工业互联网典型安全解决方案案例

编写说明

为落实《中国制造 2025》规划，工信部明确了工业转型升级的重点领域和工作要求。工业互联网作为新一代信息技术与工业系统深度融合形成的产业和应用生态，是全球工业系统与高级计算、分析、感应技术以及互联网连接融合的结果。它通过智能机器间的连接并最终将人机连接，结合软件和大数据分析，重构全球工业、激发生产力，让世界更美好、更快速、更安全、更清洁且更经济。工业互联网的发展得到全球主要国家以及我国政府的高度重视和积极推进，产业界也正在加速开展相关探索和实践。

工业互联网广泛应用于能源、交通以及市政等关系国计民生的重要行业和领域，已成为国家关键信息基础设施的重要组成部分。工业互联网打破了传统工业相对封闭可信的制造环境，病毒、木马、高级持续性攻击等安全风险对工业生产的威胁日益加剧，一旦受到网络攻击，将会造成巨大经济损失，并可能带来环境灾难和人员伤亡，危及公众安全和国家安全。工业互联网自身安全可控是确保其在各生产领域能够落地实施的前提，也是产业安全和国家安全的重要基础和保障。

本案例汇编了工业互联网领域十三个典型安全解决方案案例，可作为工业互联网生态链上下游供应商、工业企业用户等在规划、建设和运营工业互联网时的安全参照。

本汇编由中国移动通信集团有限公司牵头编制，重点参与单位有中国信息通信研究院、360 企业安全技术（北京）集团有限公司、北

京威努特技术有限公司、中国电子信息产业集团第六研究所、华为公司、深圳市腾讯计算机系统有限公司、江苏敏捷科技股份有限公司、长扬科技（北京）有限公司、常州万联网络数据信息安全股份有限公司。

本报告的参编人：张峰、田慧蓉、陶耀东、吴云峰、王绍杰、张旭武、侯聪、郭念文、崔君荣、马洁、倪海燕、马驰、王正、翟尤、李建文、黄超。其中，林欢、闫霞等协助审核了全文，并提出了诸多宝贵意见，在此一并致谢！

因为案例汇编内容较多，且时间仓促，难免存在诸多不足之处，希望业界同仁多提宝贵意见。

工业互联网产业联盟 安全组

二〇一八年十一月

一、 工业互联网安全概述

1. 工业互联网安全概况

工业互联网是涵盖六大重点领域：工业互联网网络、工业传感与控制、工业互联网软件、工业互联网平台、安全保障以及系统集成服务等。安全作为其中的重要环节之一，面临着严峻的挑战。一方面，工业领域信息基础设施成为黑客重点关注和攻击目标，防护压力空前增大。另一方面，相较传统网络安全，工业互联网安全呈现新的特点，进一步增加了安全防护难度。在此背景下，我国应积极加强对工业控制系统的安全体系化研究，从安全规划、安全防护、安全运营、安全测评、应急保障等各方面，提出针对性安全解决方案，积极进行技术试点，探究技术可行性，逐步形成可推广、可复制的最佳实践，切实提升我国工业互联网安全技术水平。

2. 工业互联网安全相关政策进展

近年来，我国从法律法规、战略规划、标准规范等多个层面对工业互联网安全做出了一系列工作部署，提出了一系列工作要求。

2016 年 12 月国家互联网信息办公室发布的《国家网络空间安全战略》提出要“采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏”。《中国制造 2025》提出要“加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系”。

2017 年 6 月起正式实施的《中华人民共和国网络安全法》要求对包括工控系统在内的“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”实行重点保护。

2017 年 12 月发布的《关于深化“互联网+先进制造业”发展工业互联网的指导意见》以“强化安全保障”为指导思想、“安全可靠”为基本原则，提出“建立工业互联网安全保障体系、提升安全保障能力”的发展目标，部署“强化安全保障”的主要任务， 为工业互联网安全保障工作制定了时间表和路线图。

2016 至 2017 年，工业和信息化部陆续发布《工业控制系统信息安全防护指

南》、《工控系统信息安全事件应急管理工作指南》和《工业控制系统信息安全防护能力评估工作管理办法》等政策文件，明确工控安全防护、应急以及能力评估等工作要求，构建了工控安全管理体系，进一步完善了工业信息安全顶层设计。

3. 工业互联网典型安全问题

我国工业互联网安全主要面临以下几方面的问题：

（1）工业控制系统漏洞频发，脆弱性高

工控设备的操作系统较为老旧，且升级更新周期长，众多工控系统存在漏洞，易被恶意病毒或代码感染，脆弱性高。根据国家信息安全漏洞共享平台(CNVD)统计，2017 年新增信息安全漏洞 4798 个，其中工控系统新增漏洞数 351 个，与 2016 年同期相比，新增数量几乎加倍，工业控制系统漏洞形势严峻且会持续呈现高发状态。

（2）生产设备大量暴露于互联网

传统工业生产设备以机械设备为主，随着工业互联网的发展，越来越多的机械设备进行数字化、信息化、网络化改造，但同时，安全防护建设速度落后于数字化信息化建设速度，导致越来越多的机械设备暴露于互联网中。暴露的设备一旦被攻击者扫描发现，可被远程操控或被利用成为“肉鸡”武器进行 DDoS 攻击等，危害巨大。

（3）企业内网安全性低，易作为跳板渗透工业系统控制层

2018 年 5 月份，Positive Technologies 公司发布的《2018 工业企业攻击向量报告》中指出 73%的工业企业办公网络边界防护不严，且普遍存在安全漏洞，容易被黑客利用作为跳板渗透工业系统控制层。企业内网成为黑客突破工业网络的最佳入口之一。

（4）数据安全问题

工业互联网的核心是工业数据采集，但目前数据接口、数据格式标准不一导致数据采集难度加大。且工业互联网的数据体量大、种类多、结构复杂，数据通信缺乏加密认证，数据的存储、传输、分析与共享存在安全风险。

二、 安全解决方案典型案例

案例一 基于威胁情报和白名单的轨道交通安全解决方案

1. 方案概述

2012 年 10 月开工建设的西成高铁，是第一条穿越秦岭进入四川的高速铁路，堪称名副其实的“高速蜀道”，于 2017 年 12 月 6 日全线开通运营。我国高速铁路信号系统基于 CTCS（中国列车运行控制系统）规范，包括计算机联锁系统（CBI）、列车自动防护系统(ATP)、列车控制中心(TCC)、无线闭塞中心(RBC)等系统组成。

随着这些数字化、网络化设备在高速铁路上的应用，基于通信传输的网络设备已经成为信号设备中非常重要的一部分。随着高铁信号系统各个子系统之间互联互通，工业控制系统内部网络开放性提高，网络管理系统（网管系统）成为高速铁路中不可或缺的网络检测设备。此系统虽然采用了一些安全防护措施，但仍面临日益严峻的信息安全风险。

2. 典型安全问题

高铁信号系统网管子系统可能面对的信息安全风险包括：

1） 操作人员违规使用移动存储设备

各地方铁路公司一般对在信号系统中使用移动存储设备有比较严格的信息安全管理措施。但在系统升级、数据备份等过程中仍存在违规操作风险，把病毒引入系统。

2） 系统组件的供应链污染

各铁路信号系统集成商一般都建立了比较严格的信息安全管控流程。但由于系统组件多，生产供应链长，在组件采购、生产、安装、调试过程中易受到病毒或恶意代码感染。

3. 安全解决方案

首先用工业信息安全检查评估工具箱和工业临检 U 盘对信号系统的网管子

系统进行 APT 攻击和病毒检测。确认无毒后，部署 360 工业安全管理系统、360 主机安全防护软件，进行安全防护。

360 工业信息安全检查评估工具箱结合威胁情报知识库和异常行为检测模型对实时数据和历史数据进行威胁分析与检测，可为高铁信号系统网管子系统进行安全检查、风险评估、等保测评、项目管理、合规性检查、工控资产发现、工控漏洞扫描、工控流量分析、威胁情报分析、安全事件、行为日志、报告自动生成等服务。该工具箱依据对原始流量数据的采集、存储、分析、挖掘和可视化展示，实现对攻击的快速检测和持续分析。此外，360 工业安全检查评估工具箱为便携式产品，带有高清显示屏幕，便于在多个单位进行现场快速分析，接入镜像流量即可，无需复杂配置。

利用工业临检 U 盘对信号系统的网管子系统客户端进行病毒检测，通过终端的威胁特征及潜在威胁风险、安全缺陷进行抓取、分析、评估。同时，引入 360 病毒检测能力和威胁情报，在不影响高铁信号系统网管子系统正常运行的前提下，帮助用户去检测、评估、自查本身终端安全威胁和风险。一旦检测到攻击可形成可量化评估报告，为高铁信号系统安全加固，提供防护能力。即插即用的临检 U 盘设备采用国密芯片，是国家密码管理局认证通过的安全芯片，摒弃了传统的数据加解密处理方式，使数据流加解密速度大幅提升，特别适用于高速数据流加密。

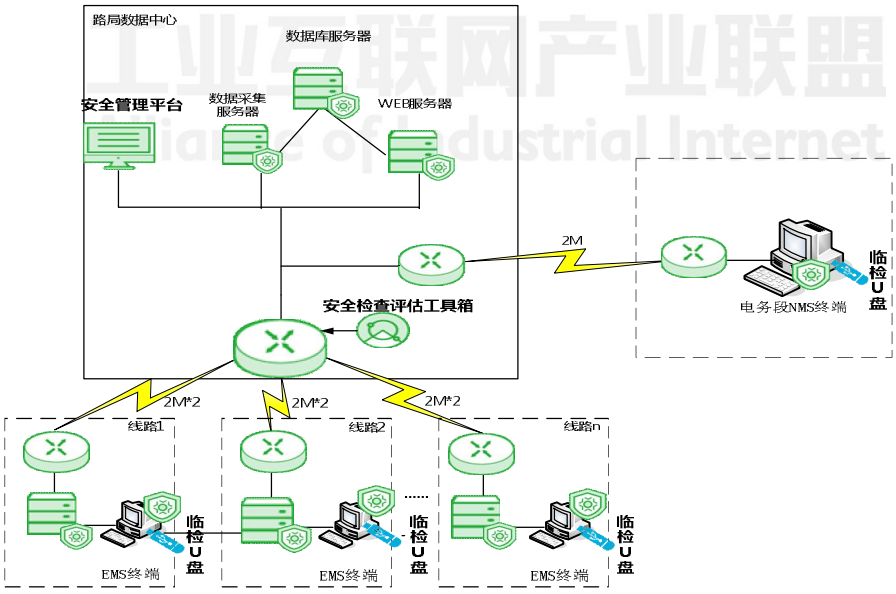

图 1 问题处理及安全防护示意图

为解决病毒、恶意程序攻击等问题，在高铁信号系统网管子系统主机、服务

器部署基于白名单机制的360主机安全防护软件。该软件基于轻量级“应用程序白名单”技术，能够智能学习并自动生成工业主机操作系统及专用工业软件正常行为模式的“白名单”防护基线，放行正常的操作系统进程及专用工业软件，主动阻断未知程序、木马病毒、恶意软件、攻击脚本等运行，为高铁网管系统工业主机创建干净安全的运行环境。

对更好对部署的工控安全设备和系统进行管理，对高铁信号系统网管子系统部署360工业安全管理系统，全面记录工业网络中的工业主机安全日志等情况，为高铁信号系统网管子系统提供管理体系。

经过以上操作，高速铁路信息安全防护得到极大提高，西成高铁顺利开通运营。

4. 创新点和应用价值

1）先进性及创新点

该案例解决方案基于威胁情报大数据和白名单技术对高铁信号系统网管子系统进行安全防护。工业信息安全检查评估工具箱能够快速发现威胁，对流量回溯取证，及时产生应急响应。工业临检U盘可对终端、服务器进行全方位的威胁扫描，对于威胁指标进行总体全面评估、量化结果。360工业主机防护软件高稳定、低开销、无需升级库文件等特点真正贴合了工业企业的实际需求，操作简单的特点也符合生产技术人员的操作习惯。

2）实施效果

创新性的将威胁情报、大数据的理念应用于高铁信号系统网管子系统的安全防护中，工业信息安全检查评估工具箱基于机器学习、威胁情报对网络攻击研判引擎；临检U盘利用360的大数据中心，采用国密芯片对终端进行威胁评估，基于白名单机制的主机安全防护软件有着实时报警、日志审计的优势，全链条的立体化工控安全技术防护方案对轨道交通制造企业提供较好的选择。

5. 案例提供方

360企业安全技术（北京）集团有限公司

案例二 工业互联网数据安全解决方案

1. 方案概述

随着我国“两化融合”进程的推进与《中国制造 2025》的提出，我国工业控制系统逐步向数字化、网络化、智能化转变，企业研发设计、生产制造、经营管理、销售服务等各个方面产生了海量数据。近年来，工业互联网的安全问题暴露的越来越明显，需加强对工业制造数据的智能安全管控。机器学习、自然语言处理、数据挖掘、大数据平台、云计算、移动互联网等技术的变革和发展，使数据安全管理呈智能化趋势，数据安全不仅仅是采用一刀切的数据强制加密方式来实现，更需要根据多样化的需求场景采取不同层次的安全控制手段，实现智能化安全管理。同时，工业控制网络和信息系统日趋复杂，要求我们必须将信息安全技术依据一定的安全体系设计进行整合、集成，达到综合防范的要求。加快信息安全产业发展是国家安全建设的需要，是保证国家信息化建设健康发展的需要，给处在快速成长阶段的我国数据安全厂商提供了无限的商机。

本方案通过分析工业互联网企业工业设计数据所面临的信息安全问题，提出了构建面向工业设计数据全生命周期安全管理的解决方案，采用基于内容识别的数据加密、应用软件指纹识别、安全云存储等技术，为企业间的高效协同提供一个安全平台。方案具体提出了企业应采取的安全策略和解决措施，阐明了全面构筑工业互联网数据安全云平台，确保工业设计环境中上下游企业在高效协同的同时，最大限度的防止商业秘密数据外泄、防止数据恶意篡改、减少图纸数据大范围分发的数据残留风险。

2. 典型安全问题

根据工信部对《深化“互联网+先进制造业”发展工业互联网的指导意见》的解读，工业互联网安全问题从实施角度可分为网络安全、数据安全、应用安全和云安全等几个部分。企业间的设计协同、制造协同逐步由原来的纸质信息传递，转变为以三维设计模型为核心的电子文件交换，带来了便利的同时，也带来了诸如：商业秘密泄露、图纸数据随意篡改、电子文件残留等数据安全风险，所以本

方案解决没有安全手段时候协同设计过程中人机交互过程的低效率、易出错（版本迭代时候人工的安全手段导致的版本更新不及时）、协同过程中多人互动图纸易泄漏问题。针对工业设计数据面临的三大威胁及痛点，敏捷科技工业互联网数据安全云平台构建了面向工业设计数据全生命周期安全管理的解决方案，包括：终端数据智能安全、网络数据防截获、云平台数据防泄露和丢失。

3. 安全解决方案

针对工业设计数据面临的三大威胁，敏捷科技工业互联网数据安全云平台构建了面向工业设计数据全生命周期安全管理的解决方案，包括工业图纸协同研发设计环节的安全可控，及图纸下单给外协方的电子商务结算环节、出图进行资源调配确定生产计划环节，直至下发至智能车间生产环节，及后续产品发布环节的图纸安全控制问题，主要包括：终端数据智能安全、网络数据防截获、云平台数据防泄露和丢失等功能。

图 2 安全协同设计图

图 3 安全协同制造图

图 4 核心数据强制加密保护模式

图 5 终端数据智能防泄漏保护模式

图 6 多种系统集成模式

本平台借助敏捷科技核心专利技术，基于我国密码标准算法构建。通过终端数据智能安全防护、网络数据安全防护、云平台数据安全防护等三方面的数据防护作用，确保工业设计环境中上下游企业在高效协同的同时，最大限度的防止商业秘密数据外泄、防止数据恶意篡改、减少图纸数据大范围分发的数据残留风险。

如下图所示：

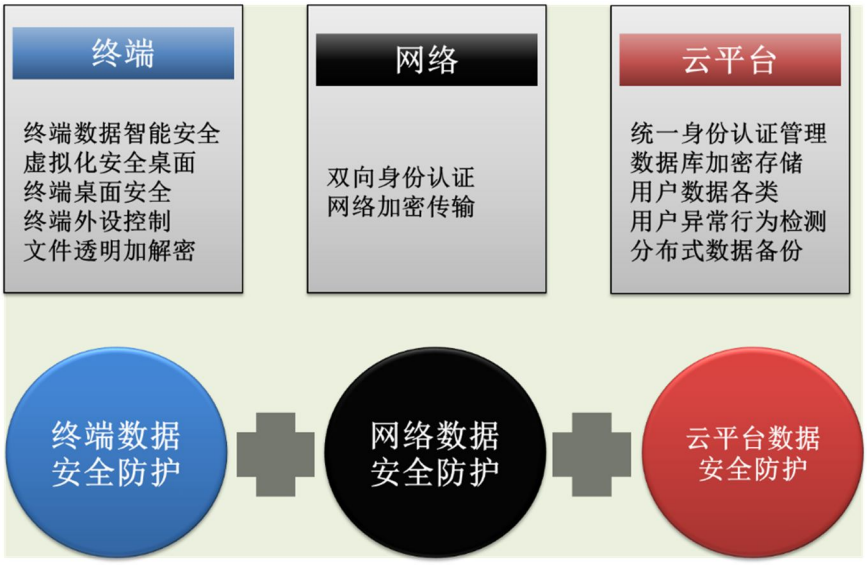

图 7 智能制造数据安全云平台功能框架示意图

1） 终端数据智能安全防护

终端数据安全防护由五个子系统组成，包括：数据智能安全子系统、终端虚拟化桌面子系统、终端桌面安全子系统、终端外设控制子系统、文件透明加密子系统。

数据智能安全子系统包括终端核心数据加密防护、网络出口拦截、敏感数据定期扫描、数据敏感度分析等功能。

终端虚拟化桌面子系统包括传输加密、介质加密、密钥产生和使用、容错备份还原、断线续用、服务器多机热备、域控身份认证等功能。

终端桌面安全子系统：通过远程监控、补丁推送、软硬件资产统计、终端程序控制策略、本地虚拟运行环境等技术使终端桌面工作环境安全。

终端外设控制子系统：不论是打印端口、串口、1394 还是 USB 接口，系统都可以进行开关及内容过滤控制，并且针对 USB 移动存储设备提供注册、审计、私有格式等功能，确保终端外设安全可控。

文件透明加密子系统：确保终端用户在操作电子文件的方式不发生改变的情况下，电子文件以密文方式存储。采用驱动层透明动态加解密技术，在操作系统和磁盘之间的数据加密和解密程序，自动对存储到磁盘的数据作加密运算，对从磁盘读取的数据做解密操作。通过指定文档类型、或者处理进程，能够达到所有存储介质上存在的该类型文件全部加密，有效防止机密信息泄漏。

2） 网络数据安全防护

敏捷科技工业互联网数据安全云平台在网络数据安全防护方面，提供了虚拟安全网络子系统。该子系统采用基于 P2P 技术构建的先进的虚拟安全域/网技术，根据权限和安全策略动态的将被访问的各种应用系统资源划分到一个独立的安全虚拟网络中，确保具体业务应用系统环境的专用性和“干净性”，实现了基于具体业务应用系统的动态“专网专用”，也从安全管理角度上对网络数据进行安全精细化管理。

