工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

工业控制系统核心区安全防护

汇报人：北京北信源软件股份有限公司、刘建兵
汇报日期： 2019年9月18日

工控安全威胁的性质

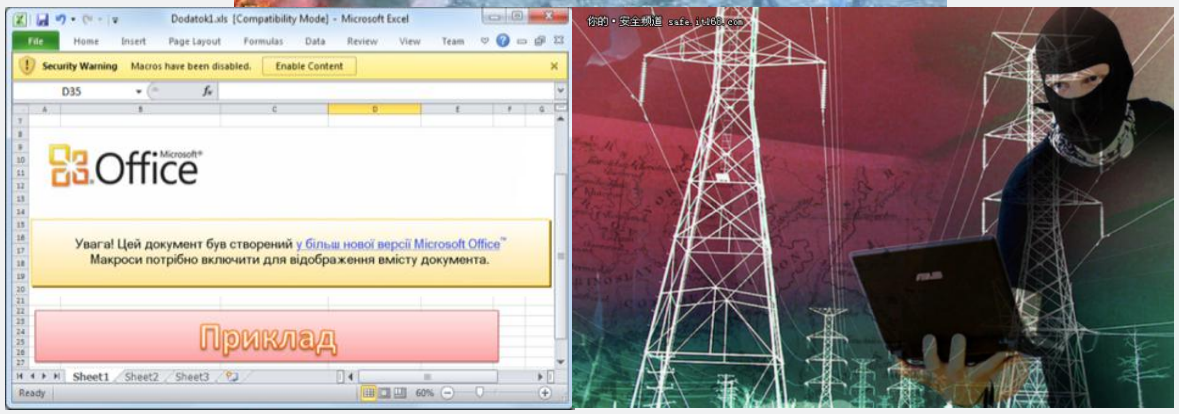
震网病毒

2010年，第一个专门针对大型工业计算机系统的蠕虫病毒-震网病毒出现了。最初研究人员看似病毒是要窃取工业机密，但9月份发现，这种蠕虫病毒是为了破坏伊朗的核计划而开发的。震网病毒会查找可编程逻辑控制器中的某些设置，并以伊朗布什尔省的核反应堆为目标。11月底，伊朗总统内贾德承认，这种病毒已经给该国的部分核离心机造成了问题。

- 准战争背景
- 国家力量
- 体系攻击

工控安全威胁的性质

乌克兰电网事件



2015年12月3日，乌克兰伊万诺－弗兰科夫斯克地区持续停电数小时之久。黑客使用后门程序BlackEnergy（黑暗力量）攻击了在发电站和多家能源公司。攻击者在微软Office文件中嵌入了恶意宏文件，并以此作为感染载体来对目标系统进行感染。乌克兰电网系统遭黑客攻击，数百户家庭供电被迫中断，这是有史以来首次导致停电的网络攻击，此次针对工控系统的攻击无疑具有里程碑意义。

- 战争状态
- 国家力量
- 体系攻击

工控安全威胁的性质

WannaCry 勒索病毒

2017年5月12日，WannaCry蠕虫通过MS17-010漏洞在全球范围大爆发，感染了大量的计算机，该蠕虫感染计算机后会向计算机中植入敲诈者病毒，导致电脑大量文件被加密。受害者电脑被黑客锁定后，病毒会提示支付价值相当于300美元（约合人民币2069元）的比特币才可解锁。

截止2017年5月15日，WannaCry造成至少有150个国家受到网络攻击，已经影响到金融，能源，医疗等行业，造成严重的危机管理问题

- 和平状态
- 国家力量
- 非针对性

工控威胁再认识

2018中国网络安全年会在北京举行。**安天创始人兼首席技术架构师肖新光**做了题为《敌情想定下的网络安全防御思考》

面对高级网空威胁行为体发动的攻击，我们必须考虑到：

- 高级威胁行为体有突破目标的坚定意志，且具有充足的资源、成本准备，并进行体系化的作业。
- 任何单点环节均可能失陷或失效，包括网络安全环节本身。
- 信息系统规划、实施、运维的全过程，都是攻击者的攻击时点。
- 防御者所使用的所有产品和环节同样是攻击方可以获得并测试的。
- 攻击者所使用的攻击装备有极大可能是“未知”的。

工控威胁再认识

正确的敌情想定是有效防护的前提

安天提出对于关键信息基础设施、重要信息系统等防御场景，“敌已在内、敌将在内”这是最基础和最重要的敌情想定。

思考一：基础信息技术自主先进和网络安全能力发展要相互促进发展，反对网络防御的虚无主义。

思考二：需要以体系化防御对决体系化的进攻，反对寻找银弹。

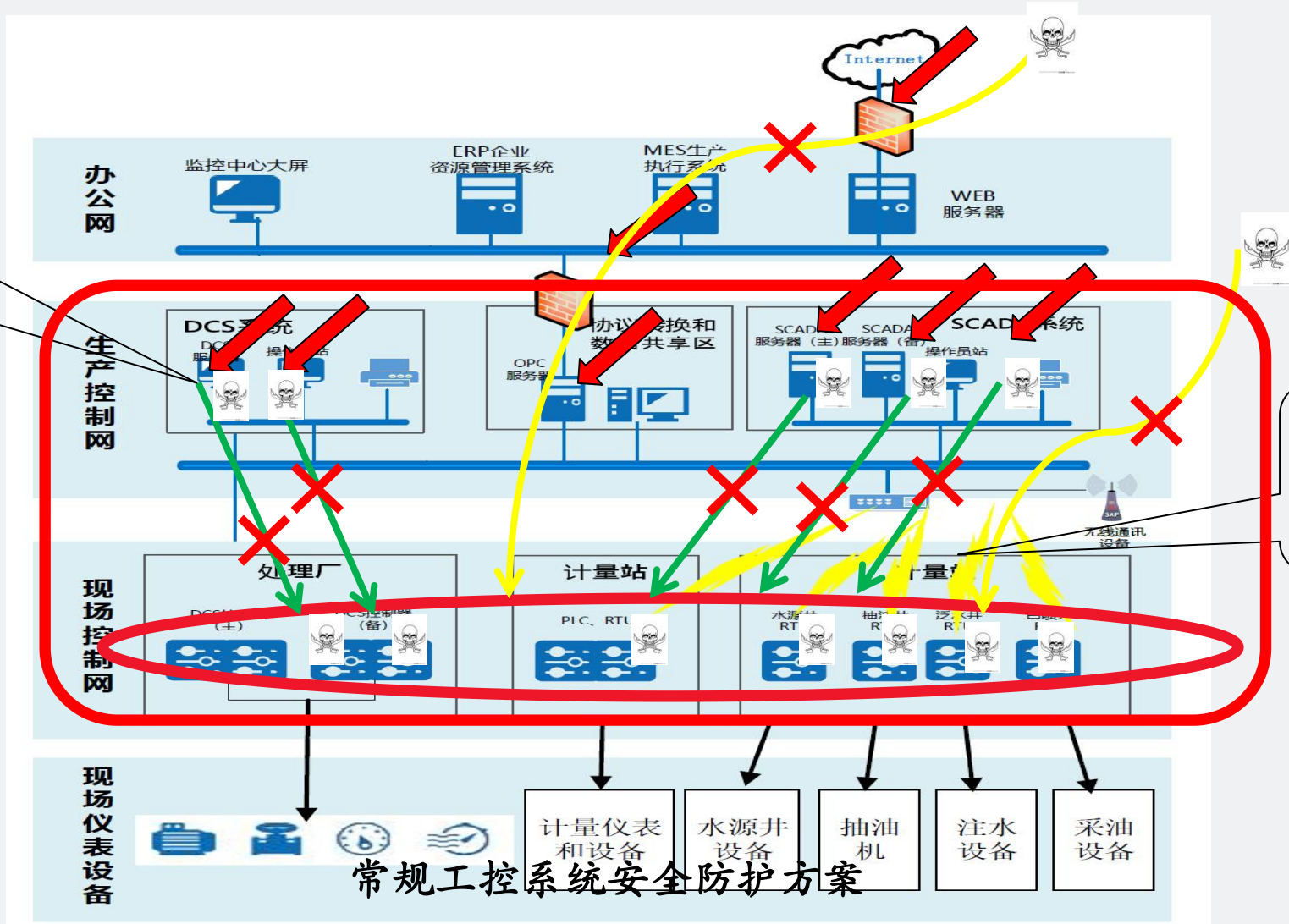
思考三：网络安全建设需要三同步叠加演进，走出先建设后安全的误区。

- 常规威胁和体系化威胁并存，体系化威胁是更致命的风险
- 需要秉持平战兼顾的理念，加强和提高应对体系化威胁的能力
- 在“分域防护、纵深防御”实践中，关注域内，拓展纵深

