工业互联网
典型安全解决方案案例汇编

V3.0

工业互联网产业联盟（AII）

2020 年 8 月

工业互联网产业联盟

Alliance of Industrial Internet

目　　录

前　言

工业互联网作为新一代信息技术与制造业深度融合的产物，通过对人、机、物的全面互联，构建起全要素、全产业链、全价值链全面连接的新型生产制造和服务体系，是数字化转型的实现途径，是实现新旧动能转换的关键力量。2019 年全国两会报告指出“加强人工智能、工业互联网、物联网等新型基础设施建设和融合应用”，工业互联网作为“新基建”的七大领域之一，其重要性上升到一个新的高度。工业互联网的投资和建设将加快我国智能制造步伐，激发新型消费和投资、促进就业创业、解放生产力、打造经济发展新动能，对人们生产生活带来重大而深远的影响。

工业和信息化部在 2019 年 1 月发布了《工业互联网网络建设及推广指南》，提出加快培育网络新技术、新产品、新模式、新业态，支撑制造强国和网络强国建设。工业和信息化部在 2020 年 3 月发布了《工业和信息化部办公厅关于推动工业互联网加快发展的通知》，提出了加快工业互联网发展“二十条”。2019 年 7 月，工业和信息化部、教育部、人力资源和社会保障部、国家卫生健康委员会等十部委联合发布了《加强工业互联网安全工作的指导意见》，制定了 2020 年和 2025 年两阶段发展目标，并提出了 7 大任务、17 项重点工作及 4 项重点保障举措，为开展工业互联网安全工作提供切实可行指引。

目前，工业互联网安全仍然面临很多新挑战和问题亟待解决。一方面，5G、边缘计算、大数据、人工智能等新技术与工业互联网技术

的融合为工业互联网安全带来新的挑战，暴露面持续增大，安全场景更加复杂；另一方面，工业互联网一直存在的网络攻击、漏洞隐患等共性问题依旧突出。工业互联网安全建设任重而道远。

为使广大工业互联网从业者能了解工业互联网安全的发展情况，工业互联网产业联盟安全组启动编写了《工业互联网典型安全解决方案案例汇编（2019）》，报告汇编了业内优秀的安全解决方案，希望为解决工业互联网安全的新挑战和突出问题提供有益参考，共同促进工业互联网安全工作的建设。

本报告是在工业和信息化部网络安全管理局指导和支持下，由中国移动通信集团有限公司牵头编制，工业互联网产业联盟安全组多家企业参加编写完成。主要参与单位有：中国信息通信研究院、奇安信科技集团股份有限公司、中国电子信息产业集团第六研究所、北京威努特技术有限公司、东软集团、北京微智信业科技有限公司、江苏亨通工控安全研究院有限公司、长扬科技（北京）有限公司、新华三技术有限公司、启明星辰信息技术集团股份有限公司、北京双湃智安科技有限公司、北京神州绿盟信息安全科技股份有限公司。

本报告的参编人：张峰、田慧蓉、陶耀东、李江力、徐一、刘晓曼、于乐、付俊、马洁、崔婷婷、郭念文、崔君荣、王晓鹏、谷久宏、申枭、胡鸥、杨继、刘健帅、张森、马驰、李鸿彬。

工业互联网产业联盟 安全组

二〇二〇年三月

1. 工业互联网安全概述

1.1 工业互联网安全形势

2019 年全国两会报告指出“加强人工智能、工业互联网、物联网等新型基础设施建设和融合应用”，工业互联网作为“新基建”的七大领域之一，其重要性上升到一个新的高度。工业互联网的投资和建设将加快我国智能制造步伐，激发新型消费和投资、促进就业创业、解放生产力、打造经济发展新动能，对人们生产生活带来重大而深远的影响。据中国信息通信研究院预计，2020 年中国工业互联网产业经济增加值规模约 3.1 万亿元，占 GDP 比重为 2.9%，对经济增长的贡献率超过 11%，并带动全社会新增就业岗位 255 万个。