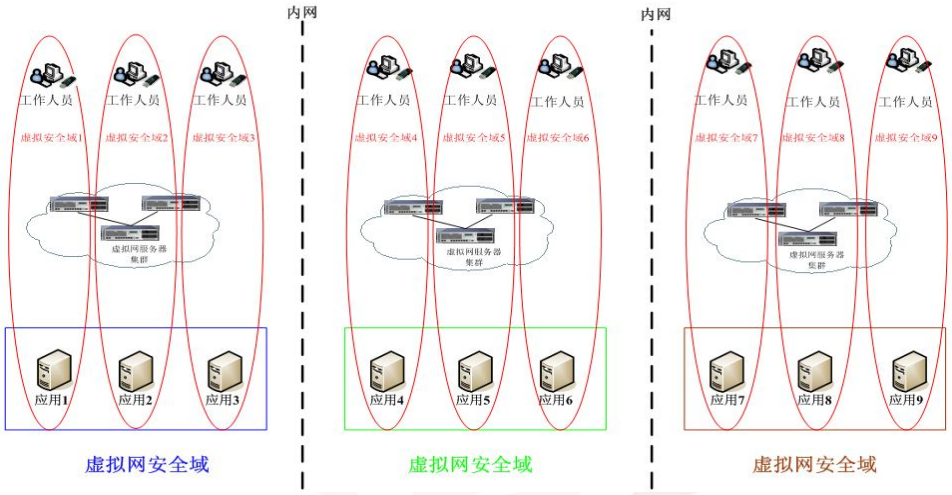

图 8 虚拟安全网络子系统

3） 云平台数据安全防护

云平台安全防护由五个子系统组成，包括：统一身份认证管理子系统、数据库加密存储子系统、多租户数据隔离子系统、用户异常行为检测子系统、分布式数据备份子系统。

统一身份认证管理子系统：从用户的应用安全需求出发，提出了“深度整合，全面安全”之理念，在应用系统的身份认证、资源访问控制、用户操作审计、数据加密解密、时间戳服务、网络数字签章、数据签名与统一验证、关键交易验证等方面分层次深入整合，满足应用系统内部和外部安全需求。

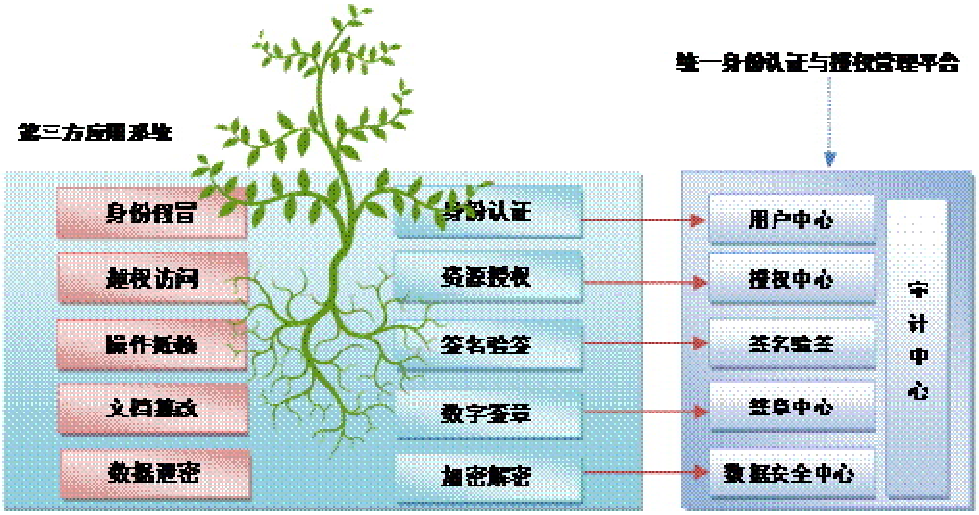

图 9 统一身份认证与授权管理平台设计

数据库加密子系统：对数据库中的数据进行加密处理，即使某一用户非法入侵到系统中或者盗得数据存储介质，没有相应的解密密钥，他仍然不能得到所需数据。

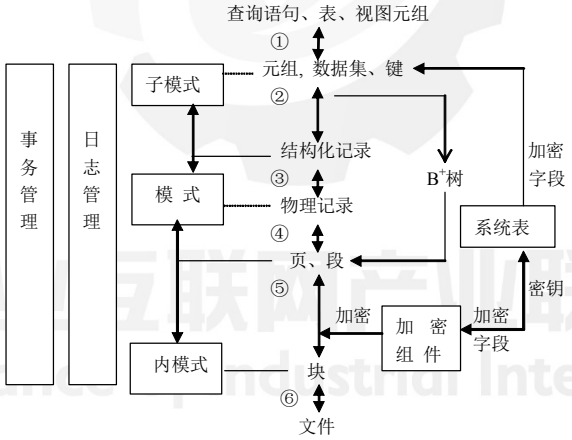

图 10 加密数据存储体系结构

可搜索加密子系统：根据云平台的需求，对敏感关键字密文进行搜索。

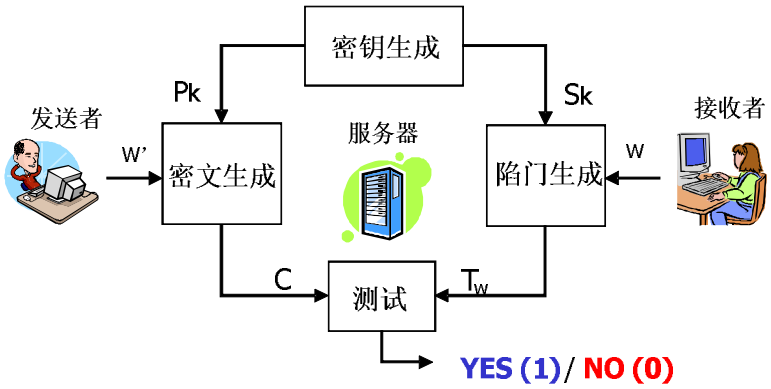

图 11 带关键字检索的公钥加密方案

①密钥生成算法 $KenGen(s)$：输入一个安全参数 s，生成一个密钥对，包含公钥 p_k 和私钥 s_k。

②密文生成算法 $PEKS(p_k,w)$：输入接收者的公钥 p_k 和一个关键字 w，生成可以检索关键字 w 的密文 $c=PEKS(p_k,w)$。

③陷门生成算法 $Trapdoor(s_k,w)$：输入接收者的私钥 s_k 和一个关键字 w，生成关键字 w 的陷门 T_w。

④测试算法 $Test(p_k,c,T_w)$：输入接收者公钥 p_k，一个 PEKS 密文 $c=PEKS(p_k,w')$ 以及要检索的关键字的陷门 $T_w=Trapdoor(s_k,w)$，如果 $w=w'$，那么该算法输出 Yes(1)，否则输入 NO(0)。

用户异常行为检测子系统：总体功能分为三大部分：审计数据采集、分析引擎、审计管理平台。审计数据采集是整个系统的基础，为系统审计提供数据源和状态监测数据；分析引擎对采集的原始数据按照不同的维度进行数据的分类，同时按照安全策略和行为规则对数据进行分析；管理平台是安全审计的 Web 管理平台，包含了安全审计平台的管理功能和信息发布管理功能。

图 12 用户异常行为检测子系统功能

数据安全隔离子系统：采用用户行为采集技术，用户行为分析技术和数据迁移技术，可以实现用户行为的有效监控，当发现云平台中存在正在进行攻击的用户时，动态调整受到威胁数据的安全级别，和云平台的访问授权策略，时刻确保云平台中收据的有效隔离，以免受恶意用户攻击的威胁。

4. 创新点和应用价值

1）先进性及创新点

- 基于内容识别的终端数据智能安全管理

采用的智能安全分析技术、操作系统内核技术、高强度的加密算法、灵活易用的安全策略，对敏感数据提供含数据发现、数据识别、数据分类、数据加密、数据分级、权限管控以及预警审计等全方位管控能力，有效的解决了企业内部合法用户有意或者无意的信息泄漏。

- 满足高性能要求的安全云桌面数据集中管控

安全云桌面数据集中管控平台技术的优势表现在它大大提升了现有 PC 的使用效率，实现了 IT 部门对分散的 PC 的集中式管理，以及客户数据、应用与底层硬件基础设施剥离所带来的高度安全性和灵活性。站在管理优化的角度，它赋

予了 IT 管理者战略性的基础架构中央管理能力和安全控制能力。而在用户层面，使用习惯的无需改变、PC 应用的无缝兼容、个性化桌面应用的灵活调用更是帮助用户将这一新架构顺利实施的推动因素之一。

- “云+网+端”一体化云数据安全解决方案

要解决云平台环境下的数据安全问题，仅仅在终端、网络、云平台中的任何一方面实施保护是不够的，必须要通过融合云平台数据安全管理技术、终端数据安全管理技术、网络安全传输技术为一体，实现对云数据的全程一体化安全管理。在云平台数据中心，重点完成用户身份认证、多租户模式下的数据隔离、租户行为异常审计、结构化数据和非结构化数据的透明加密。在终端，重点完成用户密钥生成、终端环境安全、终端外设安全、终端文件透明加密保护。在网络传输过程，重点负责完成终端与云平台之间建立虚拟安全通道。

- 针对结构化、非结构化数据的加密处理

数据在云计算环境下有结构化、非结构化两种存储形态，对关键重要数据的加密处理是确保数据安全的重要手段。敏捷科技数据安全云平台提供了针对云计算环境下非结构化数据与结构化数据的透明加密方案。

- 基于分区分域分级设计的云安全运维与安全管理

工业云平台环境相对复杂，涉及多类业务，多类系统，因此在安全防护上需要进一步细化安全域的划分以及不同安全域、不同安全级别的访问控制设计。实现安全运维操作的分级管理，对不同级别的用户予符合其安全职责划分的操作或审计权限，实现安全运维。坚持日常安全运营与应急响应相结合，以数据为驱动力，以安全分析为工作重点。

2）实施效果

本平台通过终端数据智能安全防护、网络数据安全防护、云平台数据安全防护等三方面的数据防护作用，确保工业数据集中管控的同时实现安全可靠管理，有效保护工业企业的核心资产、知识产权及其它相关数据。

产品融合集成 2000+信息系统，在制造、能源、设计、交通、政府、军工、文教卫、汽车电子、轻工纺织、冶金水电、生物医药等 500+关键领域得到广泛应用，累计客户量过万，每天有 1000 万+人使用该产品保护数据，目前已有客户包括中国中车、中国一汽、长安汽车、中石油、中粮集团、国防大学、江苏省档案

馆等，涵盖了机械、汽车、电子、国防、能源、交通、建筑、化工、商贸、现代服务业、政府、研究院所等。

项目所采用的内核级主动加密、应用软件指纹识别的加密槽等技术通过科技成果鉴定属国内外首创，填补了工业互联网安全领域的技术空白，弥补高端和前沿研究开发方面的不足；有利于强化产业技术原始创新能力，抢占工业互联网技术发展制高点；有利于促进产业的融合，带动工业互联网领域信息安全相关产业的共同发展，培养工业互联网领域高水平和专业化的创新人才；有利于保护核心工业数据，维护国家制造业主权；有利于形成工业大数据系列技术和应用标准，推进产业生态建设，为促进全国工业互联网行业持续健康发展提供有力支撑。

4. 案例提供方

江苏敏捷科技股份有限公司

案例三 汽车制造行业勒索病毒应急处理和安全解决方案

1. 方案概述

由于工业控制系统(以下简称工控系统)上位机操作系统老旧且长期未升级，存在很多的安全漏洞，病毒问题一直是威胁工控系统主机安全的一个棘手问题，从震网病毒到 2017 年末的工业破坏者，这些如幽灵般游荡在工控系统网络中的杀手总是伺机而动，一旦得手就会带来巨大的危害。

国内某知名新能源汽车制造企业遭受病毒侵袭，生产制造产线几台上位机莫名出现频繁蓝屏死机现象，并迅速蔓延至整个生产园区内大部分上位机，产线被迫停止生产。该企业日产值超百万，停产直接损失严重，虽然信息安全部门采取了若干紧急处理措施，但收效甚微。为了尽快解决问题恢复生产，该企业紧急向 360 安全监测与响应中心进行了求助。

2. 典型安全问题

工业现场的上位机大多老旧，服役 10 年以上仍在运行的主机也很常见，而工业现场的相对封闭性，使得补丁升级、病毒处理变成一件很复杂的事情。工业生产的稳定性往往会面临上位机脆弱性的挑战，一旦感染病毒就会造成巨大影响。

该企业生产网络与办公网络连通，未部署采取安全防护措施；生产制造产线上位机运行异常，重复重启或蓝屏，初步断定为病毒入侵。

由于上位机操作系统都是老旧的 Windows XP,感染病毒之后频繁蓝屏重启，无法在问题终端采样进行病毒分析。在生产网络核心交换机位置旁路部署 360 工业安全检查评估系统对生产网络数据流量进行检测，该设备基于 360 行业领先的安全大数据能力生成多维度海量恶意威胁情报数据库，对工业控制网络进行自动化数据采集与关联分析，识别网络中存在的各种安全威胁。借助工业安全检查评估系统的强大检测分析能力，安服人员很快判定该企业上位机感染了“永恒之蓝”蠕虫病毒（也称为 WannaCry）。

3. 安全解决方案

1） 应急处置

安服人员发现上位机感染 WannaCry 病毒之后，为了避免上位机中数据被加密带来进一步的危害，紧急在生产网络中部署一台伪装病毒服务器，域名设定为病毒网站，并通过策略设置将生产网上位机 DNS 指向此伪装服务器，阻止了 WannaCry 病毒的后续影响。

该企业生产园区占地范围很大，感染病毒的上位机几乎遍布整个园区，单纯依靠人力难以逐一定位问题终端。360 工业安全检查评估工具箱在此过程中发挥了巨大作用，不仅给出了感染病毒的准确研判，而且详细统计出所有问题终端的 IP 地址和 MAC 地址，结合企业提供的资产清单，安服人员和厂方技术人员很快确定了绝大部分问题终端的具体位置。

2） 感染处理

完成定位之后，360 安服人员即刻赶往最近的问题终端，第一时间关闭了 445 端口，避免病毒进一步扩散。经过与厂方生产技术工程师细致沟通，得知以下信息：

- 上位机硬件配置资源有限，无法安装杀毒软件；
- 专用的生产软件对操作系统版本有严格限制，无法对操作系统进行打补丁操作；
- 重装系统会导致专用软件授权失效，带来经济损失。

结合上述信息，安服人员只能对问题终端采取杀毒处理。为了避免杀毒过程中对上位机系统和数据造成影响，安服人员首先备份了问题终端系统及数据，然后用 360 推出的 WannaCry 病毒专杀工具进行杀毒处理，清除感染的病毒。

3） 安全加固

为了避免处理完成的上位机再次感染病毒，安服人员在上位机上部署安装了 360 工业主机防护软件，该软件基于轻量级“应用程序白名单”技术，能够智能学习并自动生成工业主机操作系统及专用工业软件正常行为模式的“白名单”防护基线，放行正常的操作系统进程及专用工业软件，主动阻断未知程序、木马病毒、恶意软件、攻击脚本等运行，为工业主机创建干净安全的运行环境。

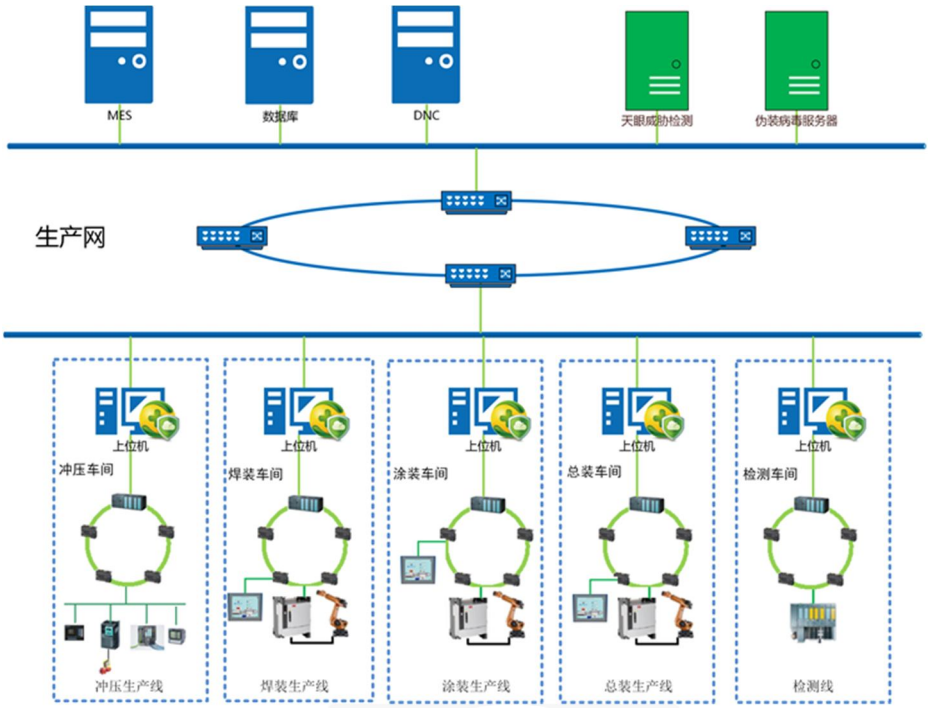

图 13 问题处理及安全防护示意图

同时，为了避免 U 盘混用带来的病毒串扰风险，安服人员利用 360 工业主机防护软件对 U 盘使用进行合法性注册和读写控制策略配置，仅允许生产技术工程师专用的 U 盘识别和使用。

此外，为了限制 Windows 网络共享协议相关端口开放带来的风险，安服人员通过 ACL 策略配置关闭了 TCP 端口 135、139、445 和 UDP 端口 137、138，并利用 360 安全卫士的“NSA 武器库免疫工具”关闭存在高危风险的服务，从而对 NSA 黑客武器攻击的系统漏洞彻底“免疫”。

经过以上病毒清除和安全加固手段，不仅解决了感染 WannaCry 病毒带来的蓝屏重启问题，而且极大的提升了上位机的主动防御能力，实现了上位机从启动、加载到持续运行过程全生命周期的安全保障。

经过此次事件，该企业对工业控制系统安全性更加重视，决定采取 360 整体工控安全防护措施，逐步建设形成覆盖汽车制造产线全链条的立体化工控安全技术防护方案。

4. 创新点和应用价值

1）先进性及创新点

360 工业安全检查评估工具箱和工业主机防护软件是解决工业主机脆弱性问题的一剂良药。360 工业安全检查评估工具箱基于 360 领先的威胁情报大数据能力快速识别威胁和资产。工业主机防护软件基于轻量级“应用程序白名单”技术，高稳定、低开销、无需升级库文件等特点真正贴合了工业企业的实际需求，操作简单的特点也符合生产技术人员的操作习惯。该方案能够适用于大部分工业控制系统，是一套成熟可靠的安全解决方案。

2）实施效果

针对汽车制造行业容易被病毒攻击的安全问题，首先部署伪装病毒服务器阻止病毒的后续影响，利用 360 工业安全检查评估工具箱快速识别定位病毒威胁，工业主机防护能够自动生成工业主机操作系统及专用工业软件正常行为模式的“白名单”防护基线，为工业主机创建安全的运行环境。

5. 案例提供方

360 企业安全技术（北京）集团有限公司

案例四　某电厂信息安全监管与预警平台建设案例

1. 方案概述

近年来，电力行业中的自动化与控制系统的网络安全问题受到关注与重视。网络安全防护措施不再是“锦上添花”，而是至关重要。在过去 10 年内，包括水电站在内的各种电站均配有自动化保护与控制系统。基于开放式标准(如:IEC61850 或者 IEC60870-5-104)并采用可靠以太网技术进行开发，使不同厂家间的产品和系统间实现了操作互通。