常规防护的问题

如何让
白名单白？

- 核心区域外围
- 快照式白名单



如何控制
核心区访问？

常规工控系统安全防护方案

常规防护的问题

防火墙不是保险箱

任何防火墙都是可以被攻破的，抵御一般攻击有效，应对体系化攻击风险大；
核心区域外围防护，一旦突破，全面失守，缺乏防御纵深；

快照式白名单白吗

严重依赖现场人员能力的自学习+人工配置，不能保证白名单是白的，可能包含了持久化工具；
快照式白名单是自我安慰的甜味剂，不能发挥体系的能力；

防护效果：可避日常风雨，难挡八级风暴

工业控制系统安全威胁的核心问题

国家利益：工业是国家战争能力的基础，保护工控系统就是保护国家利益

企业责任：肩负保护国家重要工业基础设施的责任

目标对手：重大利益冲突国家网军、国家力量背景黑客组织

核心问题：工业控制系统安全秉持平战兼顾，和平时期清除潜伏威胁，建立有效的防护体系

为应对八级风暴未雨绸缪

工业控制系统安全威胁的对策-三只锦囊

构建可信白名单：

采用新的技术机制研制自主可控的白名单验证工具，并基于检测认证体系建立工业主机进程的可信白名单库，弥补自学习和人工设定的缺陷，为生产装置提供可信白名单

建立核心区访问控制：

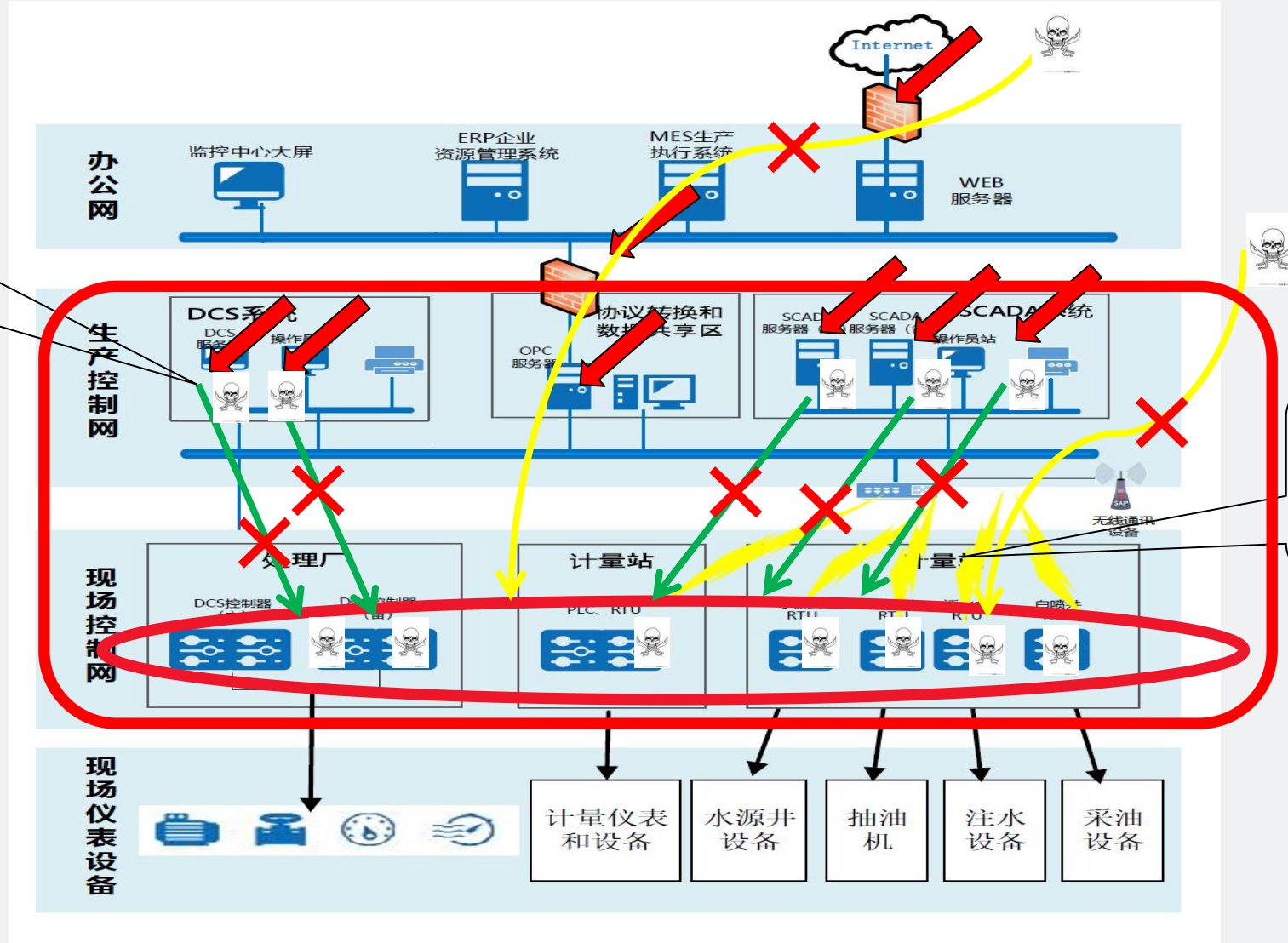
研发自主可控的工控安全交换机，提供核心区的访问控制能力，在工业现场实现基于可信白名单的工控核心区的访问控制策略，建立纵深防御能力

体系化建立企业/行业/国家检测认证机制：

依托自主可控的白名单验证工具和安全工控交换机，企业（国家）建立关联供应链的工控安全检测认证机制

工业控制系统安全威胁的对策-三只锦囊

如何让
白名单白？



如何控制
核心区访问？

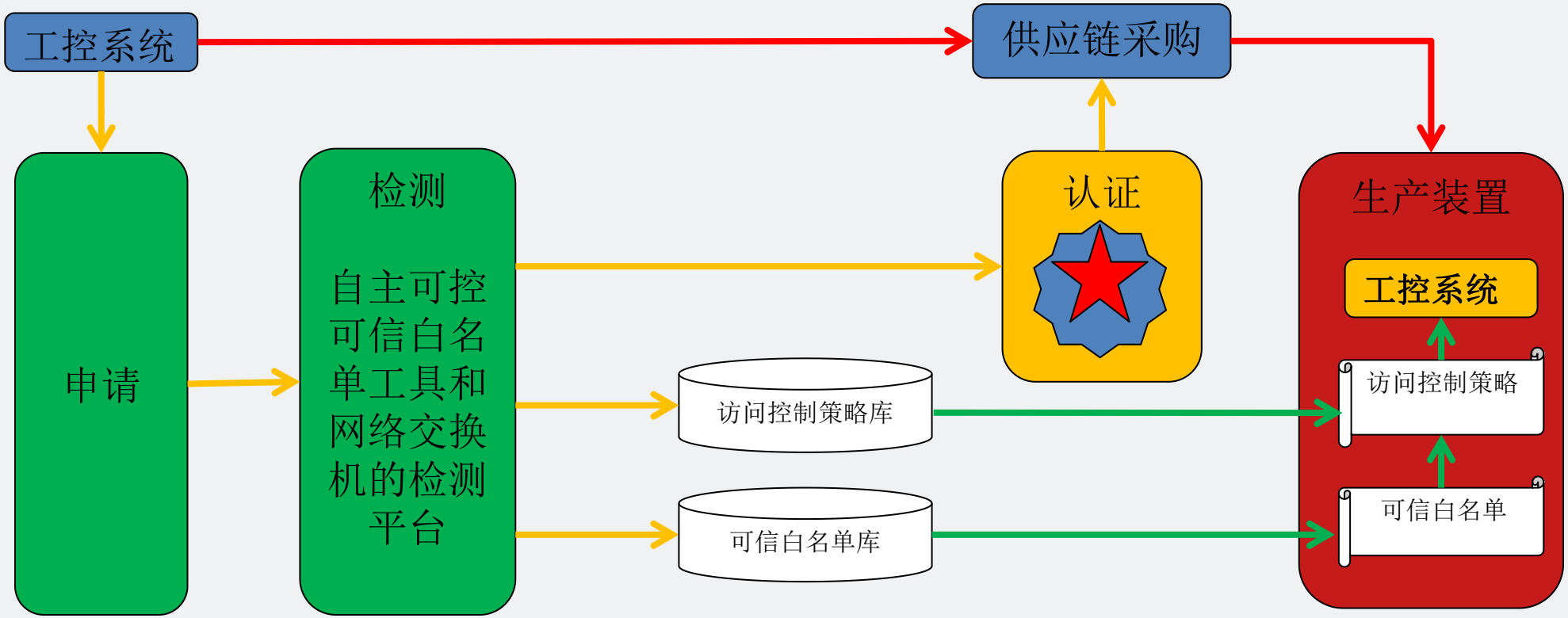
北信源工控安全解决方案

体系化的管理技术一体防护技术和产品，在外围防护的基础上，对工控系统核心区采用自主可控技术和产品加强防护，建立工控系统第二道防线，拓展防御纵深，以非对称技术取得工控核心区防护优势，平战兼顾，实现体系对抗下的核心区本质安全。

