技术有限公司联合发布。双方一致同意如下描述和结论。

双方就以下产品在通用系统上依照《信息安全技术 网络安全等级保护基本要求》开展了兼容性、功能性测试。双方产品功能、性能等方面均可正常完整实现与达成。

联合测试产品

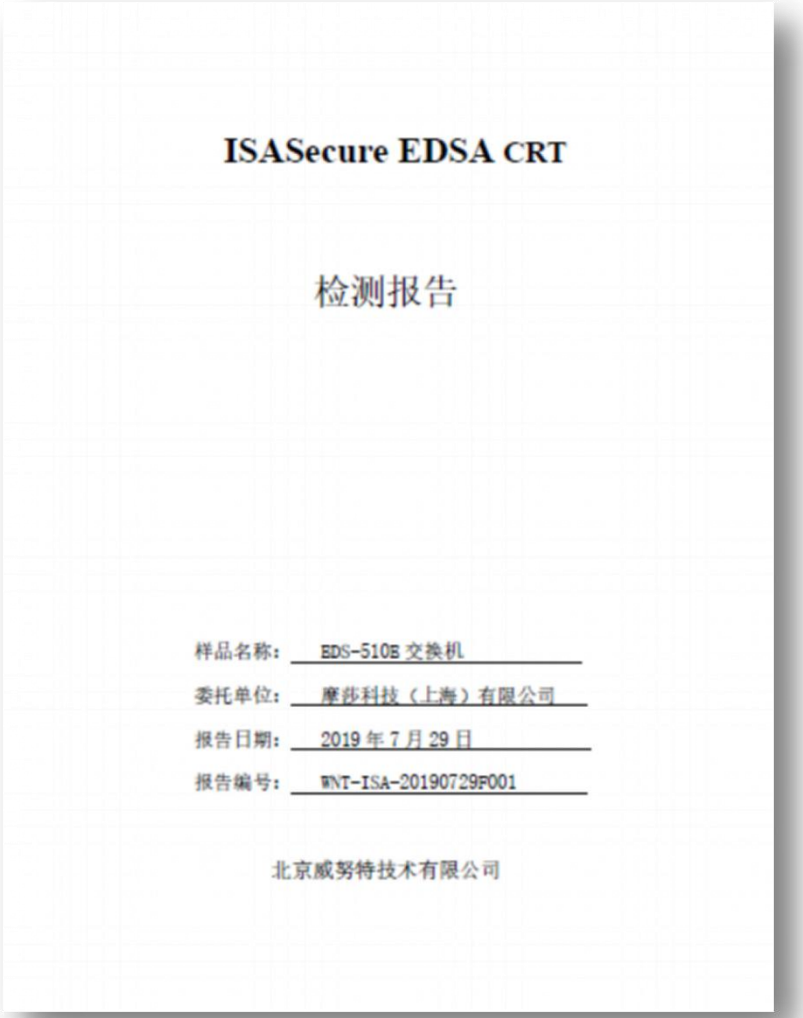
产品名称	制造商	地址
工业三层、二层网管交换机[1] 工业无线 工业网关	摩莎科技（上海）有限公司	上海市闵行区闵虹路 166 弄中虹环球创意中心 T3-3 层
工业防火墙[2] 工控安全监测与审计系统[3] 工控主机卫士[4] 统一安全管理平台[5] 入侵检测系统[6] 安全运维管理系统[7]	北京威努特技术有限公司	北京市海淀区上地三街嘉华大厦 F 座 901

[1]. 摩莎科技（上海）有限公司生产搭建，包含工业交换机、无线、网关，PLC 系统，仿真真实运行工业控制系统。
[2].北京威努特技术有限公司生产，应用于工业生产网络实现网络边界隔离、访问控制的软硬件一体化产品。
[3].北京威努特技术有限公司生产，应用于工业生产网络实现网络流量分析、异常监测的软硬件一体化产品。
[4].北京威努特技术有限公司生产，应用于工业生产网络实现工业主机应用程序启动控制，外设接口管理的软件产品。
[5].北京威努特技术有限公司生产，应用于工业生产网络实现对[2]、[3]、[4]集中管理的软硬件一体化产品。
[6].北京威努特技术有限公司生产，应用于工业生产网络，实现攻击监测、病毒检测的软硬件一体化产品。
[7].北京威努特技术有限公司生产，应用于工业生产网络，实现用户授权管理、综合审计的软硬件一体化产品。

摩莎科技（上海）有限公司
签章：
日期：2019 年 1 月 10 日

北京威努特技术有限公司
签章：
日期：2019 年 1 月 10 日

兼容性声明



ISASecure EDSA CRT

检测报告

样品名称：EDS-510B 交换机
委托单位：摩莎科技（上海）有限公司
报告日期：2019 年 7 月 29 日
报告编号：WNT-ISA-20190729P001

北京威努特技术有限公司

安全漏挖设备对交换机测试
威努特VMhunter

Thank You

摩莎 Moxa

扫一扫，关注我们

MOXA®
Reliable Networks ▲ Sincere Service