系统越来越复杂，互联也越来越多，为电站的运行人员提供了更多信息，进一步提高了实时监控水平。该变化不是发生在单个电站，而是涉及到整个公用设施系统。随伴着电力能源市场中电厂控制系统、调度和交易系统之间网络通信应用的稳步发展，公用设施系统发展与时俱进。

从经营角度看，先进技术带来了巨大效益，但与传统工业控制系统面临的问题类似，电站业主和运行人员也面临网络安全威胁。过去几年来，电力工业领域网络攻击事件显著上升，控制系统中发现的漏洞也越来越多。水电厂作为重要基础设施，重要性高且具有一定的战略意义，一旦遭受攻击影响巨大，较易成为敌对势力攻击的目标。因此如何更有效的结合水电厂既有防护措施和业务系统，提高安全防护等级，保障业务持续稳定，是一个需要考虑的关键问题。

某电站是某省实施西部大开发战略的标志性工程和国家西电东送的骨干电源和重点工程。工程以发电为主，兼有防洪、灌溉、拦沙及航运等综合利用效益。某电站是中国目前水电站单机容量最大的电站之一。

2. 典型安全问题

现某电厂生产控制系统中，生产控制大区与管理信息区已实现单向隔离，与某集控中心、某省中调和南网总调远动通道已实现纵向加密，控制Ⅰ区与Ⅱ区通过南网调度数据网已实现逻辑隔离。但与此同时，当前的安全措施也存在一定的不足，网络边界防护、监控大区病毒防护、安全审计、操作系统加固等还不完善，具体需求如下：

需要满足《电力监控系统安全防护总体方案》（36 号文）有关电厂安全防护的相关要求，需要满足电网的电力调度安全防护和国家能源局电力监控系统安全防护的重点要求；

1） 目前水电厂内各系统（各机组测温系统、开关站系统、共用系统、厂用电系统和坝区系统等）之间未进行有效的网络隔离，可随意互访，单区域或单节点遭受病毒感染或恶意攻击将直接影响其它区域的正常运转，尤其是底层控制系统，需按照相关要求采取安全隔离措施，防范病毒扩散及恶意攻击行为对其它系统造成影响等；

2） 随着水电厂智能化、信息化等新技术的应用，“无人值班，少人值守”的远程监控管理模式快速发展，机组和远方集控中心通过网络进行数据及控制指令传输，使生产控制大区遭受攻击的风险增加，需采取相应手段对关键指令下发及误操作等行为进行实时监测和告警；

3） 发电厂生产控制系统中的管理终端（如服务器、工程师站、操作员站等）存在移动介质、串口设备、并口设备等外设滥用和主机安全策略配置级别较低的情况，需采取有效措施对移动 U 盘等外设的使用进行管理，并增强主机安全防护能力；

4） 电厂在执行特定工作(如系统调试和维护)时，需要通过本地或远程方式接入第三方设备，就需要对接入的人员及终端设备采取有效的安全监管措施，需要重点管控维护过程中的关键操作行为并对所有操作行为进行取证。

3. 安全解决方案

经过对现场网络结构、主机设备、系统软件、安全设备等运行情况进行安全调研和分析，识别出系统资产和脆弱性，确认了水电站现场所存在的安全隐患和安全防护缺失项，明确了采用自主可控的工控安全核心技术的技术路线。为加强某水电站网络安全防护，构建的安全防护方案如下：

1） 在各机组 LCU 与控制网络之间部署工业防火墙，通过对 Modbus 协议进行深度解析与“白名单”控制功能，能有效保护电厂使用的施耐德 Quantum 系列 PLC，防止针对 PLC 漏洞的恶意攻击行为及违规操作；

2） 在水电厂环网交换机上旁路部署工控安全监测与审计系统，对控制网络

中的网络流量进行实时监测，特别是异常指令下发、违规操作等行为，同时记录原始 pcap 文件，以便调查取证。

3） 旁路部署入侵检测设备，通过收集和分析网络行为、安全日志、审计数据、其它网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

4） 在主控层的工程师站、操作员站和服务器上部署主机加固系统，对系统中安全相关的设置进行全面扫描及策略设置，对关键业务进程、程序予以保护，建立白名单库，将普通操作系统透明提升为安全操作系统，大大提高工业主机的安全性；

5） 在控制环网交换机上部署安全运维管理系统，实现账号统一管理、资源和权限统一分配、操作全程审计，提升运维过程的安全性。

6） 通过统一安全管理平台对所部署的安全设备进行统一的安全管理，包括策略下发、日志审计、报警展示等，简化运维管理工作流程、提高运维管理工作效率。

图 14 某水电站安全防护方案

4. 创新点和应用价值

1）先进性及创新点

通过建立可信任网络“白环境”和“白名单”防护理念，以自主可控的核心技术投入，以完全符合工业现场的产品设计，为某电厂构筑 “安全白环境”整体防护体系，保护某电厂生产控制系统信息安全监管与预警平台系统设施的稳定

运行，达到“只有可信任的设备，才能接入控制网络”、“只有可信任的消息，才能在网络上传输”、“只有可信任的软件，才允许被执行”的防护效果。该方案打破了传统“黑”的防护模式，打破工控安全信息孤岛，以更符合工业现场特性的防护手段，以“一个中心，三重防护”的防御体系，将传统的“被动防护”转化为“主动防御”。

2）实施效果

- 解决方案具有完全自主的知识产权，满足《电力监控系统安全防护总体方案》（36 号文）要求；
- 有效检测工业网络中通信异常和协议异常并进行阻断，实现控制系统的安全网络隔离、访问控制以及专用工控协议的深度解析，避免关键控制设备被攻击，防止造成重大生产事故、人员伤亡和不良社会影响；
- 提升了现有操作系统的安全等级，有效的防止来自内部的误操作和恶意操作；
- 对服务器日常访问、操作进行监控和审计，实现对用户运维过程的标准化管理；
- 实时监测针对工业协议的网络攻击、用户误操作、用户违规操作、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；
- 将工控网络中的安全设备和系统统一管理，减少管理人员的工作量，降低企业人力资源的投入，通过技术手段弥补人工管理方式上的不足，提高企业工控网络安全管理效率；
- 实现水电站总体安全现状分析，帮助客户实时了解自身安全状况，并提供简便易用的回溯功能，为工业控制系统安全事故调查提供技术手段；
- 全面提高生产控制网络的整体安全性，为华能澜沧江某水电厂安全生产保驾护航。

5. 案例提供方

北京威努特技术有限公司

案例五 石化油气工业互联网安全解决方案

1. 方案概述

当前，世界各国深刻认识到信息技术的重要性，纷纷确立了以推进信息技术发展为特征的发展战略，并加大对信息技术投入，促进和保障信息技术成果的应用转化，尤其在工业领域应用信息技术方面都进行了持续关注。近十年来，国际金融危机频发，造成工业增长明显放缓，下行压力加大，大批中小企业陷入困境，大企业受到重创。但在金融危机的影响下，各国都提出“IT 救市”计划，希望通过信息技术，促使工业企业管理更加精细化、成本更加集约化，实现调整产业结构、加快新兴产业发展。石化油气工业是我国重要的战略性产业，对国民经济和国家安全有着重要作用。如何提升石化油气工业的运营效率和确保安全生产成为当前行业关注的重点。

腾讯工业互联网安全平台的价值主张是助力客户“共生共赢”：

1） 定位与平台运营者互补：扮演助力者，不涉足自营

2） 发挥平台优势：基于腾讯云成熟的应用开发框架、大数据 AI 平台、全方位安全防护、运维计费系统，打造强大工业互联网“中台”。

3） 打造开放生态：建立智能物联接入和工业应用生态，提供完整方案。

4） 深度技术助力：以腾讯大数据、人工智能技术为依托，帮助工业企业实现技术转型，提升生产效率。

5） 根据油气工业需求和挑战，腾讯以问题为导向，重点从工业互联网大数据安全云平台、移动生态安全系统（HSE&EAM）、移动 OA 系统来提供油气工业互联网安全解决方案。

2. 典型安全问题

当前石化油气工业主要面临以下安全问题和挑战：

图 15 石化油气工业安全挑战

1）如何确保设备安全，减少产量损失，提高设备生产时率和作业效率

2）如何提高 HSE 安全管理水平，实现地上地下一体化实时安全监控

3）如何实现生产自动化大规模覆盖，形成规模效益，同时应用智能化，实现自动预警，准确预测，减少安全损失。

3. 安全解决方案

1） 石化油气工业互联网安全云平台

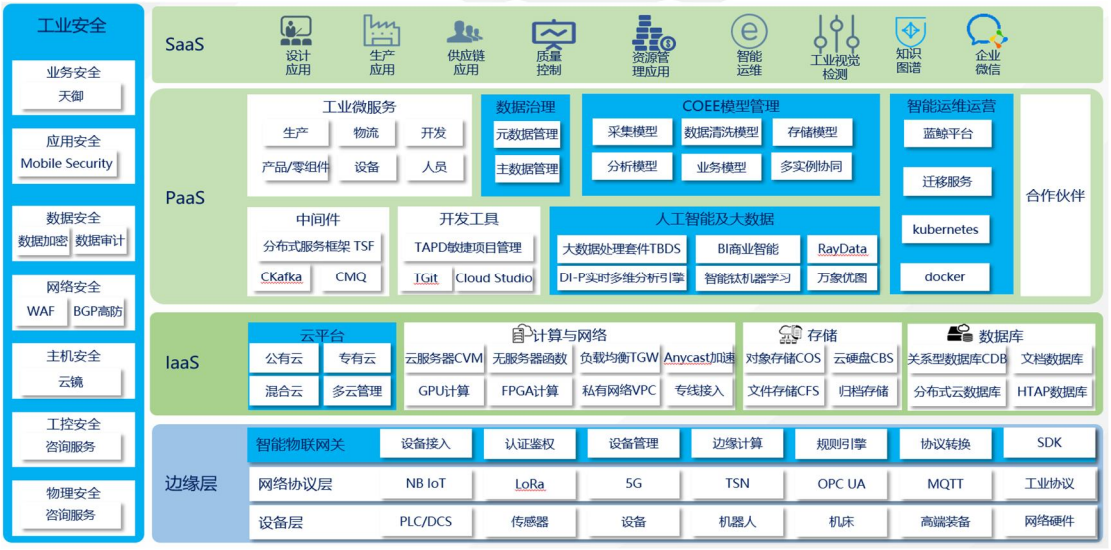

图 16 石化油气工业互联网安全云平台

基于腾讯云的网络安全能力，将石油化工设备全程接入，包括不同类型设备和海量传感器。组成“消息队列+数据库+大数据安全平台+数据安全”“公有云 IaaS+BGP 网络+专有云+网络安全”的系统安全措施，实施完成故障检测、预测性安全运维、远程安全维护等工作。炼油企业通过预防和预测设备故障的能力，从

而极大地提高了设备安全性、生产力和法规遵从性。

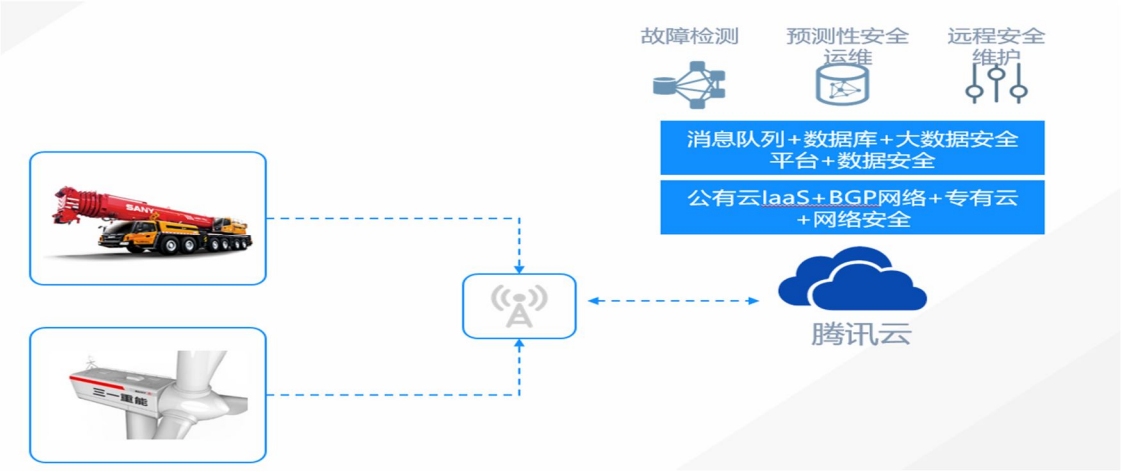

图 17 安全能力

在石油化工行业运输、产品制造等关键环节进行数字化、全流程安全保护，确保数据流动和设备的安全运转。确保在全生命周期中设备管理的安全性和一致性，通过数据的移动化和可视化服务，提升设备的使用效率。从而大幅减少运行地震算法所需要的时间，可以有效处理和分析与钻场、油藏相关的实时数据。

图 18 工业互联网安全平台数字化示意图

依托腾讯工业超级大脑，结合大数据安全平台和机器学习平台，有效提升石油化工行业产品及设备检测准确率，帮助企业减少人工检测差错，进一步提升产品工序效率和安全性，确保产品安全和质量，全流程实现数据化和可操作性。炼油企业可以通过采用腾讯云的解决方案来预测人员事故并提高炼油设备的安全性。

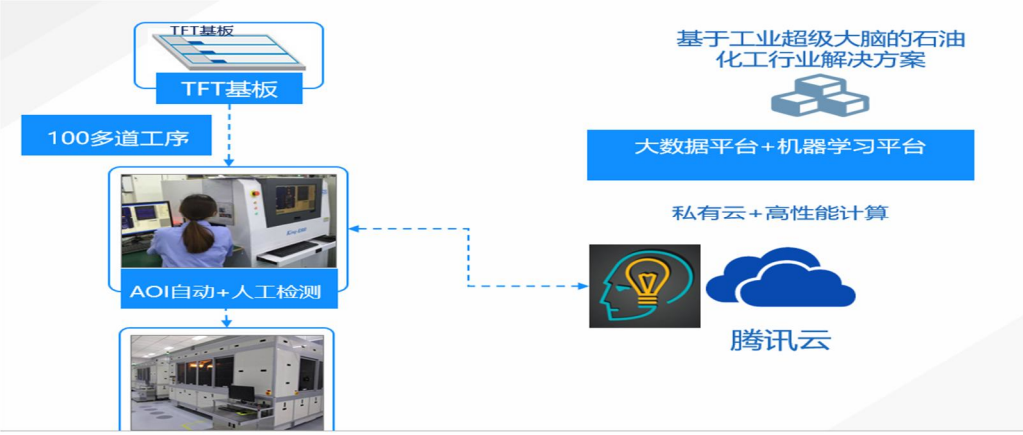

图 19 大数据和机器学习平台

总的来看，通过石化油气工业互联网安全云平台，可以有效提升运营安全标准，带动石油炼制与生存效率，对石化油气业务的勘探决策、降低勘探安全风险、精准数据收集和安全决策、确保设备安全运营方面有巨大价值。

2） 移动 HSE

HSE 管理体系：健康 Health、安全 Safety 和环境 Environment 三位一体的管理体系，其中责任制是 HSE 管理体系的核心。

当前石油化工行业存在以下问题：

图 20 需改进的问题

通过事故分析，我们发现 95%发生在一线现场，现场安全管理是重中之重，但是现有的信息系统不能帮助安全制度在一线有效落地。为适应性的业务发展和管理需要，石化 HSE 系统需要从动态、集成、智能三个方面入手进行提升，与生产管理过程紧密结合，支持生产安全管理，实现生产作业受控。

从静态到动态系统。实现对业务过程的管理，实现对生产作业过程的管理，实时数据，而非事后数据。从孤立系统到集成系统。与管理系统的集成，如 ERP。与生产管理系统的集成，如生产运行管理系统。与底层监控系统的集成，如污染源监测系统。专业 HSE 系统集成，如 HAZOP。从体系建设到智能决策分析。建立早期预警机制，支持管理决策，知识管理。

图 21 移动 HSE

移动 HSE 现场总管：全功能、全数据、人性化的移动平台。

在全功能方面，HSE 领先的劳动生产力平台+业务插件解决方案，覆盖安全生产和人员效能的全局管理功能。在全数据方面，HES 打通模块间直接信息传递，实现信息的统一收集和追溯，使业务联动、交叉关联分析成为可能。在人性化方面。HES 实现以人为本的设计理念，使产品更加人性化，便于用户的使用，提高工作效率。在分阶段方面，实现一个平台、多个插件满足现有和未来扩展需求。

图 22 移动 HSE

HSE 可以真正为一线员工打造的现场安全管理应用，大幅减少重复录入和纸面作业，真正汇总现场和一线信息，同时确保相关信息的安全性。

图 23 HSE 应用

4. 创新点和应用价值

1) 先进性及创新点

预见性安全维护有助于减少意外停机、改善开采动态。该解决方案帮助维护了一个监测设备性能数据的集中控制中心，以创建智能的、按优先级排列的维护作业顺序。同时，可以将检测潜在不良部件性能、提供潜在设备故障警示的设备功能中重复出现的偏差标记出来。

环境和员工安全解决方案可帮助企业有效监测和控制生产现场。该解决方案帮助分析大量动态数据，以移动的方式，实时监测环境条件该解决方案通过分析和评估各种数据（如设备数据、检查数据、历史、日志文本等）来预防运营问题的出现。

2) 实施效果

预见性安全维护，可以有效提高预见性维护与修复性维护的比率。通过减少意外停机时间，将资产可用率提高 3-5%。库存需求减少 10-20%。

环境和员工安全解决方案，可以有效提高获得监管批准的可能性，提高达到零有害排放目标的能力，及时对不利环境问题作出反应。

5. 案例提供方

深圳市腾讯计算机系统有限公司

案例六 某电子制造企业的安全解决方案

1. 方案概述

某电子制造企业的制造基地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。目前该企业通过自建私有云方式实现“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私有云平台实现生产协同。

由于企业的制造智能化和管理 IT 化的水平比较高，其制造业务的面临安全挑战非常大。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。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，基于先改造 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，提高防攻击的反应能力和预警能力。生产基地在此基础上，还结合主机安全加固、反病毒机制和定期的安全测试检查等措施，有效地应对了多次安全攻击事件，例如在勒索病毒和 ARP 攻击等针对基地的攻击事件中，能够做到及时预警和快速反应。

2. 典型安全问题

该企业在设计生产园区的安全防护体系时，充分考虑到以下安全问题：

1） 不同业务平面需要进行网络辑隔离，防止网络安全事件发生时，存在风险快速横向扩展导致大面积业务瘫痪风险。

2） 由于历史原因，车间的工控系统自身防护能力非常弱，包括工控协议本身没有考虑安全设计，计算机 OS 老旧，软件升级和补丁更新缓慢，且很多设备

并不适合安装杀毒软件。

3） 生产管理应用系统需要向外协工厂和厂内办公网络开放，存在黑客从外网直接攻击生产管理系统的风险，也存在办公区设备被病毒感染，而蔓延到生产管理系统的风险。

4） 生产网络的边界管理需要强健，避免像有些企业那样，只采用简单的 ACL 隔离，车间生产设备采用分配固定 IP 地址，且用户可以无限制次数地直接访问这些生产设备等等。

5） 面对高级持续威胁和 WannaCry 等这种新型病毒，传统单点和静态防护常常束手无策，等到攻击事件爆发时才制定相应安全措施。

3. 安全解决方案

针对上述安全问题，如图 24 所示，制造基地采取了如下的安全部署策略：

1） 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。

2） 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，采用设备和用户双因子鉴权机制，设备需要先通过云的合规性和杀毒检测，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。