- 体系化：具备一定能力水平的组织行动，组织能力，技术能力，专业水平
- 体系化管理下的策略可信优势
- 体系化管理和技术对决体系化攻击

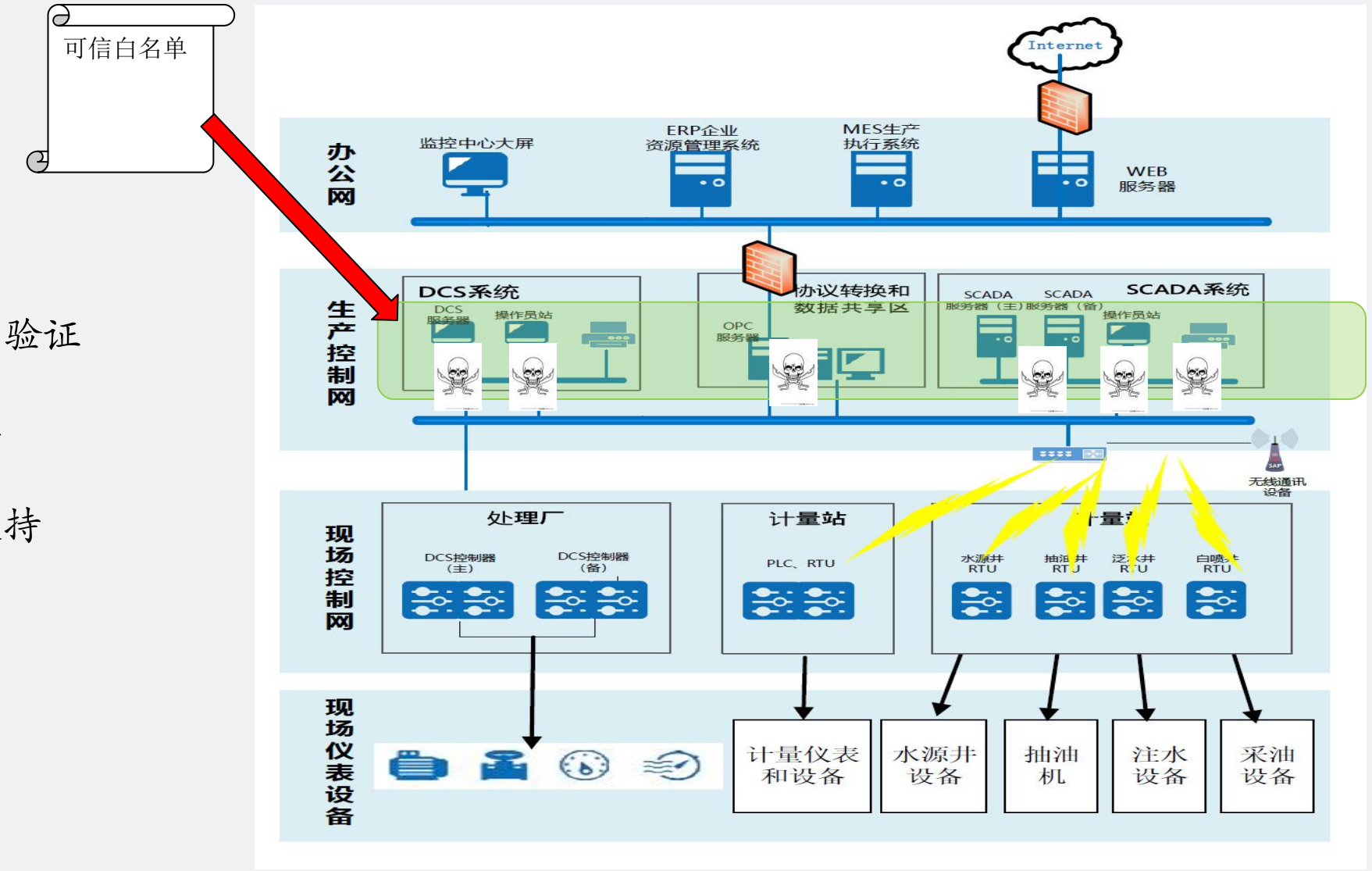
联系供应链的检测认证机制

凭借体系力量建立检测认证机制，全面掌握工控系统安全主导权，
建立可信的“两库”，体系化实施现场工控系统防护措施和策略



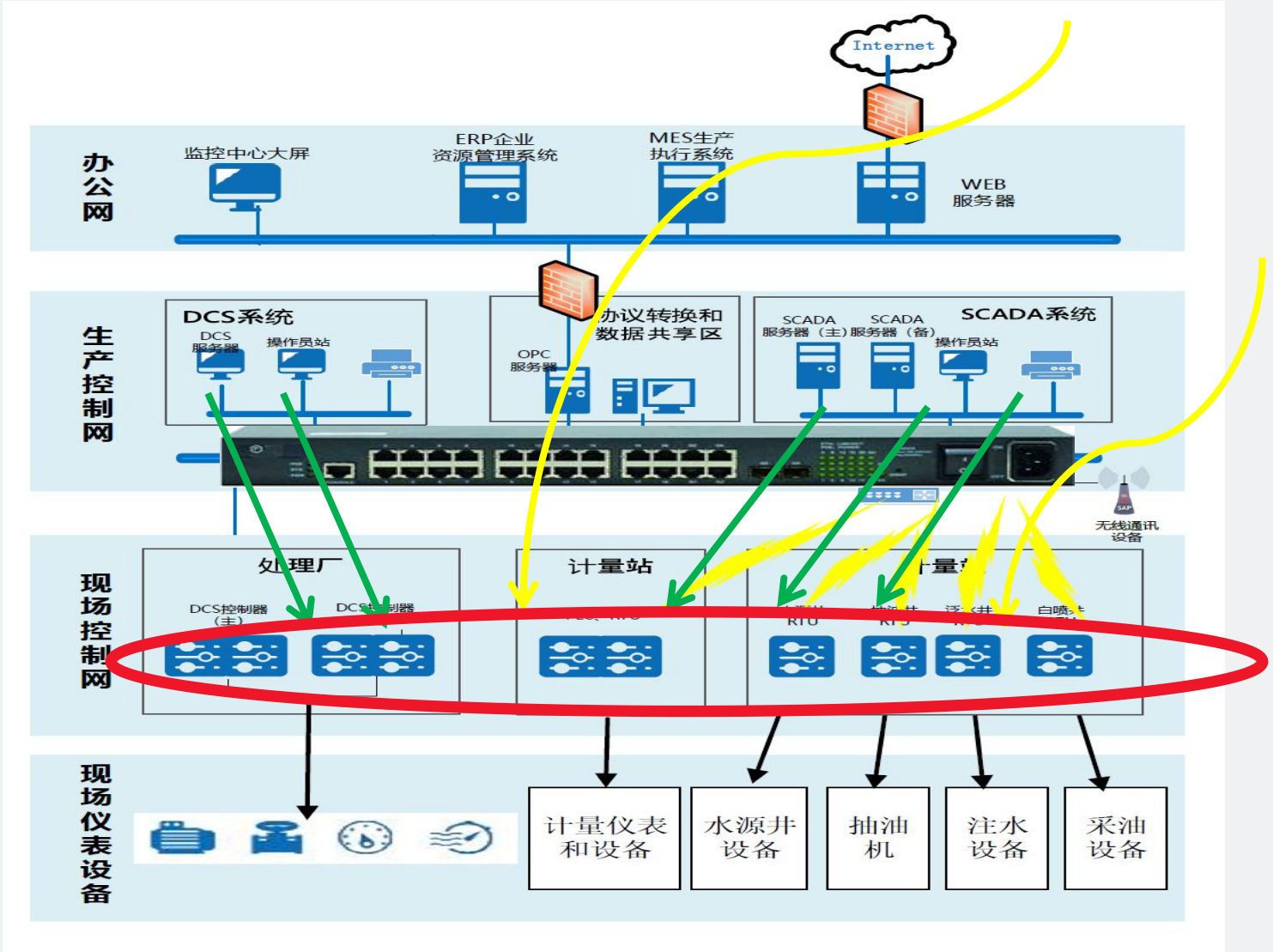
如何让白名单更白

- 体系化检测验证
- 白名单工具
- 专业知识支持



核心区访问控制

- 门户洞开畅通无阻
- 没有纵深
- 相互之间没有控制

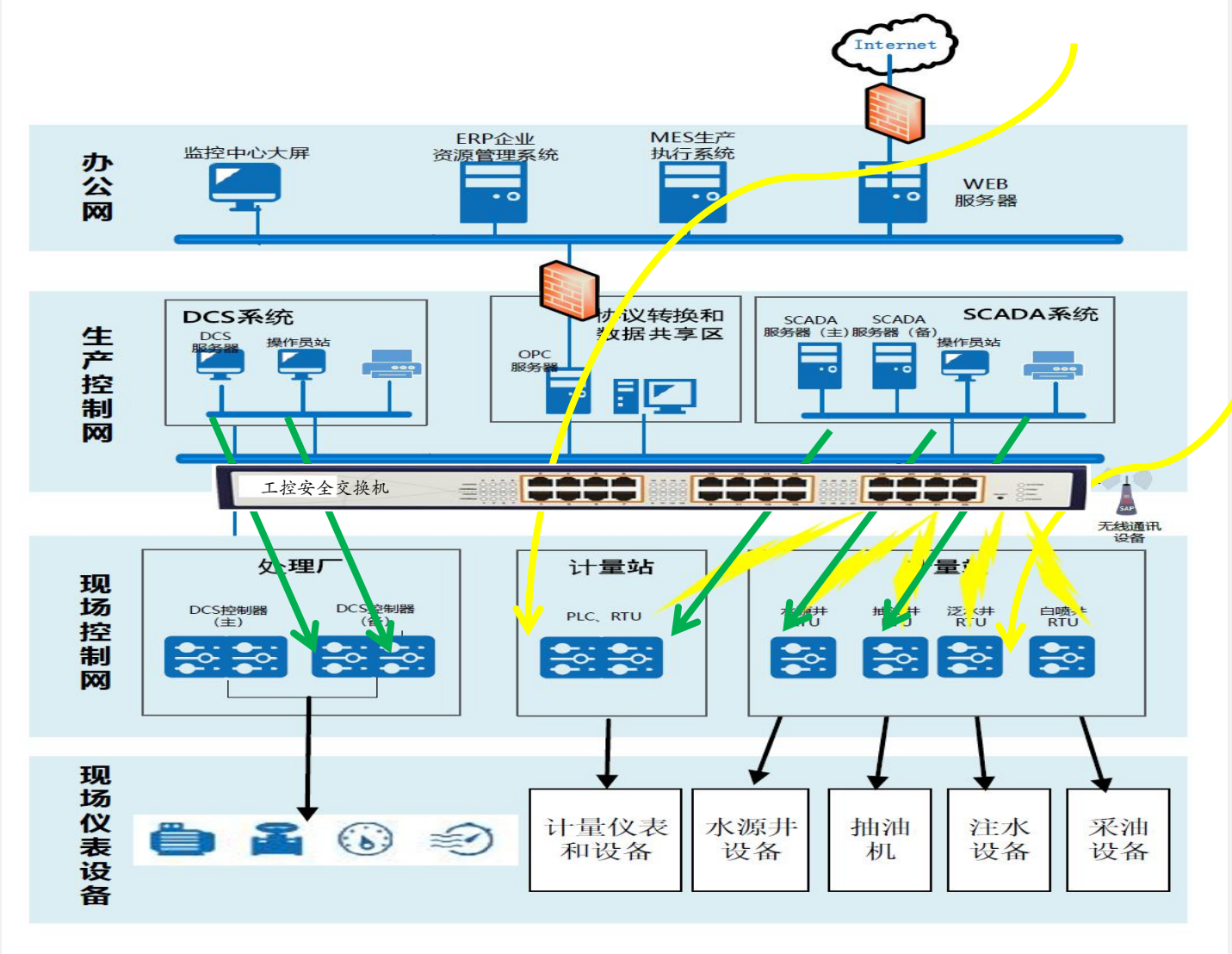


核心区访问控制

如果工控安全交换机

- 自主可控的硬件和固件
- 二层数据包的访问控制
- 基于IP、协议的控制粒度
- 指定端口的配置
- 物理端口的接入控制
- 流量输出的镜像能力

就可以将可信白名单和访问控制联系起来，切断网络攻击路径，实现纵深防御



北信源产品和技术

安全工业网络交换机，亲手设计，亲身打造，自主可控，独特创新，分布架构，边缘计算，国密算法，专利加持，为工控安全提供全新解决方案，拓展防御纵深，保护工控核心，是构筑工控安全新防线的不二之选。

北信源工安卫士，是基于北信源终端安全多年技术积淀，符合工控行业主机安全防护要求的综合防护软件，也是安全工业交换机的最佳搭档。

北信源产品和技术

安全工业交换机

机架式核心汇聚交换机

VRV 7032

导轨式接入交换机

VRV 6211

导轨式无线交换机

VRV 6220

北信源产品和技术

硬件技术指标

机架式核心汇聚交换机

VRV 7032

关键特性

- 支持可选4个万兆端口，满足更高带宽需求
- 支持ABRing极速分布式自愈环，自愈时间小于5ms
- 支持静态路由、RIPv1/v2、OSPF v2等路由技术
- 支持PIM-DM、PIM-SM 组播路由协议
- 支持IGMP Snooping,、静态组播
- 支持VLAN、QoS、GVRP、LACP、RSTP/MSTP、VRRP、IGMP Snooping、ACL等管理功能
- 支持端口聚合，端口限速，广播风暴抑制
- 支持DHCP snooping、IP Source Guard、ARP Inspection 等网络安全功能
- 支持ABView集中式管理系统，可视化拓扑状态管理
- 支持专用管理端口接入，提升网络安全
- 支持远程端口镜像功能，方便远程诊断
- 支持SNMPv1/v2c/v3、Console、Telnet、Web等多种网络管理方式
- 符合工业四级电磁兼容性要求
- 绿色工业以太网，无风扇、低功耗设计
- 多种可选电源电压输入
- 冗余双电源输入设计
- 宽温工作（-40℃～+85℃）
- 满足严苛工业环境可靠工作要求
- IP40防护等级，金属外壳

北信源产品和技术

硬件技术指标

导轨式接入交换机

VRV 6211

关键特性