《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》将安全保障与网络、平台建设并列为工业互联网三大体系之一。各上级单位高度重视工业互联网安全，并相继发布了一系列工业互联网安全方面的指导意见和要求，涵盖安全管理、安全标准、安全评估、试点示范、考核指标等领域。

2019 年 7 月，工信部等十部门印发的《工业互联网安全工作的指导意见》中，指导企业建立监督检查、信息共享和通报、应急处置等工业互联网安全管理制度，构建企业安全主体责任制，探索构建工业互联网安全评估体系；指出要至少形成 20 个创新实用的安全产品、解决方案的试点示范，培育若干具有核心竞争力的工业互联网安全企业。预计到 2025 年基本建立起较为完备可靠的工业互联网安全保障体系。2019 年 9 月，工业和信息化部发布《省级工业互联网安全监测与态势感知平台建设指南》，指导各地工业和信息化主管部门、地方通信管理局建设专业化安全监测和预警通报技术手段。国资委印发的《中央企业负责人经营业绩考核办法》中，将网络安全纳入了中央企业负责人的考核指标。2020 年 3 月，工信部发布了《工业和信息化部办公厅关于推动工业互联网加快发展的通知》，明确提出加快新型基础设施建设、加快拓展融合创新应用、加快健全安全保障体系、加快壮大创新发展动能、加快完善产业生态布局、加大政策支持力度等 6 个方面 20 项具体举措。

同时，工业互联网安全相关的法律和标准也在同步推进，为行业和企业的安全建设提供参考。2019 年 1 月，工信部、国标委两部委联合印发了《工业互联网

综合标准化体系建设指南》，明确了网络、平台、安全、应用相关建设内容。其中安全标准包括“设备安全”、“控制系统安全”、“网络安全”、“数据安全”、“平台安全”、“应用程序安全”、“安全管理”。2019 年《中华人民共和国密码法》正式通过，规范密码应用和管理，保障网络与信息安全。等保 2.0 国家标准中新增了工业控制系统安全的扩展要求，涵盖了物理和环境安全、网络和通信安全、设备和计算安全、安全建设管理、安全运维管理等方面的要求，对提升工业互联网安全保护能力具有重要意义。为推动工业互联网安全责任落实，工业和信息化部针对工业互联网企业网络安全实施分类分级管理，研究起草了《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿），可提升工业互联网安全保障能力和水平。水利和电力等重点行业也相继出台了安全管理办法和实施指南。

在工业互联网安全试点应用方面，工信部办公厅发布《关于开展 2019 年工业互联网试点示范项目推荐工作的通知》，共公布了 81 个工业互联网试点示范项目，其中共有 17 个工业互联网安全试点示范项目，覆盖安全测试、态势感知、集中管控、平台安全防护、安全认证、数据安全等多个安全细分领域，这些试点示范项目将不断深入推动工业互联网安全的落地建设工作。

1.2 工业互联网安全挑战

工业互联网安全工作在深入推进的过程中，面临一系列新兴和固有的安全问题亟待解决。

（1） 新技术融合带来新风险

工业互联网技术与 5G、边缘计算等新技术的融合以及第三方协作服务的深度介入增加了信息泄露、数据窃取的风险。5G 协议的全面互联网化，被外部攻击的可能性显著性增加。边缘计算对工业互联网数据就近处理减少了敏感数据泄露的风险，安全防护能力不及云中心，且对原有的集中式内容监管模式带来挑战。

（2） 暴露面持续增大

随着 5G+工业互联网、工业上云等工作的推进，网络日益开放，大量工业互联网设备暴露在互联网上且不断增多。暴露在互联网的工业互联网设备长期遭受恶意嗅探，仅 2019 年上半年上半年嗅探事件达 5151 万起。

（3） 漏洞病毒依旧突出

由于工业互联网设备软件更新缓慢、用户及厂商通常无法及时发现或修复漏洞，导致设备漏洞较多。根据 CNCERT 对电力设备的安全摸底测试，70 余个型号的产品中均发现了中高危漏洞。

同时，设备漏洞易被攻击者利用来构建完整攻击链路，并获取更高权限，甚至制造病毒长期危害工业互联网安全。近几年全球水电、核电、制造等重要行业的企业遭受病毒攻击和感染的事件众多，造成了大范围停电、生产线停摆等重大影响。