3） 部署智能的主动防御系统

通过安全态势系统、安全策略智能管理和网络诱捕系统，“三位一体”构建主动防御体系，提高了对未知的威胁感知能力和安全响应能力。

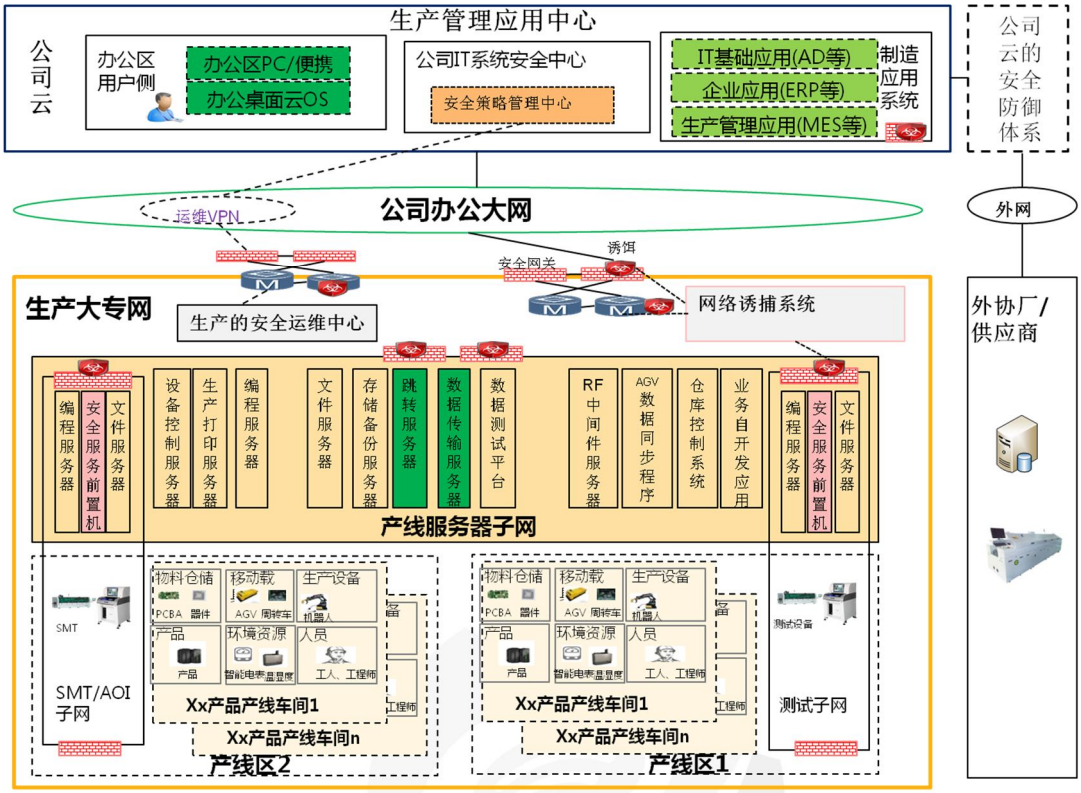

图 24 制造基地安全部署示意图

4） 安全域的划分

安全区域划分是安全隔离的基础，承载网络隔离、防火墙等安全网关部署、ACL 等安全策略都围绕安全区域划分策略展开 。同一安全区域内的子网或设备具有相同或者相近的安全保护需求，较高的互信关系，并具有相同或者相近边界安全访问控制策略，安全区域设备之间为信任关系。网络安全区域与安全区域之间主要采用 VPN+VLAN、安全网关进行相互隔离。如图 25 所述，制造基地园区划分为下面几个安全子区域：

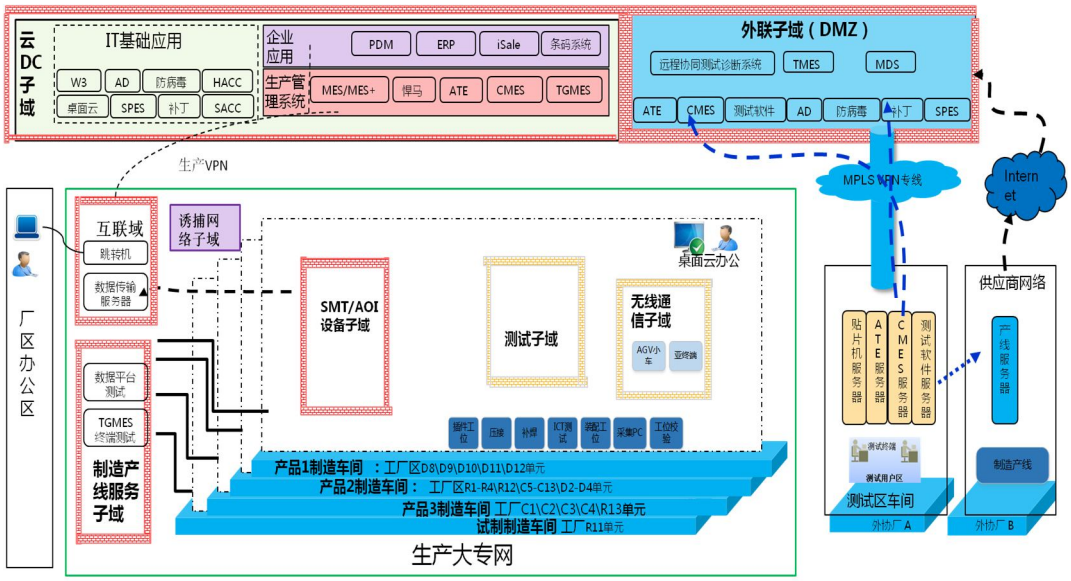

图 25 制造基地的安全域划分

- SMT/AOI 设备子域：是生产线核心的设备，包括贴片机 SMT、自动光学检测设备 AOI、回流焊服务器等；
- 产线服务器子域：是产线设备的管理和控制服务器区域，包括设备编程服务器、设备控制器、安全服务前置器、产线文件服务器、生产打印服务器、产线数据存储备份器等；
- 产品测试子域：包括产品自动化测试设备、测试仪器和软件测试服务器等
- 无线通信子域：采用 eLTE 和工业 WiFi 通信的设备，如厂区的一些数据采集器、自动搬运车、移动测试台和自移动工业机器人等，无线通信采用双向鉴权和空口加密方式。
- 云 DC 子域：制造基地部署在公司云平台中的各种服务器，包括生产管理系统、企业应用服务器和通用的 IT 服务器等
- Extranet 子域：实际上就是公司云平台专门画出的一个 DMZ，部署了需要和外协厂及供应商网络进行互联互联的服务器，以及进入生产网络前的安全检查软件服务器等。

5） 边界访问控制

除了禁止普通办公终端直接进入生产网络之外，生产网络各安全子域采用多层边界访问控制机制：

- 层 2 的隔离措施：汇聚交换机或者路由器中配置不同的 VLAN，将各个安全域的数据流映射到对应的 VPN 中，实现不同安全区的数据流相互隔离

- 层 3 访问控制措施：各生产安全子域网关和设备主机采用白名单双层 ACL 机制，各生产子域，不能直接和办公网络进行通信，需要经过生产大专网的跳板服务和数据镜像服务器进展中转；各生产子域的 ACL 名单由公司安全策略中心进行统一的电子流管理。另外网关和子域内设备，只开放有用的 IP 端口，并关闭 FTP, Telnet 等高危险协议端口；外部 Intranet 区，只对外协厂和供应商特定的 IP 地址开放，并采用 SSL 的数字证书机制进行身份认证。

- 上层访问控制措施：进入生产大网的所有终端都必须通过云安全中心进行安全检测，才能接入生产网络，用户的访问生产大网和子网权限由云安全策略中心进行统一管理和鉴权。

6） 部署主动防御体系

如图 26 所述，基于华为公司的安全产品构建主动防御体系，包括如下几个关键组件：

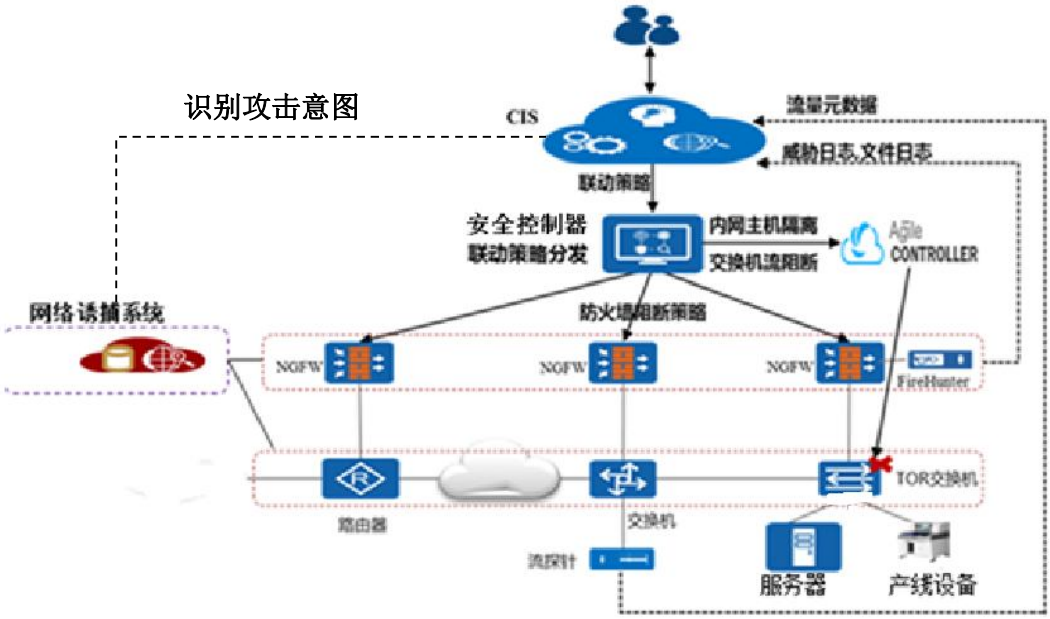

图 26 主动防御体系架构示意图

关键组件如下：

- CIS/FireHunter：安全分析器，具备大数据安全分析和文件分析的能力，能够通过文件，流量和日志综合分析，结合威胁情报，识别未知威胁，联动安全

控制器下发安全策略；

- SecoManager：安全控制器，接受分析器的安全处置措施，编排成为设备可执行的策略，并自动下发给执行；
- NGFW:安全执行器，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，进行安全业务部署，实现安全处置闭环，同时对接CIS，实现本地信誉升级。
- 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
- 主动防御系统的关键流程步骤：
- 数据采集：流探针或防火墙等采集器采集网络中的流量、日志数据，并将分析结果上报给 CIS 大数据平台进行关联分析。
- 威胁检测：CIS 通过大数据分析方法从海量数据中分析出异常流量和威胁，生成两种联动策略：一种是直接进行 IP 五元组阻断的策略；另外一种是将攻击者引诱到蜜罐的策略。
- 策略下发：将 CIS 下发的关联策略转换成安全策略，下发到对应的安全执行器 Firewall 或者交换机，安全策略包括攻击报文阻断策略、诱骗响应策略等。
- 攻击阻断：Firewall 根据 SecoManager 下发的安全策略执行阻断策略，实现五元组阻断。防火墙可以配置定时从 CIS 下载信誉更新，实现全网的本地信誉同步，提升安全防护能力。
- 蜜罐诱捕：交换机或者安全网关将攻击报文，重定向到蜜罐后，蜜罐通过提供虚假资源与其进行交互，并进一步确定其攻击意图，从而改变各安全节点的安全配置策略。

制造基地的主动安全防御体系部署方案，如图 27 所示，关键部署要点如下：

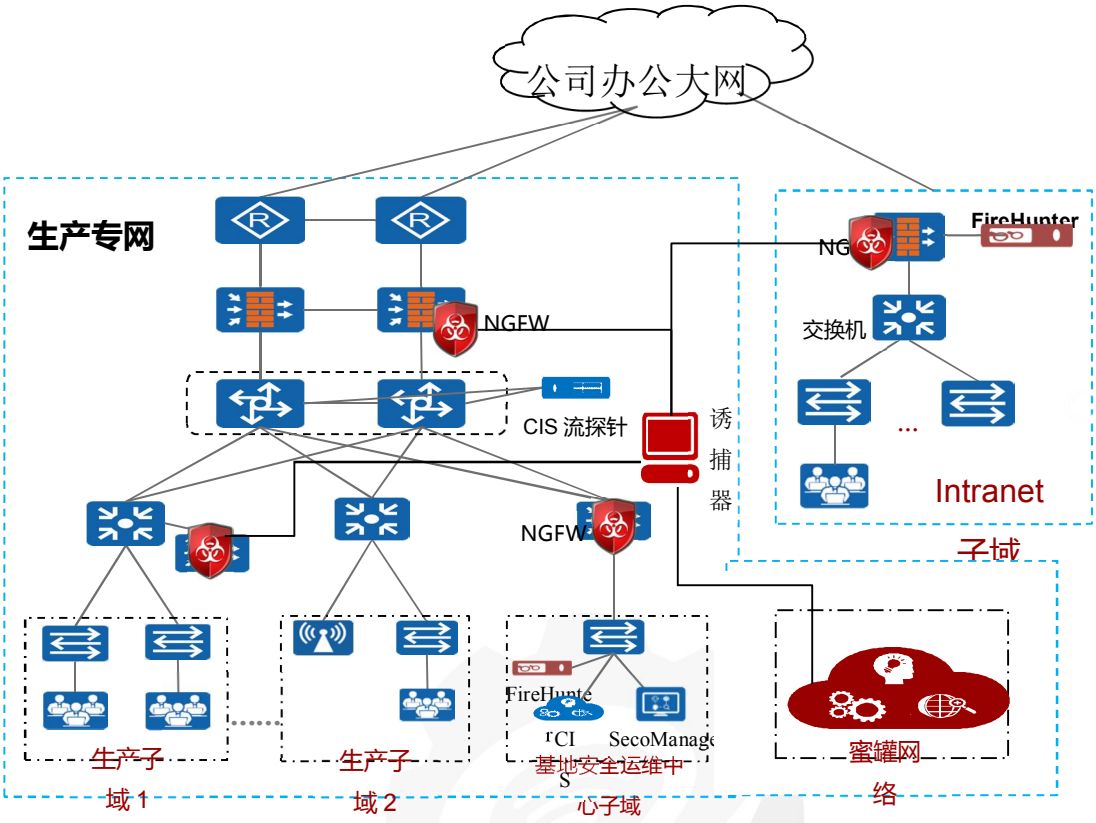

图 27 主动安全部署策略示意图

关键部署要点：

- 制造基地的安全运维中心部署 CIS 平台、沙箱 FireHunter、安全控制器 SecoManager；生产大网和各子网的关口处部署 CIS 流探针，通过交换机端口镜像获得原始流量。
- CIS 流探针提取流量 Metadata 元数据上报 CIS，同时还原文件送给 FireHunter 检测。
- 总部 NGFW 和 FireHunter 的日志信息上报 CIS 采集器。
- 各子安全域关口部署 NGFW 和沙箱，通过 NGFW 和沙箱联动部署实现恶意文件的检测。
- 诱骗功能部署在关口的防火墙上或者交换机上，通过诱骗功能器，将非法扫描等工具报文引入到独立的蜜罐网络中。
- CIS 基于流量、文件、日志采集信息，结合自身的高级威胁检测模型进行分析，发现威胁，并根据联动规则进行联动策略的下发，通过防火墙或交换机进行五元组阻断和主机隔离，实现威胁快速闭环。
- CIS 将 FireHunter 分析出的风险目标（威胁文件、恶意 URL）汇聚为内

部情报资源，以本地信誉的形式共享给网络中的传统安全设备（例如 Firewall、NIP-IPS 设备），实现本地文件信誉在全网的快速共享，提升整体防御能力。

4. 创新点和应用价值

1）先进性及创新点

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，提高防攻击的反应能力和预警能力。

2）实施效果

适用于各种电子制造基地、无需对现有的网络和设备进行大规模改造，另外主动防御体系不影响现有生产的数据通信，该制造基地的安全部门在此方案的基础上，还结合主机安全加固、反病毒机制和定期的安全测试检查等措施，有效地应对了多次安全攻击事件，包括 17 年的勒索病毒和 ARP DDoS 攻击等针对基地的攻击事件中，能够做到及时预警和快速反应。

5. 案例提供方

华为公司

案例七 某油田公司风城油田作业区工控安全加固案例

1. 方案概述

近年来，随着工业控制系统信息安全事件不断发生，“震网”、“火焰”、“毒区”、“Havex”等恶意软件严重影响了关键工业基础设施的稳定运行，充分反映了工业控制系统信息安全面临的严峻形势。工控安全威胁长期以来就已存在，但由于信息的曝光度不高，并没有引起广泛重视。随着两化融合的推进，工业控制系统面临的安全威胁就更加凸显。面对越来越严峻的信息安全形势，国家已高度重视工业控制系统信息安全工作，各级政府监管机构和行业组织也相继发布法规或指南等指导性文件。

风城油田作业区是某油田公司下属的一个专门从事油气田开发的二级单位，油区面积 248.3km²，生产战线长达 128km。2014 年，风城油田生产超稠油 248.3 万吨，成为全国最大的整装超稠油油田。风城油田作业区一直致力于搭建一套实用有效的安全体系架构，解决采油厂工控网络信息安全问题。

2. 典型安全问题

1） 工业控制网络体量庞大，结构复杂；

2） 工业控制网络安全防御等级低、无灾备能力；

3） 依据《工业控制系统信息安全防护指南》的相关规定，在安全软件选择与管理、配置和补丁管理、边界安全防护、身份认证、远程安全访问、安全监测和应急预案演练等方面都存在不足。

3. 安全解决方案

根据现场的具体安全问题，威努特采用以“白名单”为基础的工业控制系统安全“白环境”构建理念，对作业区工业控制系统采取“垂直分层、水平分区、边界控制、主机防护、内部审计”的设计方针。

“垂直分层”即对工业控制系统垂直方向化分为四层：现场仪表层、工业控制层、生产管理层、信息管理层。

“水平分区”指各工业控制系统之间应该按相同安全防护级别，并对相互信任的系统进行分区分域，使整个工业控制系统在信息安全防护建设过程中做到纵向多层防御，横向从点到面。

“边界控制”即对系统边界各操作站、工程师站、工业控制系统连接处要进行边界防护和准入控制等。

“主机防护”即对工程师站、操作员站、OPC 服务器等主机系统进行安全防护。

“内部审计”即对工业控制系统内操作人员的操作行为进行事前监控、事中记录、事后定位，最后将各层面的日志统一收集起来，进行综合分析，得出整个工业控制系统信息安全防护态势，帮助信息安全管理人员对单位内部的安全状况有个全面而细致的了解。

设计方案具体内容包含：

1） 通过部署工业防火墙对作业区内的多个采油厂工控网络进行区域隔离，配置不同的访问控制策略，杜绝非法行为；

2） 在采油厂各工程师站、操作员站上部署工控主机卫士，通过白名单的方式，防止病毒对工业主机、工控网络造成破坏。配合使用适配于工控主机卫士软件的安全 U 盘实现数据的安全传输及信息防泄露；