- 支持ABRing极速分布式自愈环网技术
- 网络故障自愈时间小于5ms
- 支持可选断电光路保护功能
- 支持IEEE802.1Q VLAN、PVLAN设置
- 支持IEEE802.1P QoS功能，支持WRR(加权循环队列)
- 支持端口聚合，端口限速，广播风暴抑制
- 支持DHCP snooping、IP Source Guard、ARP Inspection 等网络安全功能
- 支持完备的ACL策略，支持L2-L4 层线速过滤
- 支持ABView集中式管理系统，可视化拓扑状态管
- 支持专用管理端口接入，提升网络安全
- 支持远程端口镜像功能，方便远程诊断
- 支持SNMPv1/v2c/v3、Console、Telnet、Web等多种网络管理方式
- 符合工业四级电磁兼容性要求
- 绿色工业以太网，无风扇、低功耗设计
- 多种可选电源电压输入
- 冗余双电源输入设计
- 宽温工作（-40℃～+85℃）
- 满足严苛工业环境可靠工作要求
- IP40防护等级，金属外壳

北信源产品和技术

硬件技术指标

导轨式无线交换机

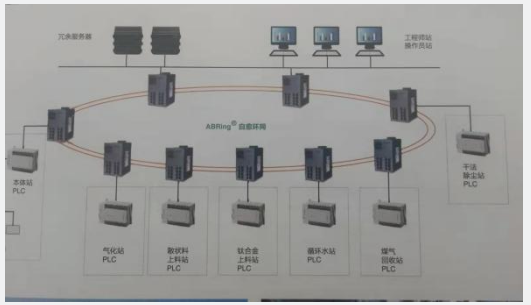
VRV 6220

关键特性

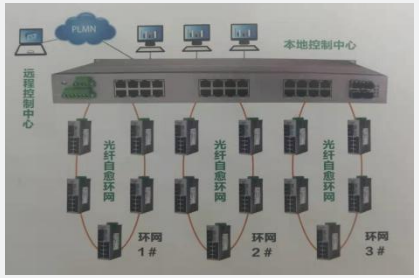
- 支持ABRing极速分布式自愈环技术，自愈时间小于5ms
- 支持8个百兆以太网电口，2个千兆SFP插槽
- 支持2.4GHz&5GHz无线AP功能，支持2*2 MIMO
- 支持1路4G全网通无线路由接口
- 支持超宽工作温度范围：-40℃～+85℃
- 符合工业四级的EMC电磁兼容性能
- 工业级设计，坚固铝合金外壳，抗冲击，防震动
- 支持VLAN、Qos、LACP、RSTP、ACL、IGMP snooping等丰富的管理功能
- 支持CONSOLE、WEB、TELNET、SNMP、ABView等多种网络管理方式
- 支持网管系统可视化拓扑管理，支持批量配置操作，提升维护管理效率

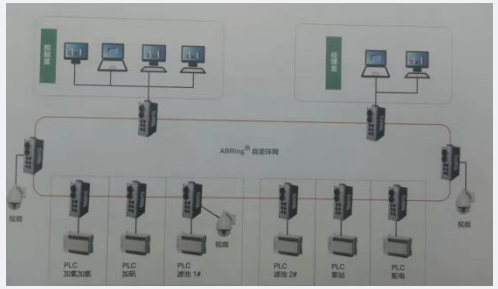
北信源产品和技术

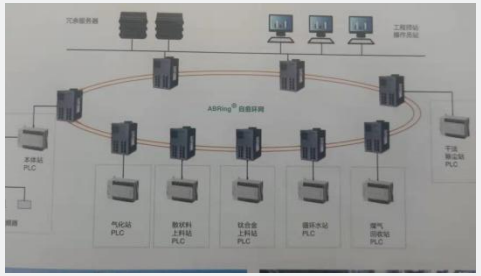
拓扑图

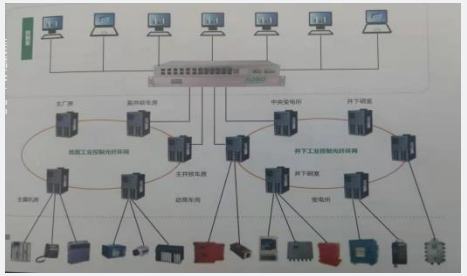


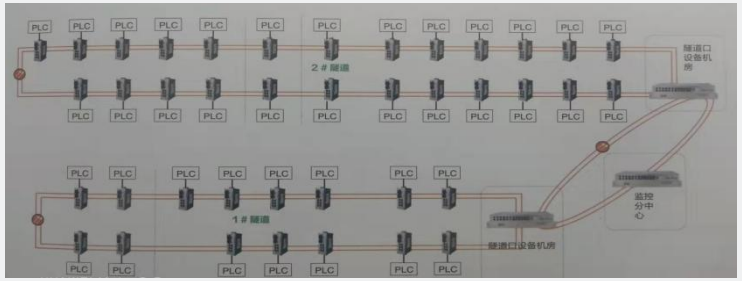
支持多种组网结构，
自愈环网适应工控
可靠性要求，灵活
可靠











北信源产品和技术

安全功能

1、专属管理端口功能

仅允许交换机的特定以太网端口访问交换机的管理IP地址对交换机进行管理和配置。禁止通过网络远程登陆交换机进行管理和配置，消除将远程配置作为攻击手段的可能性，规避交换机被远程控制的安全风险。

该功能复合了下面的“嵌入认证”功能，使交换机的管理配置不仅限制于本地特定端口，还将网络安全管理者的管理意志融入设备功能，只有网络安全管理者指定的计算机设备才能进行，改变当前网络安全管理依赖工程师，工程师不受管理控制的状况。