（4） 重点行业监控和管理系统存高危隐患

重点行业如能源、金融、物流、智能制造等，其大型工业云平台和系统持续遭受漏洞利用、拒绝服务、暴力破解等网络攻击。仅水电行业和医疗健康行业，暴露在互联网上的系统中存在高危漏洞隐患的占比分别为 25%和 72%，部分遭受境外恶意嗅探。

2. 典型安全解决方案

2.1 案例一：工业互联网边缘计算敏感数据安全防护解决方案

2.1.1 方案概述

随着 5G、物联网时代的到来以及云计算应用的逐渐增加，传统的云计算技术已经无法满足终端侧“大连接、低时延、大带宽”的需求，工业互联网相关边缘设备连接数量和产生的数据呈海量增长趋势，边缘计算应运而生。传统的云计算模型采用集中处理方式，将所有数据通过网络传输到云计算中心，利用云计算中心强大的计算能力集中式地解决计算和存储问题。在工业互联网“大连接、低时延、大带宽”对数据高效处理低延迟对背景下，云计算中心负载、传输带宽和数据安全等云计算局限性问题越来越突出，各种接入设备感知产生的海量数据使云计算的网络带宽变得更加有限，让云端不堪重负，造成更大的数据瓶颈。因此，边缘计算模型应运而生，并成为近几年的技术发展热点。

边缘计算是在网络边缘执行计算的一种新型计算模型，边缘计算的边缘是指从数据源到云计算中心之间的任意计算资源和网络资源。边缘计算面向的对象包括来自物联网的上行数据和来自云服务的下行数据。边缘计算允许终端设备将存储和计算的任务迁移到网络边缘节点中，既可满足终端设备的计算能力扩展需求，又能有效地节约计算任务在终端设备与云服务器之间的传输链路资源。可见未来边缘计算对应用场景和覆盖程度将非常广泛。

在工业互联网领域，边缘计算是在靠近物或数据源头的网络边缘侧，构建融合网络、计算、存储、应用核心能力的分布式开放体系，通过边缘计算能够“就近”提供边缘智能服务，满足工业在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。

边缘计算具有数据处理实时性、数据多源异构性、终端资源受限性和接入设备复杂性，使得传统云计算环境的安全机制不再适用于边缘设备产生的海量数据的安全防护，边缘计算的数据存储安全、共享安全、计算安全、传输和敏感数据保护等问题成为边缘计算模型必须面对的挑战性问题。因此，只有有效

的解决边缘计算的各种安全问题，才能促进边缘计算技术在各个领域健康快速的发展。

面向未来复杂网络环境下的边缘计算的敏感数据保护需求，主要包括边缘节点互联问题、边缘资源调度问题和边缘网络安全问题等现存问题，上述问题目前虽然各种问题都有一些解决方案，但还不能从根本上解决问题，边缘计算应用亟需数据安全保护方案。

2.1.2 典型安全问题

工业互联网应用场景相对孤立，不同行业的数字化和智能化水平不同，对边缘计算的需求也存在较大差别。以机械制造行业为例对行业需求进行分析。

机械制造业在国家行业中处于基础性地位，同时也是一个国家的支柱型行业。通过企业现场调研，查阅资料、文献等方式对机械制造行业边缘计算现状和需求进行分析，机械制造行业整体基础设施建设水平不一，建设质量参差不齐，普遍面临如下问题：

（1） 数据开放性差且工业协议标准不统一

目前在机械制造行业领域，设备基本具有数据接口，但设备和系统的数据开放性不够，缺乏数据开放接口及文档说明。存在 RS232、RJ45、Profibus、MTConnect、MODBUS/TCP、Profinet 等多种工业协议标准，各个自动化设备生产及集成商还会自己开发各种私有的工业协议，各种协议标准不统一、互不兼容，导致协议适配、协议解析和数据互联互通困难。

（2） 数据采集种类有限

机械制造行业车间内的设备多数已有数据采集功能，但是采集的种类有限，如数控机床多数能采集电压、电流等信号，但是振动信号等多需要外置传感器的方式进行采集，部分机床还没有部署此功能。