3） 在核心交换机上旁路部署监测审计平台，对操作人员的行为进行审计和记录，便于事后追踪溯源；

4） 部署统一安全管理平台，对工业控制网络部署的工业防火墙、监测审计平台和工控主机卫士进行统一的配置和管理，并对其日志信息进行统一收集、分析和管理。

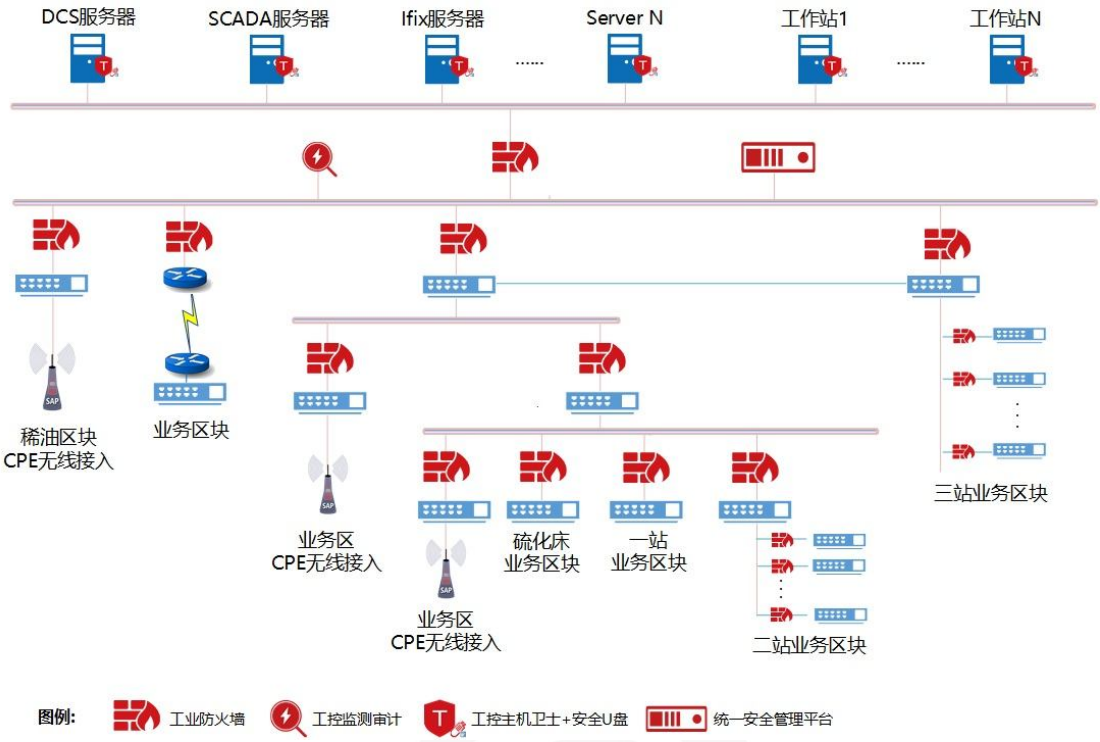

图 28 某油田公司工控安全加固

4. 创新点和应用价值

1）先进性及创新点

根据“风险分析+执行策略+系统实施+漏洞监测+实时响应+安全恢复=系统安全”的建设思路，作业区工控系统安全构建了多层次、全方位、立体的体系架构。以保障工控系统信息安全、稳定运行为出发点，结合油田生产过程的多样化，研究建立安全风险模型，奠定了安全技术与运行管理的基础。融合工业防火墙、“白名单”防护、统一安全管理等技术，建立了以主动安全防御为核心的技术体系，实现了“分区分域、纵深防御、统一监控”的建设目标，提高了风城工控系统信息安全风险防控能力。结合运行、管理、技术三个方面，建立起可管理、可控制、可信任的工控安全运行管理体系并形成长效运行管理机制。

2）实施效果

- 有效提升工控系统信息安全防御能力，实现了访问控制、协议过滤、病毒防御、主机加固、安全监控等功能，保障了生产监控业务的连续性，减少因服务中断给作业区造成的潜在经济损失，为油田生产运行安全保驾护航。

- 实现了对工控系统内所有工控安全防护设备及系统的统一管理，降低运维管理成本。
- 在 2017 年爆发的“勒索”病毒事件中，与油田公司某二级单位大面积感染导致的工控系统瘫痪相比，作业区工控系统未发生感染事件，节约了系统维护和设备购置费用，直接与间接经济效益均很可观。
- 通过不断建设和完善工控系统的信息安全组织机构、管理制度和运行管理流程，提高了作业区工控系统信息安全保护能力、风险识别与评估能力、综合管理能力和应急处理能力。
- 作业区工控系统信息安全统一监测审计，提高了管理效率，降低人员维护工作量。
- 提高了员工信息安全意识，降低工控系统信息安全事件发生的概率。

5. 案例提供方

北京威努特技术有限公司

案例八：城市污水处理厂安全解决方案

1. 方案概述

城市污水处理厂是环境保护的重要设施，也是城市关键基础设施之一。某城市污水处理厂为 AAO 处理工艺，日处理量为 15 万吨，控制系统采用分散控制、集中管理的控制模式，由一个中央监控系统、四个 PLC 控制站、工业通信网络以及现场工艺设备组成，中央监控系统对全厂实行集中监控、管理，PLC 控制站实现对各工段工艺设备进行分散控制，二者通过高速工业以太网进行数据通信。污水处理厂的关键数据通过中国联通 VPN 实时传输至某水务集团调度中心。

城市污水处理厂控制系统以往主要重视功能设计，长期忽视信息安全防护设计，近些年来，水行业工控安全事件频发，控制系统作为保障城市污水处理厂连续正常生产运行以及保证水资源水质安全的核心，其安全问题越来越受到关注。

2. 典型安全问题

城市污水处理厂控制系统存在以下安全风险：

1） 不同区域之间缺少必要的隔离措施，网络接入缺少防护、认证，存在非法接入或错误接入的可能。由于缺乏边界访问控制，工控网络极易被侵入，且受到攻击后无法追踪溯源。

2） 数据通信无加密认证机制，监控层与控制层之间的通信采用标准的工控协议，如 Modbus TCP、ProfiNet、Ethernet IP、ControlNet 等，监控层与管理层之间的通信采用 OPC 协议。实时运行时，系统维护、组态操作缺乏认证、完整性、审计方面的控制，容易遭受 DoS、IP-Spoofing 等攻击。

3） 工控系统中存在各种安全漏洞，包括操作系统、工业软件、控制器、网络设备等都可能存在漏洞，且大部分漏洞不能及时修复，带来了极大安全威胁。

4） 控制系统普遍存在着未设置口令、默认口令、弱口令、共享口令等问题，使攻击者极易渗透至内部网络，执行任何操作，后果不堪设想。

5） 缺乏安全日志，对已有安全日志缺乏监控、审计，无法实现对整个工控系统安全的可感知与可控制。

3. 安全解决方案

城市污水处理厂控制系统安全解决方案遵循以下设计依据：

- 《 GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》
- 《GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求》
- 《信息安全技术 网络安全等级保护基本要求 第 5 部分：工业控制系统安全扩展要求》
- 信息安全技术 网络安全等级保护测评要求 第 5 部分：工业控制系统安全扩展要求》
- 《信息安全技术 网络安全等级保护安全设计技术要求 第 5 部分：工业控制系统安全扩展要求》
- 《工业控制系统信息安全防护指南》
- 《GB/T 26333-2010 工业控制网络安全风险评估规范》

充分考虑到城市污水处理厂控制系统的业务连续性和工业特性，并且结合上述设计依据，以及针对城市污水处理厂控制系统的相关技术要求，形成如下安全解决方案：

1） 边界安全防护：污水处理厂控制系统与水务集团调度系统之间的通信需要实施边界防护措施，采用身份认证、访问控制、数据加密等技术，保护控制网与管理信息网之间的边界，阻止来自管理信息网的安全威胁。

2） 主机加固防护：中央控制室监控系统中的历史数据服务器、工程师站、操作员站均进行主机安全加固，采用白名单技术，不在列表中的应用软件、脚本、U 盘文件都不允许执行，防止恶意代码通过应用软件、脚本文件、U 盘威胁主机安全。

3） 横向区域隔离：各个 PLC 控制站之间采取区域隔离措施，保护工控网络内部不同安全区域的边界，阻止来自该安全区域外的安全威胁。

4） 控制数据加密：通过实现监控层上位机与 PLC 系统的身份认证，完成关键指令的解密和验证，确保上位机接入及操作指令下发的完整性和保密性。

5） 安全监控审计：在中央监控系统核心交换机中采用旁路监控的方式，监控并记录系统运行过程中企业层与监控层之间、监控层与控制层之间的一切操作

行为，对偏离基线异常操作行为进行告警上报，为事故追溯、责任划分提供证据。

6） 工控漏洞管理：建立工控安全漏洞管理系统，多渠道全方位多级采集漏洞信息，采用动态、闭环漏洞规则情报策略管理流程，使漏洞能及时得到修复。

7） 统一安全管理：实现对污水处理厂全网中各安全设备、系统及主机的统一配置、全面监控、实时告警、流量分析等，降低运维成本，提高安全事件响应效率。

具体部署如下：

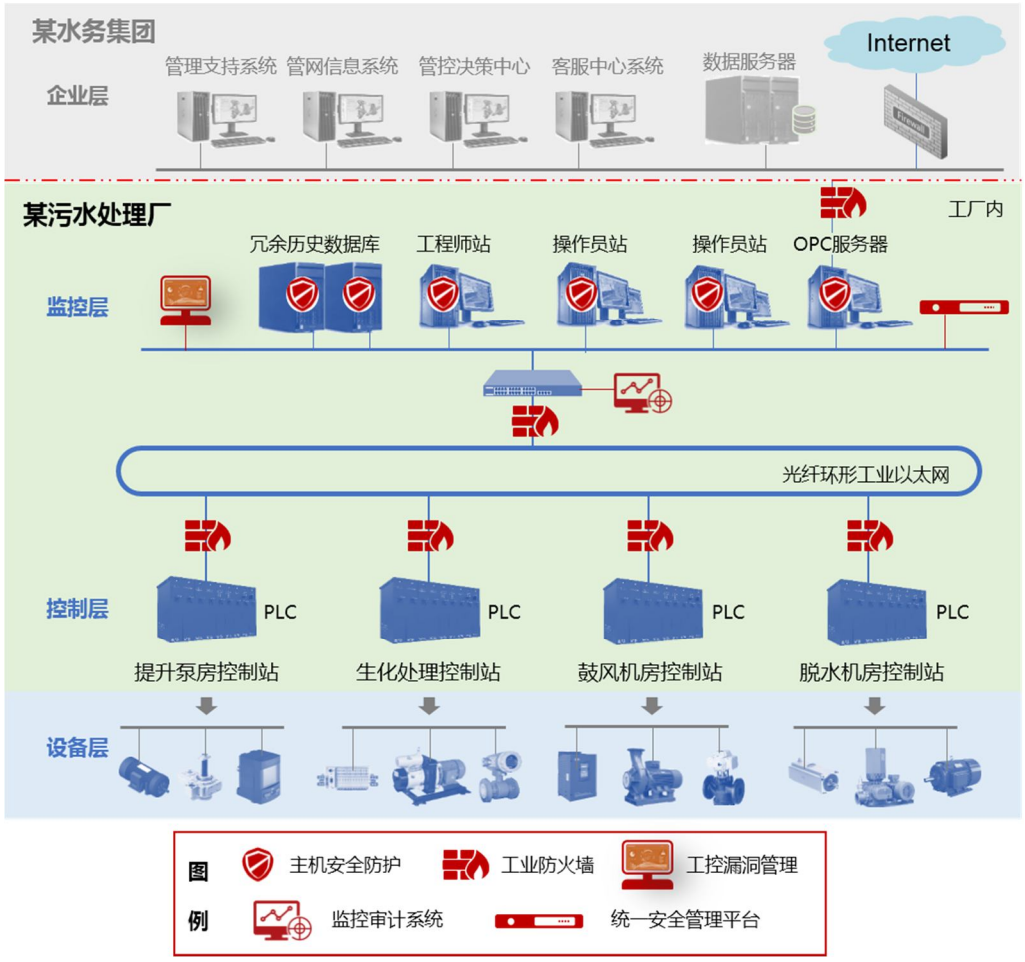

图 29 城市污水处理厂控制系统安全防护体系部署图

监控层部署边界防护网关、白名单主机安全卫士、安全监控审计系统、工控漏洞管理系统以及统一安全管理平台。控制层部署工业防火墙。

1）边界防护网关

- 部署位置：在 OPC 服务器数据出口部署边界防护网关。
- 解决问题：防止来自企业信息网的安全威胁，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。

2）白名单主机安全卫士

- 部署位置：在中央监控系统中的历史数据服务器、工程师站、操作员站均部署白名单主机安全卫士，实现主机安全加固。
- 解决问题：（1）阻止非授权软件或进程的安装和运行，防止恶意代码攻击；（2）避免定期升级病毒库及漏洞库，变被动为主动；（3）防止操作员使用移动介质带入病毒在业务网中扩散；（4）杜绝信息非法窃取、数据和系统遭受非法破坏的行为发生；（5）对关键服务器进行加固，保证服务器安全。

3）安全监控审计系统

- 部署位置：在中央监控系统核心交换机旁路部署安全监控审计系统。
- 解决问题：（1）实时检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，帮助客户及时发现，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。

4）工控漏洞管理系统

- 部署位置：在中央监控系统部署工控漏洞管理系统。
- 解决问题：实现对全厂控制系统全生命周期漏洞管理，确保漏洞及时快速修复。

5）统一安全管理平台

- 部署位置：在中央监控系统中部署统一安全管理平台。
- 解决问题：（1）对全厂安全设备统一管理，如策略下发等；（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）便于中央级维护人员进行维护管理，实现安全事件报警管理。

6）工业防火墙

- 部署位置：在每个 PLC 控制站部署工业防火墙。
- 解决问题：通过工控协议深度解析及应用协议白名单机制，实现监控层上位机与 PLC 系统之间的身份认证、数据加密，阻止不同系统之间的越权访问行为，保障 PLC 系统的安全。

4. 创新点和应用价值

1）先进性及创新点

本安全解决方案参照工控安全相关标准规范，根据某城市污水处理厂控制系统结构、功能及工艺流程要求，构建了覆盖控制系统基础设备安全、实时控制行为安全、业务流程作业安全的一体化深度安全防护体系，防止非授权或意外的访问、篡改、破坏和损失，确保控制系统能长期安全稳定地运行，保障城市污水处理厂出水水质的安全。

2）实施效果

采用纵深防御思想，实现工控网络结构安全和深层防御能力，提升了城市污水处理厂控制系统信息安全总体防护水平，以及网络安全防护管理的合规性，提高了运维人员的工作效率，降低人力投入成本，使得企业的安全投入物有所值。

5. 案例提供方

中国电子信息产业集团有限公司第六研究所（简称电子六所）

案例九 某燃气 SCADA 工业系统安全防御建设项目案例

1. 方案概述

根据 ICS-CERT 的统计显示，从 2009 年至 2017 年，工业控制领域的信息安全事件逐年增多，并且攻击的方式呈现出多样化、复杂化的特点。中国已经成为遭受网络攻击的最大受害国之一，自 2009 年以来，网络攻击已经增长了十几倍，其中 30%是针对关键基础设施。随着通用协议、通用硬件、通用软件在工业控制系统中的应用，这种网络攻击的态势有愈演愈烈的趋势。

针对工业控制系统的攻击主要是威胁其物理安全、功能安全和系统信息安全，以达到直接破坏控制器、通信设备，篡改工业参数指令或入侵系统破坏生产设备和生产工艺、获取商业信息等目的。

对于工业控制系统破坏主要来自于对工控系统的非法入侵，目前此类事件已频繁发生在电力、水利、交通、核能、制造业、市政等领域，给相关企业造成重大的经济损失，甚至威胁国家的战略安全。

2. 典型安全问题

1） 集团公司下属各门站、储配站、输配站以及调度中心内部未进行安全隔离，存在各站之间随意互访造成病毒扩散、生产中断等风险，需要采取安全隔离措施和防病毒措施；

2） 对于工控网络内部可能存在的非法操作、误操作和恶意行为，缺乏审计手段，需要采取有效的安全审计措施，便于事件追踪溯源；

3） 工程师站和操作员站等多采用老旧 Windows 系统，存在大量漏洞，同时 USB 等外部接口缺乏有效管理措施，依赖 U 盘拷贝数据，导致病毒，恶意代码传播时有发生，需要采取有效的主机安全及外设安全防护措施，阻止恶意代码传播，保证生产稳定有序进行。

3. 安全解决方案

经过对现场网络结构、主机设备、系统软件、安全设备等运行情况进行安全

调研和分析，识别出系统资产和脆弱性，确认了燃气集团现场存在的安全隐患和安全防护缺失项，明确了采用自主可控的工控安全核心技术的技术路线。为加强某燃气网络安全防护，构建的安全防护方案如下：

1） 在调度中心和各场站之间部署工业防火墙，进行网络层级间的安全隔离和防护，提高门站、储配站、输配站等各站的安全防护能力；

2） 将每个场站作为一个安全域，在各场站 PLC/RTU 等工控设备的网络出口位置部署工业防火墙，对外来访问进行严格控制，以实现重要工控装置的单体设备级安全防护。

3） 在调度中心、各场站、门站的工程师站、操作员站及服务器上部署工控主机卫士，对各个区域的主机进行安全防护；

4） 在调度中心部署统一安全管理平台，对工控网络中的安全产品进行集中管理、配置和维护，便于综合分析、及时定位问题。

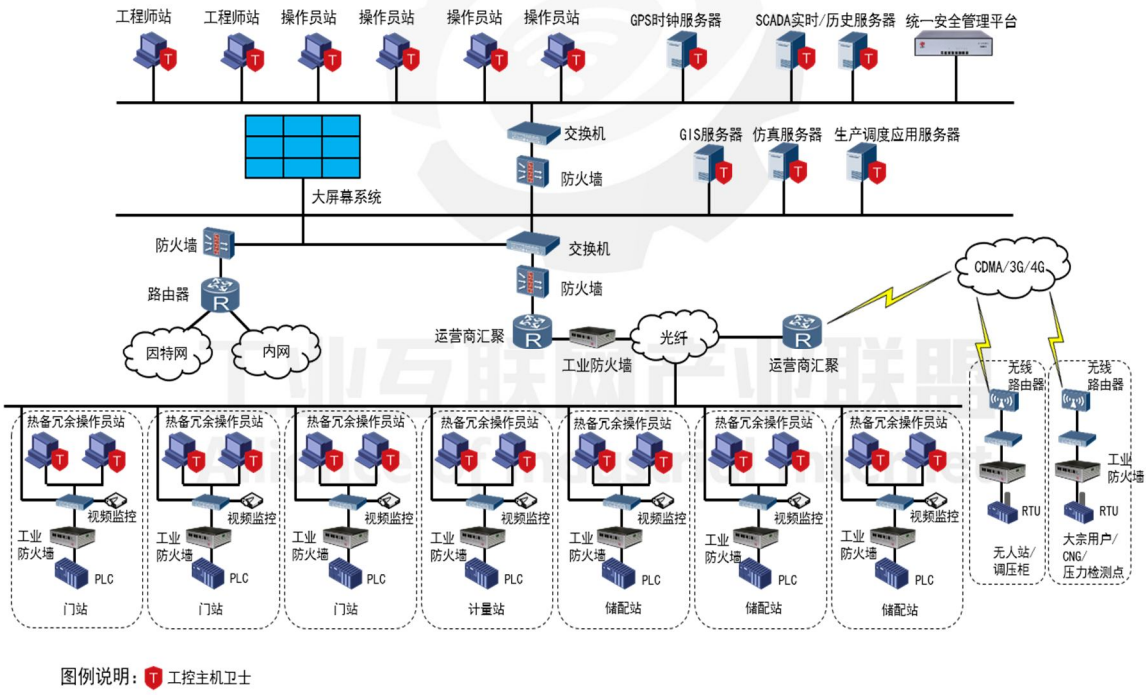

图 30 某燃气安全防护方案

4. 创新点和应用价值

1）先进性及创新点

通过建立工控系统安全生产与运行的“可信网络白环境”以及“软件应用白名单”概念，以完全符合工业现场的自主可控的产品设计，为某燃气集团构筑“安

全白环境”整体防护体系，保护某燃气 SCADA 系统设施的稳定运行，达到“只有可信任的设备,才能接入控制网络”、“只有可信任的消息,才能在网络上传输”、“只有可信任的软件，才允许被执行”的防护效果。