北信源产品和技术

安全功能

2、访问控制功能

该功能用于建立工控环境的合法通讯规则，强化合法应用的合法通讯控制能力，大幅提升防火墙类安全措施无法解决的区域内部安全能力，保证合法应用的通讯，拒绝非法应用的网络访问，对防火墙分域防护后的域内防护提供了全新的技术手段。工控网络目前完全没有实施基于交换机的网络访问控制，任何应用在网中自由通讯，业务应用没有受保护，无关应用没有被限制，这也是造成工控网络中一台主机失守，系统全线崩溃的根本原因。通过该功能在工控网络实施严格的访问控制策略，可以彻底改变目前状态，特别是保护对生产业务至关重要的PLC不受攻击。

当然，实现工控网络访问控制的规则制订和验证实施是个艰难的工作，很多用户或基于对业务细节不了解、对系统软硬件细节不了解、网络安全知识薄弱、国外厂商不支持等原因，知难而退，无功而返。但是这个工作意义重大，可能是提高工控网络安全的重要措施，可能成为未来工控安全的主要着力点。解决这个难题，不仅需要用户、厂商、产品、技术、服务等多方面的合作，更需要体系化的管理和监督，撬开这个黑盒，必将大大提升操控网络安全风险的能力。为此，北信源工安卫士专门设计了访问控制功能，可以深入的获取和直观展示主机应用和网络访问的关联关系，是获取和分析网络访问了基础数据的有力支持工具。

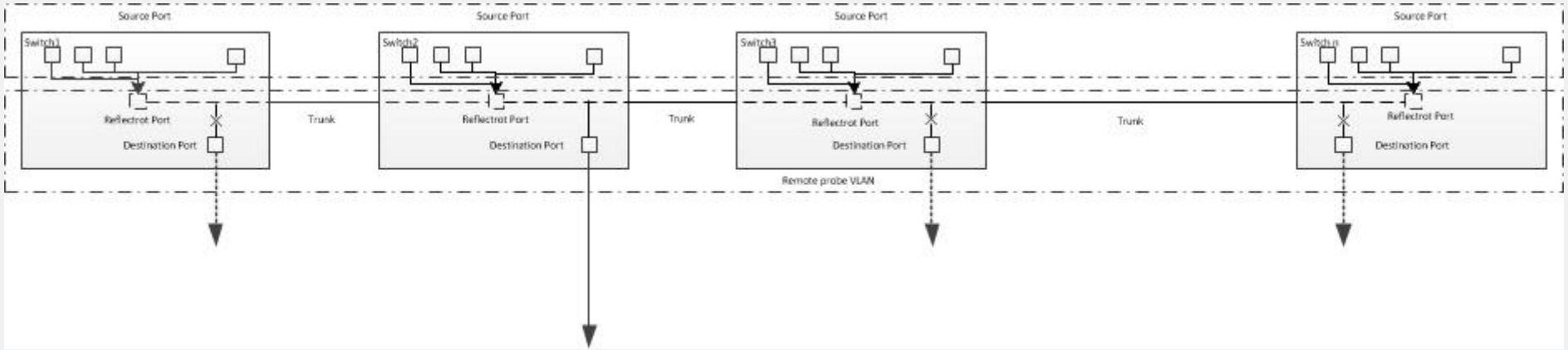
北信源产品和技术

安全功能

3、全数据输出功能

该功能在交换机内部预置了352vlan，启用该功能后，352vlan在所有北信源交换机透传，并且所有交换机端口流量将被镜像到352vlan，并在交换机唯一指定端口输出。

该特性可以实现全网数据的完全获取和集中输出，为监视工控网络数据流量、分析发现异常数据提供了极大的便利，并且可使分析数据来源完整。



北信源产品和技术

安全功能

4、内嵌认证

该功能将认证准入功能和交换机一体化，认证和准入功能内嵌在交换机中，认证和准入服务不受外部影响，系统功能可靠。所有设备接入后交换机根据配置的认证策略主动、周期对终端发起认证。在通过认证之前，不允许来自该终端的数据包被交换机转发。基于国密算法SM2，遵从X.509数字证书标准，支持IPv6。

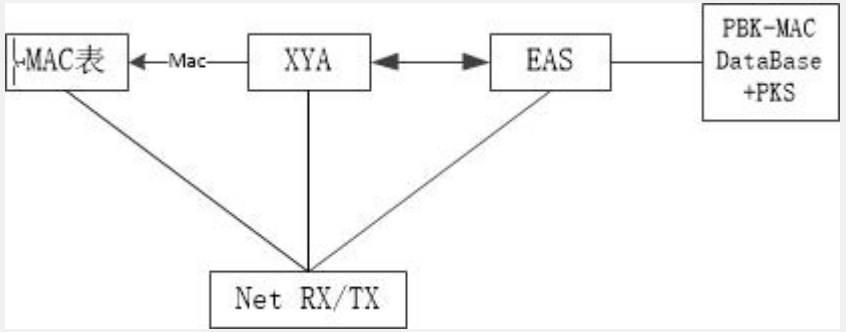
该特性在交换机接入端口实现合法接入设备的身份认证和准入控制，包括互联的网络设备，都在内嵌认证的控制之下运行，不在认证系统内的设备不能通过认证，即不能在交换机上传输任何数据，为保证工控网络环境中设备的合法接入使用提供了有力的手段，将域内网络接入提高到严格的水平，阻止外来设备接入网络造成的攻击，是强力有效的安全措施。

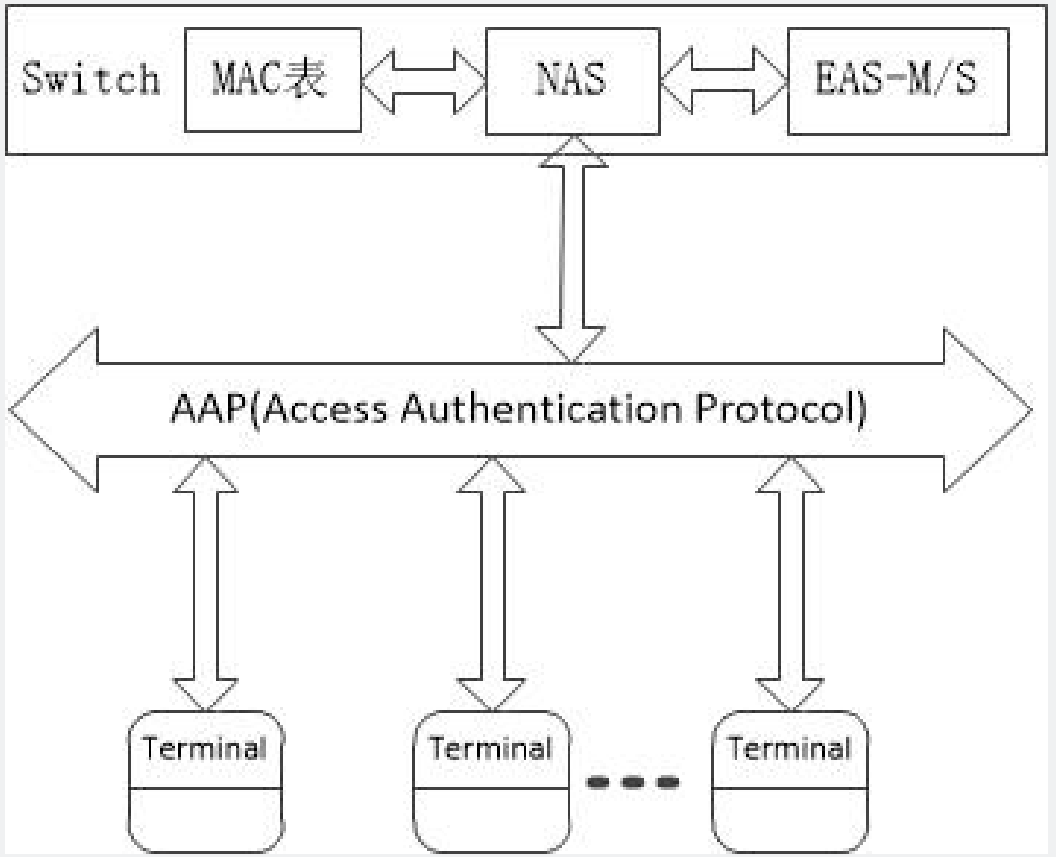
北信源产品和技术

创新技术

AAP:Access Authenitication Protocol，接入认证协议，内嵌认证中实现接入对象到交换机的认证准入数据和通讯规程。通过AAP实现XYA认证。

XYA：Xinyuan Authenitication，信源认证，特指EA实现的认证方式，通过AAP和ADSP在网络接入交换机上运行。

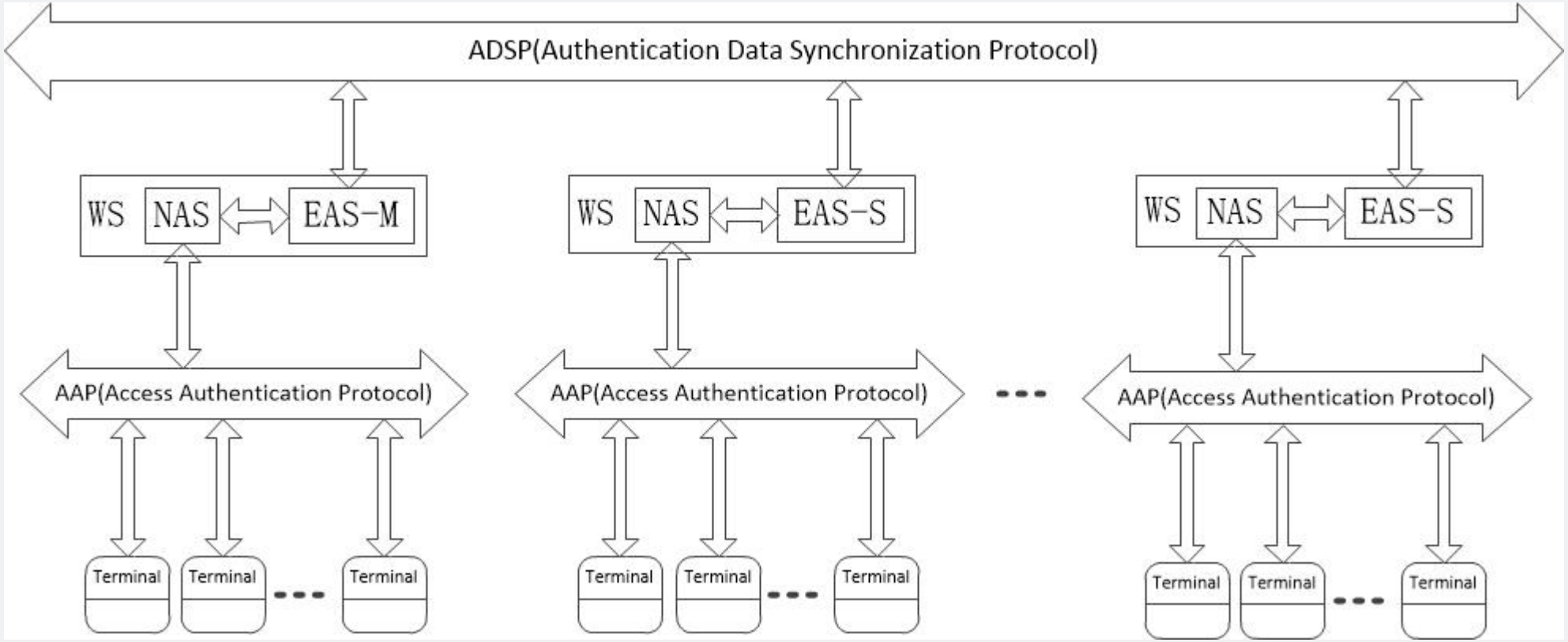




北信源产品和技术

创新技术

ADSP:Authenitication Data Synchronization Protocol，认证数据同步协议，内嵌认证中实现多个EAS间认证数据同步的数据和通讯规程。



北信源产品和技术

工安卫士

“北信源工安卫士”是北信源公司集20年终端管理经验，在千万级计算机终端安全方面获取的技术经验针对工控系统开发的主机安全软件，融合自适应安全理念和高效、稳定、兼容、易于设置的终端安全检测与防护技术，是新一代操作员站、工程师站、服务器等工业现场主机上进行安全防护加固的软件产品。

软件遵循“三权分立”模式，提供可信白名单、移动存储管理、访问控制、文件完整性保护、系统基线、日志六大实用功能。同时兼顾管理和技术融合，符合工业控制数据管理习惯。

北信源产品和技术

工安卫士

1、可信白名单库功能：

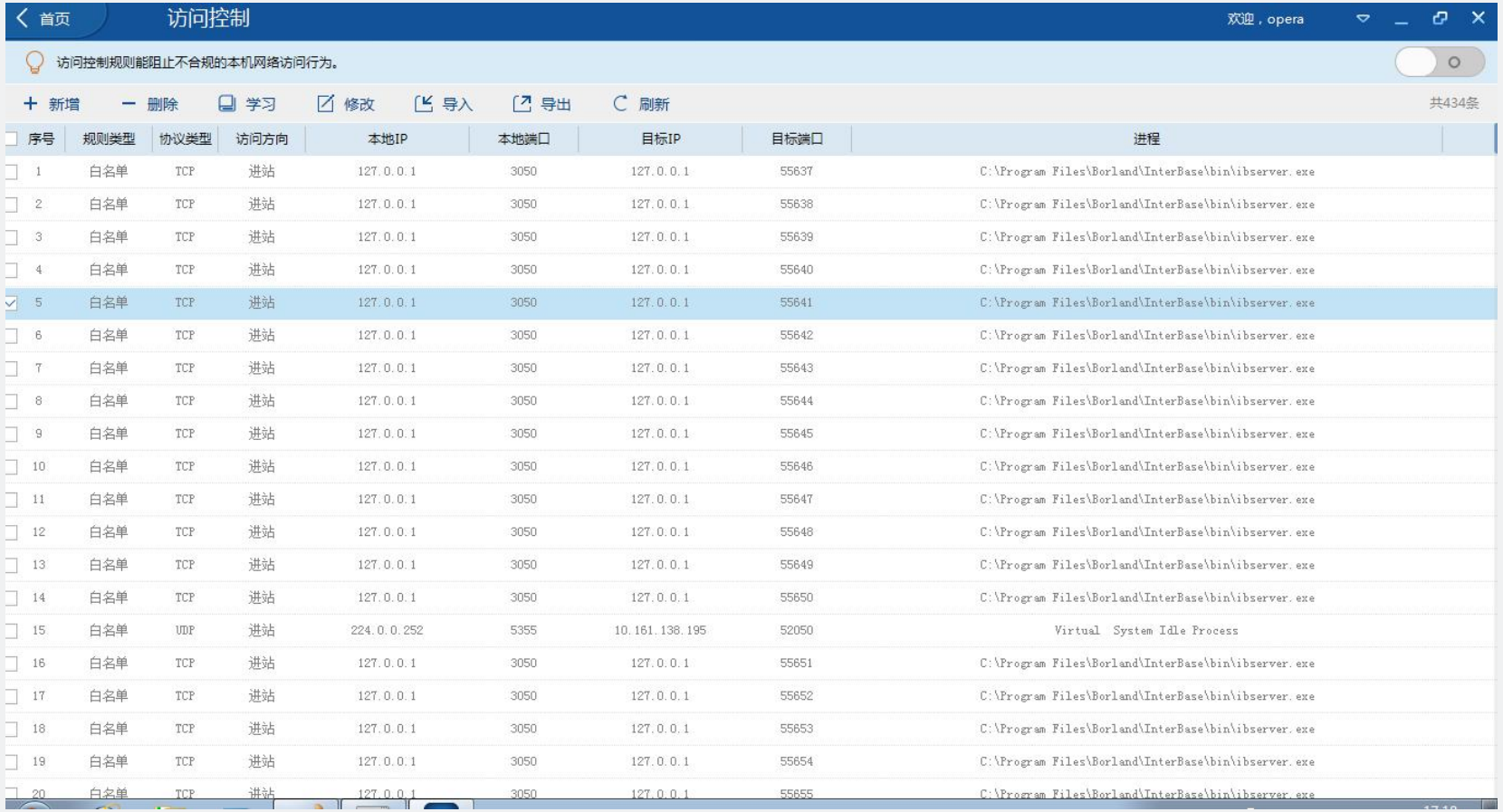
提供主机进程名单的获取和编辑和导入功能，提供管理者、网络安全专家参与进程名单的甄别和控制机制，是现场工程师和管理者融合互动。不同于现有安全软件产品进程“快照”方式添加到白名单中，开创性的把软件进程控制与进程白名单管理分开，实际有效的解决终端安全问题。

序号	进程名	来源	是否签名	进程完整路径	大小（字节）
1	BLPolicyCfgTool.exe	Beijing VRV Software...	否	E:\工作\产品文档\L-技术资料\基线策略编辑工具2015111303\BLP...	1830400
2	BLPolicyCfgTool.exe	Beijing VRV Software...	否	D:\SRC\JJ_Src\client\VRVJinjia\standard\BLPolicyCfgTool\中石...	1830400
3	BLPolicyCfgTool.exe	Beijing VRV Software...	否	C:\Program Files (x86)\TSIC\Data\BaseLine\BLPolicyCfgTool.exe	1777664
4	EdpKMLock.exe	Beijing VRV Software...	是	C:\Program Files (x86)\TSIC\EdpKMLock.exe	237480
5	EdpKMLock.exe	Beijing VRV Software...	是	C:\Windows\SysWOW64\EdpKMLock.exe	237248
6	EncryptDb.exe	BEIJING VRV SOFTWA...	否	C:\Users\Administrator\Desktop\基线测试工具\EncryptDb.exe	41472
7	EncryptDb.exe	BEIJING VRV SOFTWA...	否	C:\Program Files (x86)\TSIC\Data\BaseLine\EncryptDb.exe	41472
8	EncryptDb.exe	BEIJING VRV SOFTWA...	否	D:\Documents\Tencent Files\413622513\FileRecv\BL\BL\Encry...	41472
9	ResBaseline.exe		是	D:\SRC\SetupStore\Beta\SouceFiles\JJFX\files\gongan\JJFX\A...	155504
10	ResBaseline.exe		是	D:\SRC\SetupStore\Alpha\SouceFiles\JJFX\files\gongan\JJFX\...	155504
11	ResBaseline.exe	Beijing VRV Software...	否	C:\Program Files (x86)\TSIC\Data\BaseLine\ResBaseline.exe	139264
12	ResBaseline.exe		是	D:\SRC\SetupStore\Alpha\SouceFiles\JJFX\files\guowang\JJF...	155504
13	ResBaseline.exe	Beijing VRV Software...	否	D:\SRC\JJ_Src\client\GA III\项目信息\APP\AppPlugin\系统加固\...	139264
14	ResBaseline.exe	Beijing VRV Software...	否	D:\SRC\JJ_Src\client\VRVJinjia\standard\BLPolicyCfgTool\基线...	139264