本项目在 IEC62443 标准所提出的纵深防御理念基础上，通过深入研究某燃气 SCADA 系统的系统特点与安全需求,将纵深防御的理念引入到过程控制系统安全领域并工程化，帮助客户实现网络结构安全和深层防御能力。同时通过统一安全管理平台的部署，管理所有软硬件安全设备，实现信息安全的统计监控、集中管理，在最大限度内帮助客户提高运维效率、降低运维成本。

打破了传统“黑”的防护模式，打破工控安全信息孤岛，以更符合工业现场特性的防护手段，以“一个中心，三重防护”的防御体系，将传统的“被动防护”转化为“主动防御”。

2）实施效果

- 使用纵深防御思想，实现网络结构安全和深层防御能力，提高客户安全防护水平；
- 提升了现有操作系统的安全等级，有效的防止来自内部的误操作和来自外部的恶意操作，，提高了主机安全性；
- 将工控网络中的安全设备和系统统一管理,提高了运维人员的工作效率，降低人力投入成本，使得企业的安全投入物有所值；
- 全面提升了某燃气集团网络安全防护管理的合规性；
- 提升了某燃气集团信息安全总体防护水平,保障企业更好的为客户服务。

5. 案例提供方

北京威努特技术有限公司

案例十 某风电集控中心安全解决方案

1. 方案概述

通过分析风电企业在建设风电集控中心过程中所面临的信息安全问题，提出了风电集控中心安全解决方案，该方案阐明了在构筑风电集控中心工控信息安全防护体系过程中企业应采取的安全策略和解决措施，消除来自外部和内部的网络安全隐患，做到防患于未然。

2. 典型安全问题

1) 物理入侵发现

风机及风机控制网络被物理入侵时集控中心无法及时发现并告警；

2) 远程违规操控

风电机组综合自动化系统和风功率预测系统等关键系统，违规通过远程运维操控；

3) 数据明文传输

设备运行数据传输和存储过程中被篡改的风险；

4) 缺少入侵防御

集控中心对来自外部、内部的网络攻击行为缺乏防御手段；

5) 缺少安全审计

安全事件发生后不能迅速定位找出问题根源。

3. 安全解决方案

安全解决方案从物理与环境安全防护、安全运维、主机防护、区域隔离与边界防护、入侵检测与审计、统一安全管理六个方面来进行设计，下面分别来进行介绍。

针对集控中心无法及时发现风机及风机控制网络被物理入侵的问题，采取风塔和关键机房处部署红外防盗报警系统，将非预期进入关键区域的行为形成告警信息发送至集控中心，提醒运行人员采取相关处置措施，防止入侵行为被忽略或

损害扩大化。

提供集控中心和风场之间安全运维通道，在集控中心与风场之间采用电力专线通信，同时在场站侧和集控中心侧分别部署纵向加密认证装置，满足远程安全运维的需求。

主机安全卫士提供安全可信的操作环境，保证数据交换与储存安全，杜绝移动存储介质“滥用”的安全隐患，保障集控中心以及风场工控主机间数据安全。

集控中心划分安全 I 区、安全 II 区和安全 III 区（管理信息区）。安全 I 区与安全 II 区之间采取白名单策略和协议分析以实现逻辑隔离；安全 II 区与安全 III 区之间采用正向隔离装置物理隔离。区域隔离与部署主机安全卫士措施结合，快速识别网络上的非法操作、外部攻击和异常事件，实时告警或阻断非法数据包，提升来自内部和外部攻击行为的防御能力。

对安全 I 区部署网络监测和审计系统，实现工控网络资产管理、设备运行状态监测、异常行为监测和工控协议细粒度审计等功能。审计系统基于机器学习和深度协议分析技术，自动收集网络数据以及进行行为识别并提取特征，生成白名单规则，实现安全事件的及时追溯和定位。

在集控中心生产控制大区部署安全管理平台，实现主机安全卫士、网络监测和审计系统等安全产品的统一管理，提高管理人员的工作效率，降低企业的人员投入成本。

某风电集控中心为了满足网络安全等级保护 3 级要求，在规划设计的安全解决方案见下图。

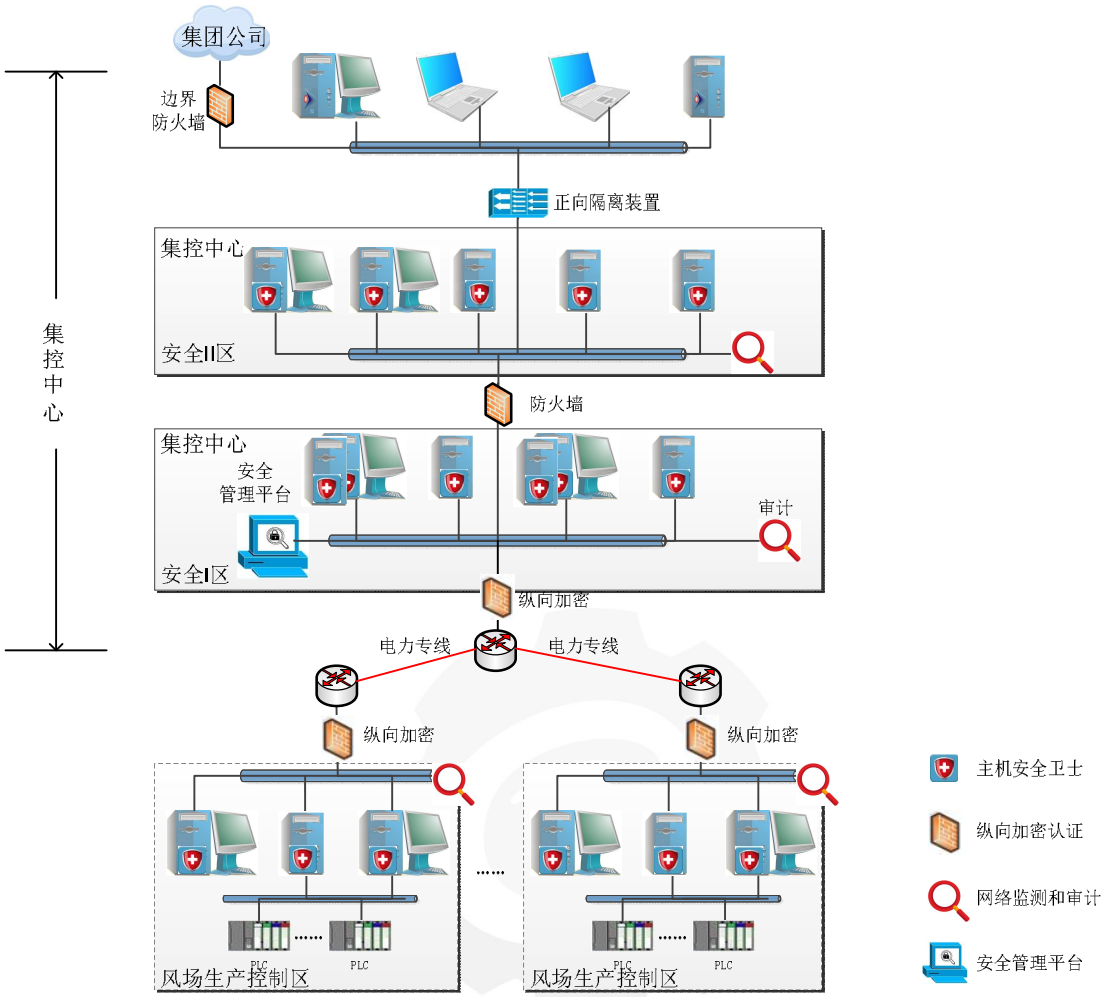

图 31 某风电集控中心网络拓扑图

1） 物理与环境安全

在风场风塔设备电子间部署红外报警设备，并将信息通过光纤环网发送至安全 I 区红外报警服务器，通过该服务器发送至集控中心进行显示和告警。

2） 安全运维

在集控中心和风场之间采用电力专线通信（2Mbps），并在场站侧和集控中心分别部署纵向加密认证装置，为远程运维提供安全加密通道。

3） 主机防护

在集控中心安全 I 区与安全 II 区服务器和工作站上部署主机安全卫士，实现进程与应用程序白名单、移动存储介质管理、补丁管理、防病毒管理、主机安全审计等功能。

4） 区域隔离与边界防护

- 区域隔离，在集控中心安全 I 区和安全 II 区之间部署防火墙。在安全 II 区与安全 III 区之间部署正向隔离装置。
- 边界防护，在安全 III 区与集团公司之间部署防火墙。

5） 网络监测与审计

在集控中心安全 I 区交换机部署网络监测与审计系统，通过对工控网络流量的采集以及协议深度分析，实现流量和状态实时监测功能，并能对所有活动提供协议和流量审计，生成完整记录，便于事后溯源。集控中心与场站侧网络监测和审计系统一起完成实时监测功能。

6） 统一安全管理

在集控中心安全 I 区部署安全管理平台，通过安全管理平台对在集控中心和厂站侧部署的主机安全卫士、网络监测和审计系统进行管理、配置和集中运维。

4. 创新点和应用价值

1）先进性及创新点

该风电集控中心安全解决方案实现场站侧和集控侧网络流量实时监视功能，实现场站侧主机安全卫士和安全审计系统的统一管理，有利于实现集中安全运维。

2）实施效果

通过本安全解决方案的部署，可满足网络安全等级保护 3 级要求，有效提升风电集团集控中心的信息安全防护水平，保障风场的安全运行。

5. 案例提供方

中国电子信息产业集团有限公司第六研究所（简称电子六所）

案例十一 某发动机制造企业SD-WAN工业专网安全解决方案

1. 方案概述

随着工业互联网的提出，工业网络正在向扁平化、IP化演进，越来越多的工厂内设备接入工业专网，并通过互联网进行跨区域传输。同时企业上云已经成为共识，通过结合公有云与私有云，打造企业混合云成为未来一段时间内的大趋势。因此工业企业各机构、厂区以及云数据中心间面临不同于以往的网络互联和网络安全挑战。传统的网络设备和网管系统使用复杂、技术要求高，不能满足工业企业对网络的便捷有效管理需求。同时为保证网络安全，需要在网关处堆叠多种不同类型的安全设备，不但组网复杂，管理维护难度大，也自然造成设备采购和运维成本高。

某发动机制造企业在智能转型过程中，通过采用 SD-WAN 工业专网安全解决方案，成功避免了上述问题带来的困扰。该方案包含位于云端的集中管理平台和用户侧的安全网关。集中管理平台利用SDN/NFV技术，在控制层实现全网业务及网关设备的集中配置与管理，包括配置网络策略、查看运行状态、监控网络异常等。安全网关为X86架构的通用硬件，多种网络功能以虚拟机或docker形式安装在网关中，实现软件与硬件解耦。

2. 典型安全问题

1） 企业总部厂区目前在进行智慧工厂改造，厂区内生产设备逐步联入企业内网并将数据上传至MES系统，一些敏感设备数据存在跨区域传输需求。但目前企业缺乏组建工业专网所需的防火墙、VPN、访问控制等边界防护措施，难以实现工厂内网与工厂外网的隔离，也就无法保证生产运营数据的安全存储和防止关键数据外泄。目前企业需要运用上述安全措施在总部厂区，工程研究院和欧洲研发中心之间组建跨区域的工业专网。

2） 企业在智慧工厂改造过程中，组建企业内部私有云平台，将关键生产系统部署于私有云上，同时部分企业应用部署于公有云，但企业缺乏组建安全的混合云网络的手段。

3） 企业管理人员缺乏统一的管理平台对网络节点进行集中管控，无法及时对网络异常状态进行有效处理，无法对设备进行远程管理维护。

3. 安全解决方案

该发动机制造企业通过部署基于 SDN/NFV 技术的 SD-WAN 网络实现工业专网的组建，并保证专网安全。SD-WAN 网络由集中管理平台与安全网关组成，集中管理平台在云端进行部署，可对整个网络进行统一管理；安全网关通过虚拟化的方式灵活部署网络功能，来提供企业工业专网所需的各种网络安全特性，同时安全网关支持通过 TD-LTE 网络进行数据传输。

该企业的 SD-WAN 工业专网解决方案如下图所示：

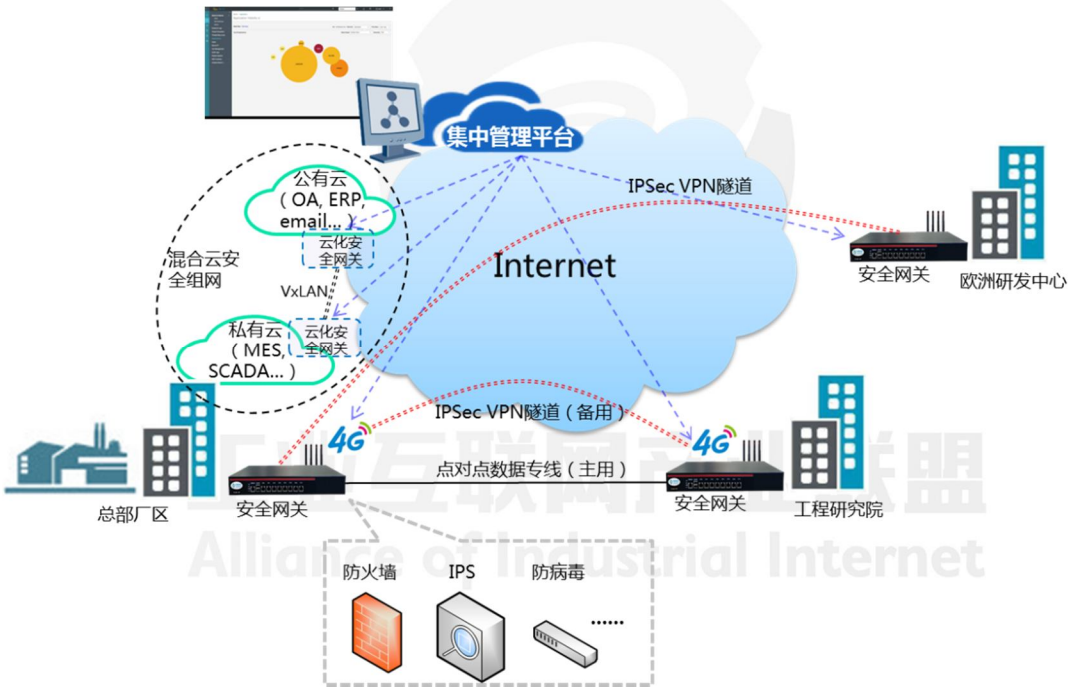

图 32 SD-WAN 工业专网解决方案

详细的解决方案说明如下：

1） 在该企业总部厂区与工程研究院之间各部署一台安全网关，通过安全网关在两点间部署主备两条数据链路进行数据传输，主用链路为一条点对点数据专线，该链路为企业专用，与 Internet 物理隔离。备用链路为使用安全网关建立的一条加密的 IPSec VPN 隧道，通过 TD-LTE 无线网络进行数据传输。基于 IPSec 的加密功能，可以保证数据的端到端安全传输。安全网关支持 TD-LTE 通信功能，

在不额外增加物理链路的情况下，快速完成备用链路的部署。在主链路故障时，业务会自动切换至 TD-LTE 链路。

2） 在该企业的欧洲研发中心中部署安全网关，并与总部厂区基于 Internet 建立加密的跨国 IPSec VPN 隧道，在原有互联网数据传输基础上保证数据的传输安全。

3） 在该企业的公有云和私有云的虚拟机上分别云化部署安全网关，并通过网关支持的 VxLAN 功能，打通公有云和私有云间的大二层网络，同时使用网关的安全功能保证混合云网络安全。

4） 该企业网关人员通过集中管理平台对全网设备、网络功能和业务流量进行统一管理，可视化管理方式使网络管理便捷高效。

4. 创新点和应用价值

1）先进性及创新点

SD-WAN 工业专网安全解决方案先进创新性体现在：

- 网关集成丰富的安全防护功能

安全网关支持 L2~L7 的安全防护能力，包括防 DoS/DDoS 攻击、防恶意端口扫描、应用层防火墙、防病毒、UTM 等。通过网关自带的主动入侵防御功能，防火墙可以识别并阻止 L7 的异常流量和攻击，提高网络可靠性实施效果。防病毒功能可以检测压缩包内的文件，并提供病毒阻断功能，防止带毒文件被下载到本地。支持对 HTTP、POP3、SMTP、IMAP 和 FTP 协议报文中的木马、病毒、广告程序、蠕虫和其他恶意程序的检测和阻挡；支持对 ZIP 或者 RAR 数据包的内容扫描功能，可以智能跳过指定大小的压缩包或者带密码的压缩包；检测到病毒之后，发送告警信息至平台。

- 采用 SDN 和 NFV 实现软硬件解耦

该解决方案采用控制平面和转发平面分离、控制平面集中实现的新型网络体系架构。控制平面利用控制-转发通信接口对转发平面的设备进行集中控制，并向上提供灵活的可编程能力。多样化的网络功能则部署在通用的 X86 硬件上，极大降低网络功能对专用设备的依赖，从而促进网络功能与服务的创新。

- 通过集中管理平台对全网设备统一进行管理维护

B/S 结构的集中管理平台，以图形化方式为用户展现网关运行状态、流量分布、告警信息、上网行为统计等，方便网络管理员在线掌握网络情况，及时处理异常事件。除此之外，集中管理平台支持用户远程配置网络功能，并根据需要下发至相应网关，实现分钟级网络配置和升级。

- 云数据中心大二层组网技术

该方案支持 VxLAN 大二层组网与网关云化部署技术，打通公有云与私有云通道，将企业分布式的云资源整合起来，从而解决逻辑网段不足、虚拟机动态迁移等问题。

2）实施效果

通过 SD-WAN 工业专网安全解决方案，该发动机企业有效的建立起了跨多个厂区和机构的工业虚拟专网，保证了工业内网与工业外网的安全隔离，实现了混合云的安全组网。同时通过使用基于通用硬件设备的多功能网关，基于 Internet 组建工业虚拟专网，大大降低了企业的网络建设和网络安全成本。利用集中管理平台对网络的统一管理，大大提高了企业管理网络的便利性。本方案可面向各类具有工业专网组网需求和网络安全需求的工业企业进行复制推广。

5. 案例提供方

中国移动政企分公司

案例十二 工业互联网云网可信互联安全解决方案

1. 方案概述

让万物拥有智慧的计划在近几年来基于技术基础不断推展，其具有的智慧和洞察力会产生更多可开采数据，我们称之为“数据虚体”，从而将使万物互联的商业价值得到进一步提高。有了健全的“数字虚体”作为基础，才有所谓的 AI 分析能力、工业应用商店、开放性架构等“上层建筑”施展的空间。为了避免让“数字虚体”生而残疾，无缝打通从底层设备到云端的链路和数据流是必备条件。这种从下到上的贯通分为两个层面：一是从设备端到云端的通讯链路畅通，即使经过网关的转换，仍能保持数据标签的和谐一致，从云端可以一线贯通，自动识别物理设备；二是从底层到上层的数据结构匹配，数据不仅能够被调用，还要能够被解读和分析。