北信源产品和技术

工安卫士

2、进程访问控制功能不同于现有安全软件产品白名单进程中的任何访问功能全部允许网络访问，工安卫士可进行针对进程的网络访问进行控制，防止进程中有后门隐藏网络访问。同时该功能将系统进程和网络访问关联起来，直观的展示业务进程的网络访问关系，为在交换机上建立网络访问控制规则提供数据和工具。



序号	规则类型	协议类型	访问方向	本地IP	本地端口	目标IP	目标端口	进程
1	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55637	C:\Program Files\Borland\InterBase\bin\ibserver.exe
2	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55638	C:\Program Files\Borland\InterBase\bin\ibserver.exe
3	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55639	C:\Program Files\Borland\InterBase\bin\ibserver.exe
4	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55640	C:\Program Files\Borland\InterBase\bin\ibserver.exe
5	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55641	C:\Program Files\Borland\InterBase\bin\ibserver.exe
6	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55642	C:\Program Files\Borland\InterBase\bin\ibserver.exe
7	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55643	C:\Program Files\Borland\InterBase\bin\ibserver.exe
8	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55644	C:\Program Files\Borland\InterBase\bin\ibserver.exe
9	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55645	C:\Program Files\Borland\InterBase\bin\ibserver.exe
10	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55646	C:\Program Files\Borland\InterBase\bin\ibserver.exe
11	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55647	C:\Program Files\Borland\InterBase\bin\ibserver.exe
12	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55648	C:\Program Files\Borland\InterBase\bin\ibserver.exe
13	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55649	C:\Program Files\Borland\InterBase\bin\ibserver.exe
14	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55650	C:\Program Files\Borland\InterBase\bin\ibserver.exe
15	白名单	UDP	进站	224.0.0.252	5355	10.161.138.195	52050	Virtual System Idle Process
16	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55651	C:\Program Files\Borland\InterBase\bin\ibserver.exe
17	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55652	C:\Program Files\Borland\InterBase\bin\ibserver.exe
18	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55653	C:\Program Files\Borland\InterBase\bin\ibserver.exe
19	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55654	C:\Program Files\Borland\InterBase\bin\ibserver.exe
20	白名单	TCP	进站	127.0.0.1	3050	127.0.0.1	55655	C:\Program Files\Borland\InterBase\bin\ibserver.exe

北信源产品和技术

工安卫士

3、系统基线管理：
可对系统基线安全加固处理，增加系统安全性能，降低攻击便利性；功能设立12种系统基线可在软件上进行设置。系统基线，对主机本身相关安全策略进行管理，如审核登录事件、审核账户登陆事件、密码杂复性要求、密码长度要求、密码周期要求、交互式登录要求、账户锁定阀值等。