混合云融合了公有云和私有云，是近年来云计算的主要模式和发展方向，但也存在缺少数据冗余、法规遵从、SLA 架构拙劣、风险管理、安全管理等问题。提供工业互联网可信联通混合云的最佳解决方案——为城市电力配电、电力调度、互联网数据云、机场枢纽、城市轨道站、大型综合医院、行业数据中心等重要场景关键基础设施故障应急处理提供一站式敏捷解决方案是本方案的主要目的。其技术可以实现低成本敏捷地部署应用于数字工厂、智慧农业、移动基站的数据采集、智能设备控制、智能楼宇、安防监控、分布式智能家居、数据中心管控、智慧交通、智慧水务、智慧能源，乃至整个智慧城市建设等场景。

本方案用于实现工业互联网云架构下为不同应用场景打开可信私有通信通道，解决设备互信联网问题，使可信设备在外网任何地点都可授权访问及控制可信混合云的“透聚节点”内网设备；在外网任何地点都可授权访问及控制可信混合云的“透聚节点”内网设备；将不同地区的“透聚节点”内网设备由云端统一管理平台控制并相互连接组成一个跨互联网的可信互联物联虚拟专网。

2. 典型安全问题

一般企业无法仅凭一己之力构建并提供安全、可扩充的工业物联网云端联机

网络服务，其中最大的挑战，便在于如何将大量非智能非网络化的设备等上云，实现将非专为云端联机设计的本地侧应用推向数字化远程服务。数字化除需符合可扩充、多样化的工业需求外，同时也要能确保数据传输的安全和实现异构网络化连接。

万联网络推出的最新网络即服务(Network as a Service;NaaS)产品 Edge 系列及物云平台解决方案，能够基于 AND 应用定义网络服务和透过三层网络透传代理技术，安全的支持连接大多数传统现场设备基于端口的云端联机，有效解决“企业上云、敏捷应用”的应用级数字化云化的平滑过渡问题，借此加速工业 4.0 的规模化部署。

3. 安全解决方案

万联的 MACnets 物云可信混合云解决方案通过 ADN 交付管理+可信控制+可视化接入分析+安全四大能力，提供了集中的智能应用交付和流控调度；可信域和节点管理；全面的安全分析防御；灵活的应用上云发布，让用户轻松过渡并跨越到多云平台的敏捷应用管理需求。

MACnet 物云 E2E 智能边缘互联设备及客户端软件： E2E 物联通 EDGE 路由/网关系列以及 CC 客户端（Client for Cloud）软件系列。智能边缘路由器服务能够让客户迅速以自有方式连接三层网络，而且无需拥有/管理路由器或实体基础设施。简化了应用上云授权管理和所有权上面的复杂问题，E2E 关键技术和服务让企业能够轻松连接云服务和本地侧应用，通过虚拟边缘对等网接入(E2E)扩展服务足迹，对接业务生态系统合作伙伴，无需部署实体网络基础设施。在 MACnet 物云 E2E 智能边缘路由器服务支持下，任何人都能获得无缝的云互联能力，从而打造经过优化的混合云、多云和多区域网络。

万联的 MACnets 物云可信混合云提供两种部署方式：

一是基于 NaaS 网络即服务，并由 MACnets 物云可信鉴权服务进行管理，简单易行，兼具备成本效益，有助于快速有效地桥接连通本地侧部署和多云世界；

二是基于 ADN 软件形态的自我域管理、可扩展的应用交付解决方案，敏捷部署于数据中心或云端。换句话说，用户根据具体业务和应用需求进行选择。

万联 MACnet 物云可以带来成本上面的节省、敏捷性和安全的连接，无需依

赖数据中心。这项服务能够支持至少一个对等网络云到本地侧的连接服务，从而实现边缘到云边缘的连接，并能支持本地端的数据包转发和智能化路由决定。在 MACnet 物云的支持下，还能直接为 SaaS 云应用服务平台提供专用的数据连接通道，而这些 SaaS 提供商传统上只能在互联网交换中心上面才能连接数据。

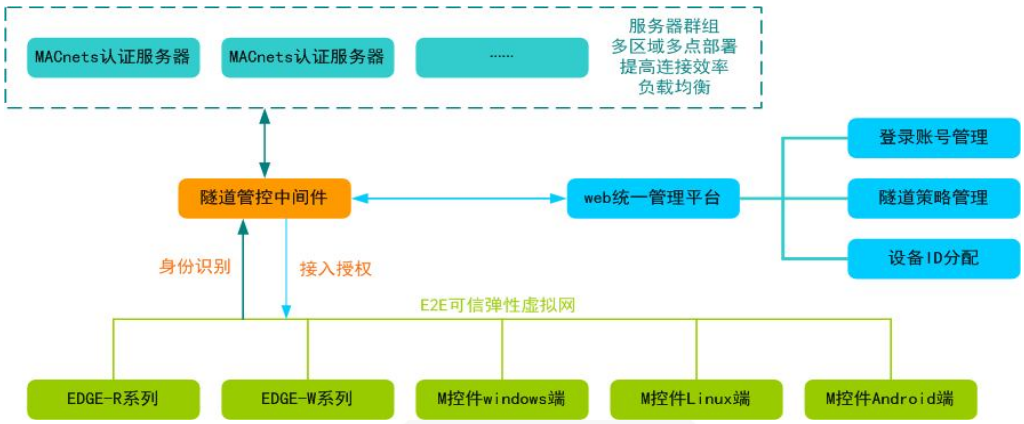

图 33 物云平台结构拓扑图

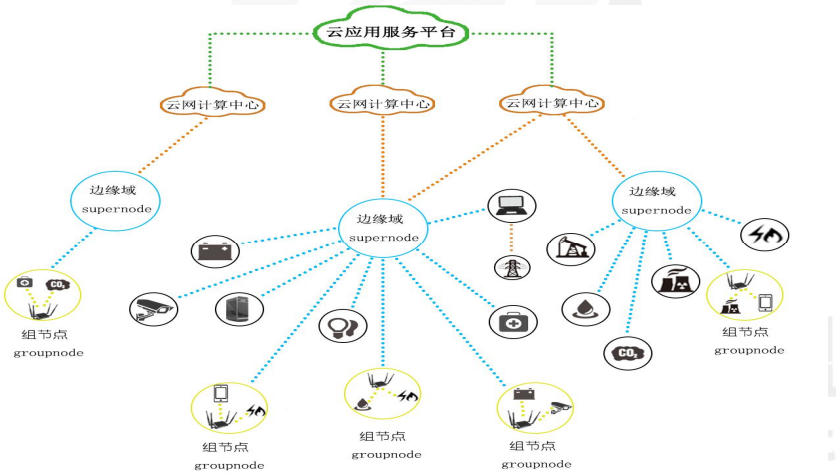

图 34 物云连接架构

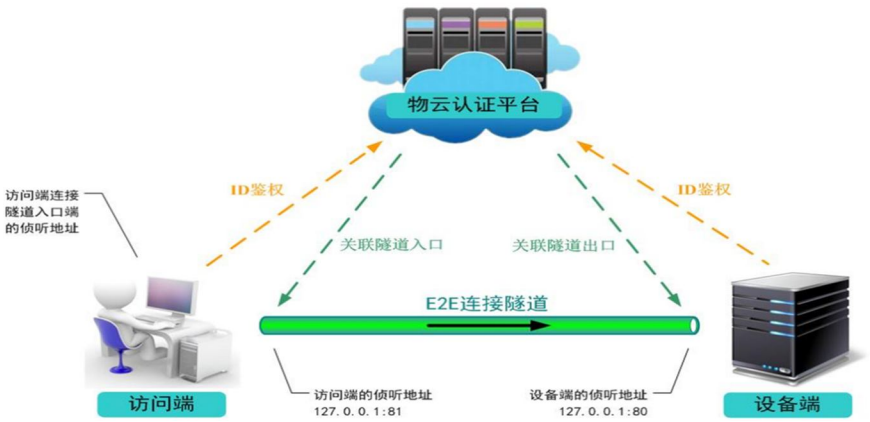

图 35 E2E 技术隧道基础结构图

	物云	拨号VPN	VPDN	运营商MPLS专线
服务开通	当天	根据情况而定	半个月	1个月
接入方式	运营商接入或自建	自建，需固定IP或DDNS	运营商接入，需固定IP及安全服务器	运营商接入，专线组网
方案配套	硬件或软件	硬件及软件	硬件及软件	硬件
组网结构	去中心全网状结构	星型结构	星型结构	点对点
管理对象	设备+端口+访问者	IP网络+访问者	IP网络+访问者	IP网络
组网模式	虚拟物联专网	虚拟业务组网	无线业务专网	业务专网
访问方式	ID→端口（支持自定义）	IP→节点	IP→节点	节点→节点
连接管理	自主可控	自主可控	运营商支持+用户管理	运营商管理
管理方式	平台化	本地	平台化	运营商管理
安全保障	等保三级	无	等保三级以上	等保三级以上
QoS等级	金（支持对时延和丢包率有较高要求的企业数据应用）	无	金（支持对时延和丢包率有较高要求的企业数据应用）	钻石（支持对时延和/或抖动要求很高的应用）
可用率等级	A以上（≥99.9%，运营商的网络服务中断不在此计算范围内）	无	A以上（≥99.9%）	AAA（≥99.99%）
服务支撑	网络工程师	专业网络工程师	运营商	运营商
使用成本	无忧	较低	较贵	昂贵
方案特点	部署灵活、快捷，管理使用方便，接入及维护成本性价比高，无需更改现有网络架构及设备配置	传统的局域网接入解决方案，支持自定义加密要求和接入方式，管理复杂，专业性强，需配合内部防火墙实现安全管控。	升级的局域网接入解决方案，由运营商提供支持，可实现云端统一管理，用户需具有一定的网络运维能力，需配合内部防火墙实现安全管控，使用成本较高。	链路稳定可靠，需额外的网络成本，只解决了固网连接，不能解决外网移动设备的接入。

图 36 万联物云方案与拨号 VPN/VPDN 及 MPLS 专线方案对比

4. 创新点和应用价值

1）先进性及创新点

MACnet 物云为云到云，或是本地侧跨越边缘侧到云等的敏捷连接需求提供支持，让 MACnet 物云客户能够在不同的云服务提供商环境中进行远程工作协同和数据穿透转移，创造最为适宜的云和本地间的混合网络解决方案，并支持混合云和多云架构。

本地侧网络和不同的云服务提供商可以在全球范围内建立虚拟边缘对等网接入（E2E），实现对业务生态系统合作伙伴的互联和对接，支持快速部署和削减拥有成本。

客户可以在全球不同的路由域中创造虚拟云端应用交付，为覆盖全球提供敏捷部署支持，并支持本地化的路由决定。

有了 MACnet 物云，便无需再购买公共 IP 地址空间或是自建专网或建立私有云系统，能有效减少涉及管理三层网络、网管行政管理审议和复杂网络结构优化和运营上面的混乱问题。

解决方案物联网特点：

- 设备互联去 IP 化，采用自定义（随机）ID 实现网内设备的管理与身份识别。
- 数据加密去中心化，每条虚拟隧道均使用 P2P 对等加密方式进行密钥协商，在保证数据传输安全性的情况下大大降低了认证服务器的系统压力。
- 集中管理弹性组网， 可通过统一的云认证管理平台实现快速构建云网接入弹性网络。
- 网内设备组网支持可信域隔离和自定义多级分组。
- 部署敏捷，去专业化。无需改变现有网络结构，无需专业网络工程师支持，一键式适配网内应用端口，授权访问和双向流控。
- 设备接入认证服务器支持主备及负载均衡，可实现百万级节点接入。
- 软硬件多模式结合，除了采用隧道控件支持常见的操作系统（windows、Linux、Android 等）配套的 PC 端、移动端设备外，还可以采用专用边缘云网接入设备对各种不具备联网功能的现场工业总线设备实现云网数据加密接入。
- 边缘云网接入设备的联网支持链路主备自动切换，支持 sim 卡及 esim 卡,还特别解决了 esim 多运营商融合联网自动切换技术。

2）实施效果

基于万联“边缘云网接入技术”的物云平台及万联 EDGE 系列云网产品可应用于数字工厂、智慧农业、移动基站的数据采集、智能设备控制、智能楼宇、安防监控、分布式智能家居、数据中心管控、智能交通等场景。将众多厂商的设备和信息节点通过互联网这个基础信息高速公路，安全、可信、高效地互联互通起来，将不同厂商、不同设备、不同网络系统、隔离的信息节点等互相认证联网打通，实现真正的可信、安全的工业物联网生态。

5. 案例提供方

常州万联网络数据信息安全股份有限公司

案例十三 石油石化行业工控安全等保服务安全解决方案

1. 方案概述

在深入调研石油石化工业企业生产控制系统现状的基础上，结合《信息安全技术网络安全等级保护基本要求》中的工业控制系统安全扩展要求，建立评估模型，开展工业企业生产控制系统信息安全风险评估工作，提出工控系统网络安全对策建议，指导后续的监控系统防护建设和管理工作。

本方案利用长扬科技自主研发的工控安全等保工具箱，可实现对多种工业场景的全流程等保自动化服务，具备方便、快捷、专业、标准化与自适应相结合等服务作业特征。

2. 典型安全问题

1） 生产控制网络缺乏自身全面的安全性设计

我国石油石化行业生产控制系统安全防护滞后于系统的建设速度，生产控制系统缺乏自身的安全性设计。在信息安全意识、策略、机制等方面都存在问题。

2） 工控网络存在一定的脆弱性

- 已建项目主要软硬件多为进口，可能存在后门。
- 油气开采、管道储运广泛使用无线通信，易被野外搭线监听。
- 部分网络借用公共电信网络和互联网组网，增加了网络接入风险。

3） 工控网络面临着现实和潜在的威胁

- 现实威胁：U 盘滥用、病毒肆虐、软件乱装、违规操作、缺乏有效的访问控制手段。
- 潜在威胁：攻击石油石化行业工控系统技术门槛越来越低，易被信息战攻击。

4） 工控网络安全防护体系尚未形成

- 关键资产底数不清楚。
- 严重漏洞难以及时处理，系统软件补丁管理困难，难以应对 APT 攻击。
- 两化融合加速了网络安全风险的暴漏。

3. 安全解决方案

1） 风险评估类型

本方案同时采用了管理和技术相结合的评估手段展开全方位的风险评估，管理风险评估包含工控系统资产风险评估和合规风险评估两种方式，技术风险评估包含流量分析评估和漏洞分析评估。

2） 工控系统资产风险评估：

根据等保要求，对工控系统的信息资产的保密性、完整性和可用性进行分析，根据资产价值识别出工控系统中的重要信息资产。根据管理现状，将资产价值与资产脆弱性、威胁发生的频率进行综合分析，最终评价出工控系统资产面临的风险级别。

3） 合规风险评估：

将石油石化公司的管理现状与《信息安全技术 信息安全等级保护基本要求 第 5 部分：工业控制系统安全扩展要求》的要求进行逐项比对，从影响范围、严重程度、控制措施全面性、控制措施有效性四个维度展开分析，最终评价出石油石化公司生产控制系统的管理方面与合规要求之间存在的风险。

4） 流量分析评估：

选取石油石化公司生产控制系统中数据流比较集中的一个或几个关节节点，通过将长扬科技的等保工具箱的威胁评估平台以端口镜像部署方式接入到节点交换机，获取该节点数据流量包，长扬科技安全实验室对数据流量包中的协议、端口、数据访问等情况展开深入分析，找出其中可能存在的异常行为。

5） 漏洞分析评估：

将资产识别过程中识别出的石油石化监控系统核心资产信息录入到长扬科技的等保工具箱的威胁评估平台，与长扬科技强大的工控系统漏洞库进行漏洞比较匹配，识别出关键网络设备、操作系统、控制器等存在的风险漏洞，并对漏洞分布情况进行汇总分析，给出针对逐个漏洞的加固建议。

管理风险评估采用了定性的风险评估方法。定性风险评估并不强求对构成风险的各个要素(特别是资产)进行精确的量化评价，它有赖于评估者的经验判断、业界惯例以及组织自身定义的标准，来对风险要素进行相对的等级划分。最终得出风险大小，只需要通过等级差别来分出风险处理的优先顺序即可。

6） 风险评估过程

为了充分获取是石油石化公司生产控制系统目前在管理和执行方面的真实现状，使评估的结果更贴合实际，在风险评估中，主要通过以下几个步骤来支撑组织的工控信息安全风险评估工作：

- 通过人员访谈、制度调阅和现场物理环境调研，了解组织的工控信息安全管理现状；
- 分析石油石化公司信息安全管理工作与工控等保等标准或行业规范之间的差距，总结待改进点；
- 通过技术接入，获取监控系统的网络流量，针对流量展开协议分析、端口分析、漏洞分析，发现可能存在风险；
- 通过现场核实分析，充分掌握石油石化公司的信息安全管理现状，为后续风险评估赋值及制定改进措施提供依据。

现状调研各环节之间的关联关系如下图所示：

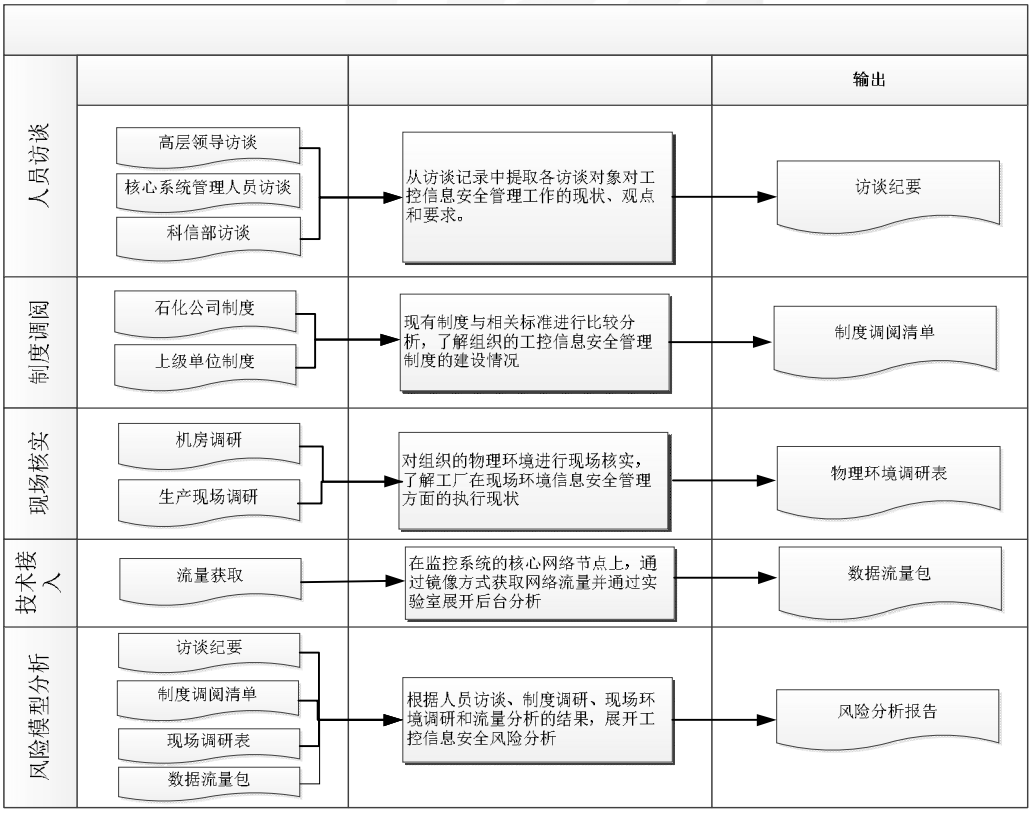

图 37 现状调研关联图

7） 风险评估结果统计及分析

从物理安全、边界防护、集中管控、生产管理层安全管理要求、过程监控层安全要求、现场控制层安全要求、现场设备层安全要求、管理制度、管理机构、

系统建设安全、系统运维安全等方面进行风险评估结果统计及分析。

8） 风险处置

- 针对本次风险评估中发现的风险，参照风险可接受准则对风险进行处理。
- 针对不同风险，主要有三种处理方法：制度修订、管理优化、技术改造。
- 针对风险评估过程中发现的问题，风险评估小组经讨论并给出风险处置措施及建议。

9） 关键组件

本方案利用我公司自主研发工控安全等保检查工具箱开展等保相关工作。

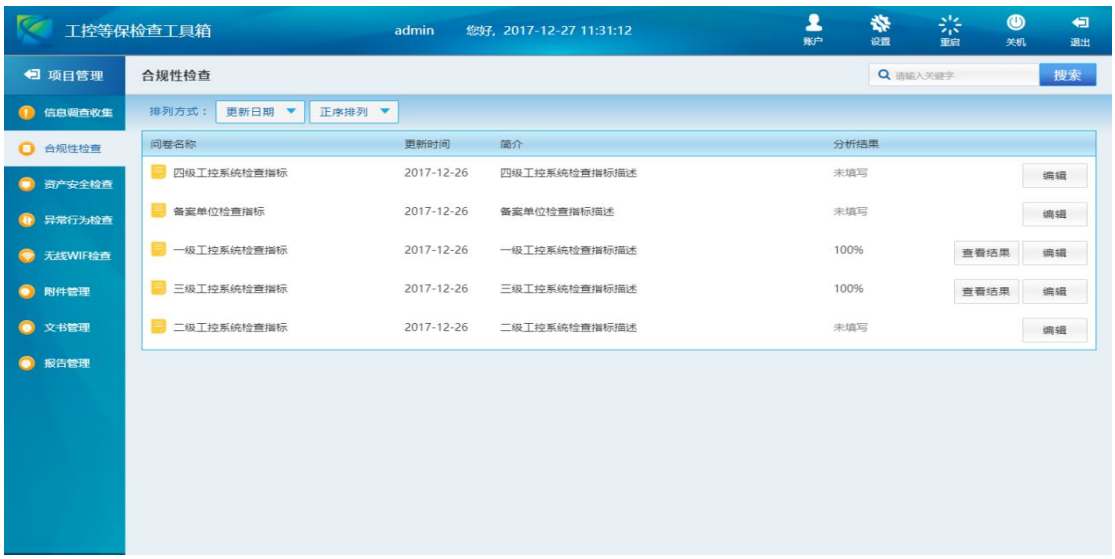

图 38 工控安全的等保检查工具箱

10）核心功能：

- 信息调查收集

检查工具支持收集检查对象的数据，包括被检查单位的基本信息、区域信息、系统基本信息、系统服务信息、系统互联信息和系统数据信息等。

- 合规性检查

基于《信息安全技术 网络安全等级保护基本要求 第 5 部分 工控安全扩展要求》进行设计，产生检查指标，可按照不同安全等级进行合规检查，并支持根据检查结果提出整改建议。

- 资产安全检查

可自动生成网络拓扑，并通过对资产漏洞的统计形成安全评分，最终形成整个区域的资产检查结果。

- 无线评估

无线分析，可对工业现场的无线热点进行探测，发现所有参与无线通信的设备，并对该无线热点进行安全评估，包括无线热点的 SSID 以及对应的 MAC 地址信息、探测隐藏的无线热点、获取无线热点所连接设备的相关信息、无线热点的弱密码评估等。

- 异常行为检查

可对工控病毒进行检查和对典型攻击行为进行检查。

- 附件管理

附件管理支持附件的上传、下载、删除、搜索等。

- 文书管理

包括《信息系统安全等级保护限期整改通知书》、《信息安全等级保护监督检查通知书》、《信息安全等级保护检查情况通知书》、《信息安全等级保护约谈通知书》、《行政处罚决定书》、《停机整顿通知书》、《反馈意见》

- 报告管理

工具基于安全检查的流程进行设计，自动生成报告模板。工具可根据用户的不同需求，可进行模板的自由定制，同时支持多种报告格式的输出保存。

- 评分系统

工具采用国际通用的 CVSS（通用漏洞评分系统）机制，并基于该机制进行拓展，衍生设备检查、区域检查、全网评分等不同评分模型，能够准确全面的对工业控制系统进行风险建模和评分体现。

- 计划管理

工具提供对检查计划进行管理的功能模块。通过该模块，可以快速的帮助用户构建一个完整的工业现场安全检查项目，同时，便于用户对计划进度进行追踪和把控，清晰地掌控整个安全检查流程。

- 日志管理

工具支持日志记录和导出。日志包含登录信息、登出信息、设备重启信息、资产分析操作信息、流量分析操作信息等。支持日志导出格式为 xml 文件。

4. 创新点和应用价值

1）先进性及创新点

- 全流程等保自动化

从计划到文书全流程工控安全等级保护自动检查：基于等保标准的检查粒度，提高检查结果的准确性，确保了检查质量；同时提高人员的等保检查的水平；规范并强化检查的内容、步骤和标准文书，强化风险评估执行流程，降低检查执行难度。

- 工控设备指纹识别能力

通过工控设备指纹对工业控制系统各组成单元进行精准识别，有效降低了等保检查执行的难度。

- 工业控制协议支持

支持多种工业现场级协议，包括 Modbus/TCP、S7、DNP3、Profinet、Ethernet/IP、IEC104、BACnet、Fox、FINS、Melsec-Q 等。

- 无损漏洞探测

工具支持无损式漏洞探测技术，采用非验证式漏洞探测的方式进行漏洞检测，不影响工业现场的正常工艺流程，利用工具检查的效率和结果客观性优点，有效降低等保检查执行的难度。

- 全面的工控信息知识库

工控信息知识库由领先的工控知识库、工控漏洞库、设备指纹库、工控设备库、威胁特征库和工控协议库构成。

- 检查结果的多维度数据分析

等保检查工具箱可对已完成检查的工业企业的采集数据进行多角度、多维度数据分析，并能提供对比分析，进而为等保工作的推进落实提供指导和数据支撑。

2）实施效果

利用长扬科技自主研发的工控安全等保工具箱，本方案评估模型可广泛适用于测评机构或行业单位对智能制造、冶金、电力/电网、轨道交通、石油石化、教育等多种工业场景评测。本解决方案可以实现对以上多种工业场景方便、快捷、专业、标准化与自适应相结合的等保工控服务。

5. 案例提供方

长扬科技（北京）有限公司

三、 结束语

工业互联网的出现模糊了传统的网络边界，而网络世界的复杂与多变性也给工业互联网带来了诸多安全挑战，如 APT 攻击和新型病毒高发、生产设备暴露面扩大、设备漏洞多、安全防护措施不到位等，工业互联网安全形势较为严峻。

案例汇编 v2.0 汇聚了工业互联网安全企业内关于威胁监测与分析、紧急安全事件应急处理、数据安全保护、端到端工控安全加固与防御、安全组网、等级保护服务解决方案等的最佳实践，以期从实践操作层面为工业企业提供安全建设参考，提升安全技术水平，协同产业链共同打造安全的工业互联网。

安全是动态的，尽管案例汇编 v1.0 和 v2.0 提供了有效的安全解决方案，未来随着工业互联网技术演进和网络攻击的升级，安全解决方案也需不断更新优化，才可为工业企业生产提供有力保障。

附录：案例提供方简介

• 360 企业安全技术（北京）集团有限公司

360 企业安全技术（北京）集团有限公司是 360 公司继个人安全市场后专注于为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务的网络安全公司，法定代表人为齐向东，注册资本 1.33 亿人民币，总部设立在北京市朝阳区酒仙桥路 6 号院 2 号楼（电子城.国际电子总部），同时公司在上海、成都、广州、大连等地设有分支机构。公司拥有 4000 余名网络安全技术、产品和服务人员。截止目前已经为 90%部委、72%央企、100%大型银行以及上百万中小企业提供了网络安全产品和服务。

360 企业安全集团基于自身在大数据、威胁情报、防病毒、安全攻防、态势感知等方面的突出优势，创新性的提出了“数据驱动工业安全”的技术发展理念，构建了层次清晰、定位明确、融合联动的工业信息安全产品体系。工业信息安全产品从低到高分为三类：防护监测类产品、安全运营类产品、态势感知类产品。数据从低到高流动，威胁情报从高到低赋能。

360 企业安全集团高度重视工业安全，专门成立了工业安全产品和服务部门，投入大量资源进行相关技术、产品和解决方案的研发，为工业用户和相关主管部门提供全方位的信息安全服务，并在政府监管、电力、石油石化、轨道交通、智能制造等领域成功应用。360 企业安全集团愿与各方一起努力，让国家关键信息基础设施运行得更安全、更可靠，360 工业信息安全为用户安全生产保驾护航。

• 中国移动政企分公司

中国移动通信集团公司政企客户分公司（简称政企分公司），前身为中国移动总部集团客户部，成立于 2012 年 8 月，是中国移动通信集团公司下属经营集团客户市场的专业化分公司。

集团客户市场是当今全球信息通信行业发展的重要蓝海。截至 2014 年 1 月，中国移动集团客户数已超过 320 万家，覆盖了全国逾 40%的法人和产业活动单位，集团成员达 2.3 亿户，集团客户的整体收入已超过中国移动整体收入的 40%。开展集团客户市场的专业化运营，已经成为推动我国信息化事业持续健康发展的必

然趋势。

按照中国移动的整体战略部署，政企分公司主要提供面向政府、大型企业等重要集团客户的销售和端到端服务；负责面向全国的集团客户产品整合和产品推广；统筹各方资源，组织协调跨省跨国业务的支撑和调度。

政企分公司将依托于中国移动在网络、客户、渠道、业务和产业链等方面的整体优势，紧密围绕“移动改变生活”的发展愿景，持续地提升面向各行各业的信息服务份额，做质量更好、服务更优、创新更强、价值更高、管理更有效的运营商和现代服务企业。

• 北京威努特技术有限公司

威努特公司是国内专注于工控安全领域的高新技术企业，以研发工控安全产品为基础，打造多行业解决方案，提供培训、咨询、评估、建设及运维等全流程安全服务。威努特率先提出工业网络“白环境”理念，迄今已服务电力、轨道交通、石油、石化、市政、烟草、化工及军工等行业的三百余家客户，受邀保障 G20 峰会和“一带一路”国际合作高峰论坛。威努特致力于为客户构建安全可靠的工业网络环境，保障国家关键信息基础设施运行安全，为中国制造 2025 护航，为建设网络强国添砖加瓦！

威努特在国内率先提出工业网络安全“白环境”为核心的整体解决方案，自主研发了满足工控安全行业需求及政策法规标准的 4 类 14 款产品，覆盖企业、科研、监管机构等用户。

目前人员规模约 200 人，主要来自于国内外知名信息安全厂商和自动化厂商。其中超过 95%本科及以上学历，多数毕业于 985、211 等一类本科院校，平均从业年龄超过 10 年。技术团队有超过 60%的信息安全和自动化专家，曾供职于国内外顶级安全和自动化公司。研发人员占比超过 1/3，在信息安全、工业控制、大数据等领域经验丰富。公司在全国已设立北京、上海、西安、成都、广州五大技术服务中心，有力的保障了客户现场的工控系统持续稳定运行，同时已拥有 7*24 小时电话服务和 24 小时内抵达客户现场服务的能力。

威努特自成立伊始，对研发技术高投入和对客户服务质量高标准就作为公司运营的核心理念之一，对研发投入的金额由 2014 年的 100 万到 2017 年的 2000

万，保持逐年递增，且每年占据营业收入的30%以上。

截至2018年4月，已取得软件著作权三十多项，申报国内专利近二十项，并获得了开展工业信息安全工作的相关资质，具体资质如下：

- 国家高新技术企业
- 信息安全管理体系认证证书
- 国家信息安全漏洞库（cnnvd）技术支撑单位（二级）
- 国家网络与信息安全信息通报机制技术支持单位
- 信息安全等级保护安全建设服务机构能力评估
- ISCCC信息安全服务资质认证证书（安全集成服务资质）
- ISCCC信息安全服务资质认证证书（风险评估服务资质）

• 中国电子信息产业集团有限公司第六研究所

中国电子信息产业集团有限公司第六研究所（以下简称电子六所）成立于1965年，直属中国电子信息产业集团有限公司（CEC），是我国最早从事电子技术应用系统研究、开发的重点科研院所之一，设有工业控制系统信息安全技术国家工程试验室，致力于打造工控系统及安全领域国内领先企业,获得中国合格评定国家认可委员会实验室认可（CNAS）、国家认证认可监督管理委员会实验室资质认定（CMA）、国防科技工业实验室认可（DiLAC）、国家信息安全等级保护工作协调小组办公室推荐测评机构、信息安全服务资质证书（安全工程类一级）、ISCCC信息安全风险评估二级服务资质、阿基里斯认证资质等资质证书以及人社部认定的工控信息安全人才培训项目全国唯一运营单位。承担近百余项国家、军队网络安全重要科研项目，并顺利完成了多项国家重大会议网络安全保卫任务，其中包括中国杭州G20峰会、全国两会、“一带一路”高峰论坛、金砖峰会以及十九大等网络安保工作。

• 深圳市腾讯计算机系统有限公司

腾讯云基于QQ、微信、腾讯游戏等海量业务的技术锤炼，从基础架构到精细化运营，从平台实力到生态能力建设，腾讯云将之整合并面向市场，使之能够为

企业和创业者提供集云计算、云数据、云运营于一体的云端服务体验。目前腾讯云产品服务超过 180 个，开发者超过 200 万个，2017 年收入同比增长 100%，同年发布腾讯工业云平台。2018 年 4 月，成功防御国内最大流量 DDoS 攻击；工业互联网智能超算中心落户重庆。腾讯云发布的超级大脑，助力传统企业数字化转型升级，超级大脑基于腾讯 20 年的技术积累和腾讯云在行业数字化转型中的实践经验而构建，其中也融入了对数字世界建设全面而长期的技术构想，腾讯云希望以腾讯过去 20 年的能力为基础，联合合作伙伴的优势禀赋，帮助更多传统企业数字化转型升级，以我所能，为你而+。腾讯云一路走来，共获取了 40 多项专项认证，是国内认证最完备的云平台之一。主要包括 ISO22301、CSA STAR 认证、ISO27001 认证、ISO20000 认证、CDN 资质说明、ISO9001 认证、可信云服务认证、大数据产品能力认证、网络安全等级保护、PCI DSS 认证、SOC 审计、ITSS 认证 ISO27018 认证、CISPE 数据保护行为准则认证等权威机构的认证和认可。

- **华为公司**

华为是全球领先的 ICT（信息与通信技术）基础设施和智能终端提供商，致力于把数字世界带入每个人、每个家庭、每个组织，构建万物互联的智能世界。华为同时也是一个主流网络安全厂商，2015 年, 160,568 台华为安全产品服务于 130 国家的 1000 多个客户 ，行业客户包括：运营商、政府、金融、医疗、互联网、传统大企业，是世界上第 5 大安全设备厂商。华为拥有近 2000 人的安全专业研究队伍，取得 1000 件以上的网络安全专利，拥有深圳、北京和杭州三个攻防实验室，2016 年 12 月举行的贵阳市大数据安全攻防演练活动中，华为安全团队攻破多个目标，获评本次安全赛事含金量最高的“安全丰收奖”。本方案是华为安全团队基于客户的生产基地实际情况，部署的安全解决方案。

- **江苏敏捷科技股份有限公司**

敏捷科技由全球主动信息防护技术原创团队创办，是国内首家原创数据加密软件厂商，从 2002 年率先推出填补国内空白的自主知识产权数据加密产品，到全国首发第一套央企商业秘密保护解决方案，再到数据安全卫士系统 DGS 这一整

体数据安全与管理解决方案，再到工业数据安全解决方案，敏捷产品始终引领数据安全新趋势。产品融合集成 2000+信息系统，在智能制造、能源、冶金水电、化工、设计、交通、政府、军工、文教卫、汽车电子、轻工纺织、生物医药等 500+关键领域得到广泛应用，累计客户量过万，每天超 1000 万+人使用该产品保护数据，包括中国中车、中国一汽、中国冶金、中煤、中国化学、国家电网、中国石油等国资央企及关键基础设施用户。

敏捷科技是工业信息安全产业发展联盟会员单位、中国网络空间安全协会理事单位、中国网络安产业联盟理事单位、中国两化融合服务联盟会员单位、中国工业互联网联盟会员单位、江苏省信息安全产业联盟秘书长单位、工业强省六大行动重点项目单位，先后获得中国网络安全和信息产业年度领军企业、中国软件和信息服务业最具创新力企业、中国信息安全最具影响力企业、中国智能制造优秀解决方案服务商、中国智能制造优秀解决方案、咨询创新奖等资质和荣誉。

• 长扬科技（北京）有限公司

长扬科技（北京）有限公司是一家专注于工业物联网安全、态势感知和安全大数据应用的创新型高新技术企业，总部位于北京，已经在上海、广州、杭州等 12 地设置分支机构和服务中心，目前已完成融资额近亿元。

公司产品聚焦工业网络安全及安全大数据领域，已推出七大自主研发产品线，通过标准化产品和行业定制化开发相结合的模式，为客户持续提供覆盖工控系统整个生命周期的网络安全产品、解决方案和安全服务。既有企业侧的防护、监测类设备，也有基于人工智能和大数据分析技术的工业互联网安全态势感知平台、安全大数据平台。产品支持多种工控协议，拥有全面的工控信息知识库支撑，具备丰富的工控漏洞库、设备指纹库、工控设备库、威胁特征库、工控协议库及多种漏洞检测挖掘手段，信息覆盖 80%厂商设备。

公司已获知识产权 20 余项，并已通过 ISO9001 质量管理体系、IEC27001 信息安全管理体系、IEC20000 信息技术服务管理、ISO14001 环境管理体系认证，拥有信息安全风险评估服务资质、信息系统安全集成服务资质、信息系统安全运维服务资质、信息安全应急处理服务资质等。

• 常州万联网络数据信息安全股份有限公司

常州万联网络数据信息安全股份有限公司（CHANGZHOU MACROUNION NETWORK & IT SECURITY CO., LTD.）2003 年在中国江苏常州设立，为股份制有限公司。2015 年 12 月 25 日成功挂牌新三板，证券代码：835111，证券名称：万联网络。

万联网络是国内较早面向工业互联网核心软件技术和可信云平台架构的创新研发公司，提供成熟的全网 IP 云架构下边缘计算软件技术和物联网云安全架构技术，以及数字化智慧运维管理技术的高科技股份制企业。万联以自主物联网智件软件技术和云网融合路由技术为核心，大力推进面向行业工业互联网+应用的上云工程服务和数字化平台的研究，促进产业互联网和企业数字化转型的信息融合，特别提供基于企业上云，敏捷交付的智慧应用建设。公司的长期发展战略是以多层次工业互联网软件技术为核心全方位的满足客户需求，即将公司多年积累的核心技术应用助推更广泛的行业互联网化的数字化转型中，成为企业上云，优化成本，数字化经营，产能结构调整的有力技术保障。

万联网络公司通过德国 TUV 机构的严格审核获得了 ISO9001：2008 质量体系认证；获得了 ISO/IEC 20000-1:2011 信息技术服务管理体系认证；获得 IEC/ISO27001：2013 信息安全管理体系认证；获得江苏省软件企业；认定为国家高新技术企业；获得江苏省科技型中小企业的认定；2014 年度常州市十佳软件企业；江苏省信息安全产业联盟成员单位；江苏省软件协会成员单位；中国电信云网商成员单位；国家工业互联网产业联盟 AII 成员单位等；在物联网技术领域拥有多达六十几项的国家发明专利及软件著作权；是中央政府采购、IBM、HP、华能集团、大唐集团、上海大众、中石化石油管理局、中科曙光、太原卫星发射基地等信息化协议供应商及服务承包商。