北信源产品和技术

工安卫士

4、移动存储管理
可通过多种方式对移动存储设备进行授权，只有授权的U盘才可以在本主机上使用。

北信源产品和技术

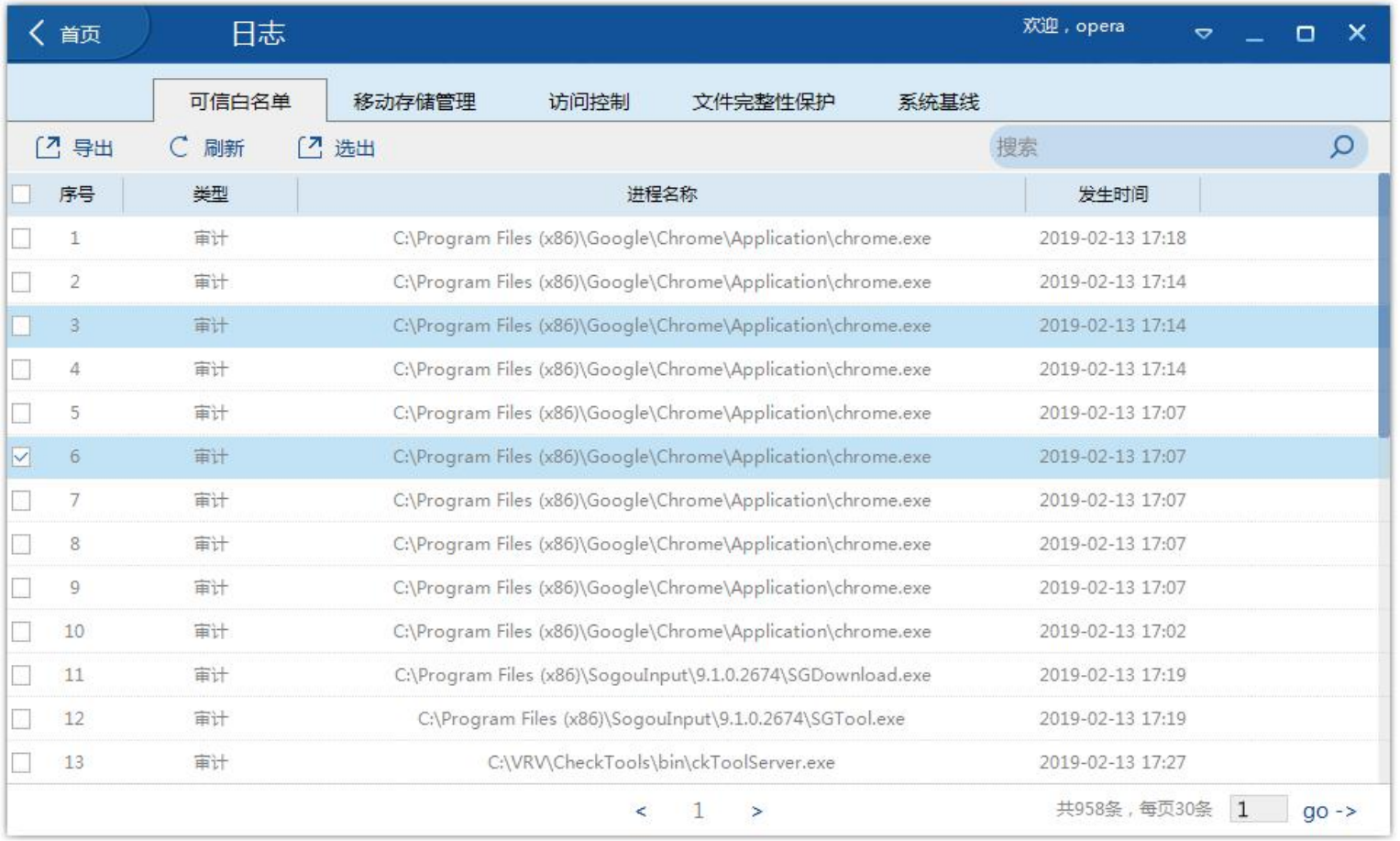
工安卫士

5、文件完整性
重要文件完整性保护，对特定文件及程序进行完整性保护，防止被篡改、删除。

北信源产品和技术

工安卫士

6、日志告警：
探测到非法进程、非法网络端口、非法USB设备时，会产生安全事件，提醒用户。

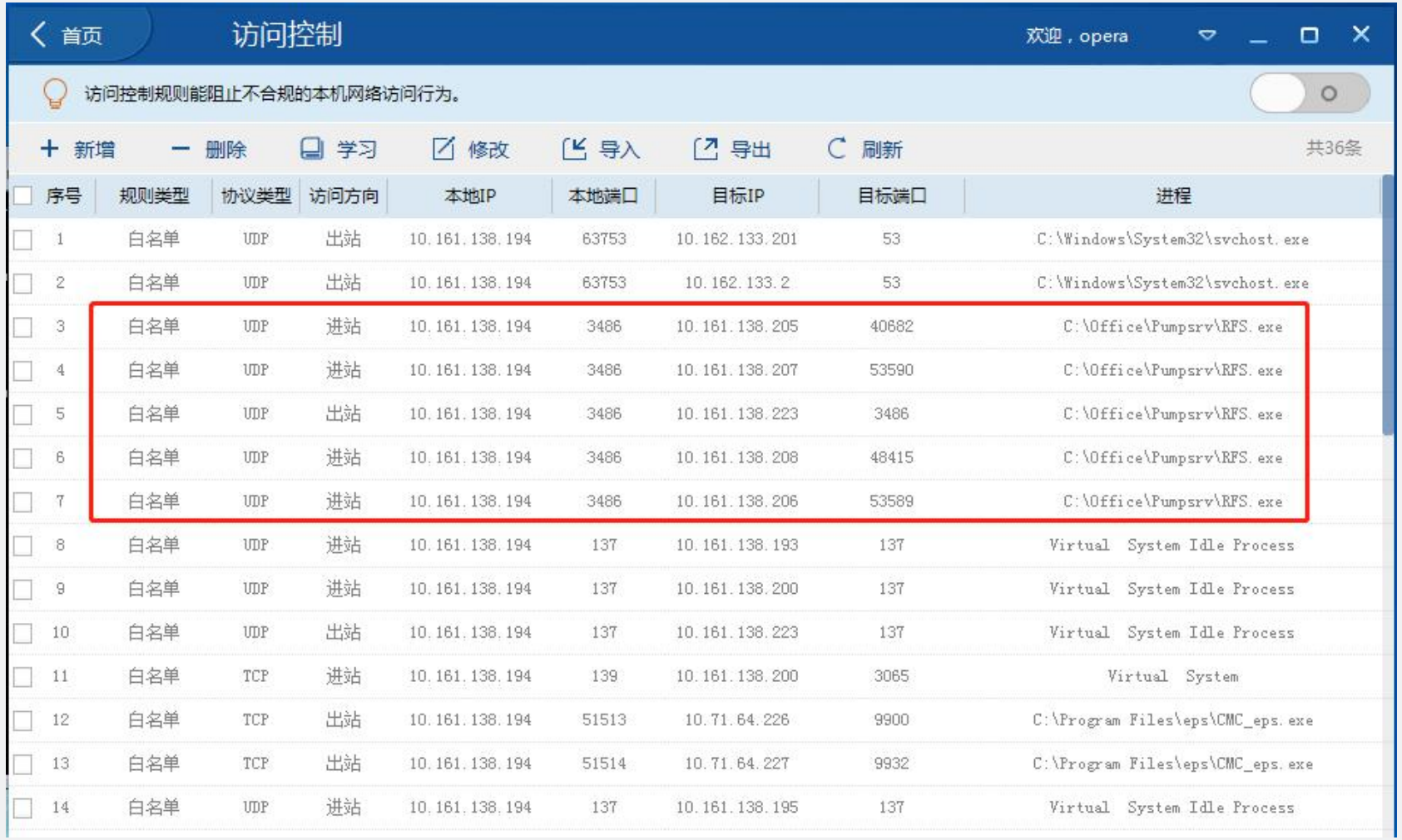


让工控更安全

北信源产品和技术

工安卫士

通过工安卫士，获取正常业务通讯关系，发现异常通讯，是建立交换机ACL的有力工具。



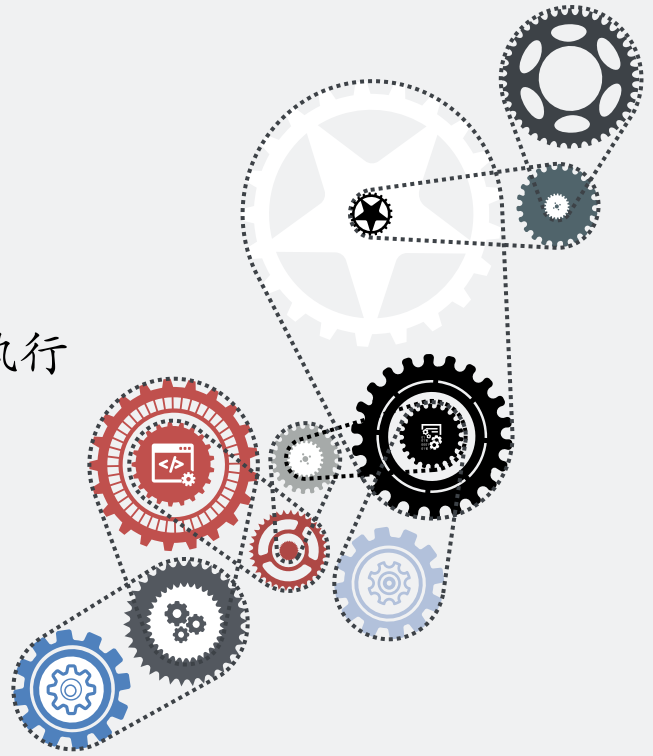
序号	规则类型	协议类型	访问方向	本地IP	本地端口	目标IP	目标端口	进程
1	白名单	UDP	出站	10.161.138.194	63753	10.162.133.201	53	C:\Windows\System32\svchost.exe
2	白名单	UDP	出站	10.161.138.194	63753	10.162.133.2	53	C:\Windows\System32\svchost.exe
3	白名单	UDP	进站	10.161.138.194	3486	10.161.138.205	40682	C:\Office\Pumpsrv\RFS.exe
4	白名单	UDP	进站	10.161.138.194	3486	10.161.138.207	53590	C:\Office\Pumpsrv\RFS.exe
5	白名单	UDP	出站	10.161.138.194	3486	10.161.138.223	3486	C:\Office\Pumpsrv\RFS.exe
6	白名单	UDP	进站	10.161.138.194	3486	10.161.138.208	48415	C:\Office\Pumpsrv\RFS.exe
7	白名单	UDP	进站	10.161.138.194	3486	10.161.138.206	53589	C:\Office\Pumpsrv\RFS.exe
8	白名单	UDP	进站	10.161.138.194	137	10.161.138.193	137	Virtual System Idle Process
9	白名单	UDP	进站	10.161.138.194	137	10.161.138.200	137	Virtual System Idle Process
10	白名单	UDP	出站	10.161.138.194	137	10.161.138.223	137	Virtual System Idle Process
11	白名单	TCP	进站	10.161.138.194	139	10.161.138.200	3065	Virtual System
12	白名单	TCP	出站	10.161.138.194	51513	10.71.64.226	9900	C:\Program Files\eps\CMC_eps.exe
13	白名单	TCP	出站	10.161.138.194	51514	10.71.64.227	9932	C:\Program Files\eps\CMC_eps.exe
14	白名单	UDP	进站	10.161.138.194	137	10.161.138.195	137	Virtual System Idle Process

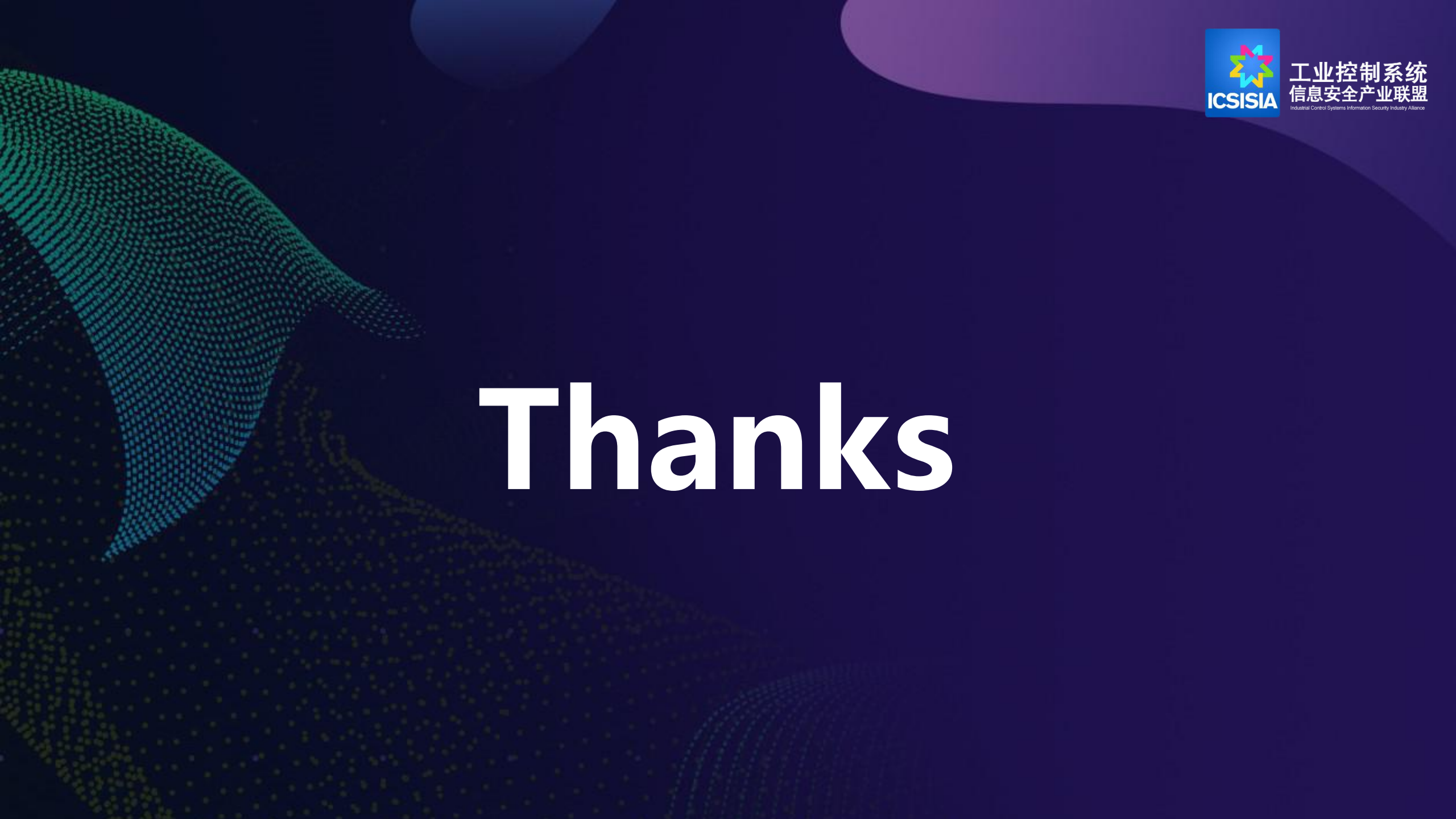
北信源产品和技术

工安卫士

三分技术，七分管理，管理和技术融合，防止管理失控，管理端和操作端分离，各负其责，操作不能越权，策略上下一贯。

- 嵌入认证：管理者可以授权操作者，也可以收回权限
- 数据导出：操作者必须导出数据给管理者确认，不能直接执行
- 数据导入：不许是来自管理者的合法数据才能导入执行
- 关联加密：导入导出数据在管理者和操作者之间绑定关系




ICSISIA
工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance
Thanks