（3） 工业数据采集实时性要求难以保证

生产线的高速运转，精密生产和运动控制等场景则对数据采集的实时性要求不断提高，传统数据采集技术对于高精度、低时延的工业场景难以保证重要的信息实时采集和上传，无法满足生产过程的实时监控需求。

（4） 全车间统一网络尚未实现

机械制造行业基础设施建设水平不一，车间内设备联网水平也参差不齐。部分设备已经实现联网，但尚未形成全车间统一网络。

（5） 工业数据采集存在数据安全隐患

工业数据采集会涉及到大量重要工业数据和用户隐私信息，在传输和存储时都会存在一定的数据安全隐患，也存在黑客窃取数据、攻击企业生产系统的风险，急需边缘计算的敏感数据防护措施。

2.1.3 安全解决方案

北京微智信业科技有限公司设计开发的边缘计算敏感数据安全防护系统主要由安全导向的网络通信平台（Security-Oriented Cyber Communication Platform，SOC2Plat）服务器、核心/边缘网关、终端软件、安全协议套件组成。

SOC2Plat 能够以服务组件形式加载并工作于云虚拟主机或服务器、网关硬件设备之上；核心/边缘网关以系统固件形式自动加载并运行于网关硬件设备之上，其核心组件为具有自主知识产权的安全通信协议套件；终端软件以客户端形式工作于常用操作系统平台之上，如 Windows、MacOS、Android、iOS 平台，需要用户主动、按需启动接入 SOC2Plat 平台。边缘计算敏感数据安全防护系统整体架构图所示：

图 1 边缘计算敏感数据安全防护系统整体架构

1. SOCPlat 服务器平台

SOCPlat 服务器平台主要功能：安全协议组件管理、安全态势管理、安全认证管理、安全服务编排管理、边缘计算设备管理、拓扑管理、安全资源调度管理、跨域安全策略管理、敏感数据知识库管理、恶意攻击知识库管理、安全预警管理。

边缘计算设备管理对外提供边缘网络设备、接入终端设备、接入终端用户、基础网络拓扑、覆盖网络链路、多域网络服务等网络与服务的综合管理和集中控制。拓扑管理模块支持 OSPF、BGP、ISIS 等协议的数据平面主机和路由发现。

2. 核心/边缘网关

由控制器代理、边缘计算模块、边缘感知模块、攻击感知模块、攻击预警模块、日志记录模块六部分组成。控制器代理与控制器创建 OpenFlow 协议控制通道，接收并反馈网关设备的状态信息。边缘计算模块进行网络接口和网络状态的实时感知，并进行网络协议识别、分类和统计。边缘感知模块负责主动发现边缘终端，并对边缘终端信息进行收集与管理。攻击感知模块通过相关攻击特征库发现攻击事件。攻击预警模块根据攻击感知情况，发出相关攻击事件预警。日志记录模块做相关审计。

3. 终端软件

由控制器代理、敏感数据识别、敏感数据检测、跨域交换、恶意攻击检测、恶意攻击防护六部分组成。控制器代理功能与网关的控制器代理功能相同，故不再赘述。敏感数据识别模块通过敏感数据特征库，发现终端上的敏感数据。敏感数据检测模块对终端上的敏感数据存储位置、相关操作和流向进行监测与追踪。恶意攻击检测模块检测针对终端的攻击，恶意攻击防护模块可以防护针对终端的网络攻击，跨域交换模块通过对终端系统进行实时、准确的监测与调控，确保跨域数据交换的安全性。

4. 安全协议套件

安全协议套件支持自主知识产权的网络安全通信协议，建立设备与设备、设备与平台间的安全互联隧道，设备间的设备身份认证、认证密钥交换、用户身份认证、认证加密传输、心跳包活机制等安全协议阶段。

2.1.3.1 技术路线

本技术路线围绕跨域安全互联互通技术、边缘网络边界控制技术、边缘安全资源调度技术和边缘敏感数据保护技术四个方面详细展开。这些关键技术融合在SOCPlat 服务器平台、边缘网关、终端软件和安全协议套件中实现。

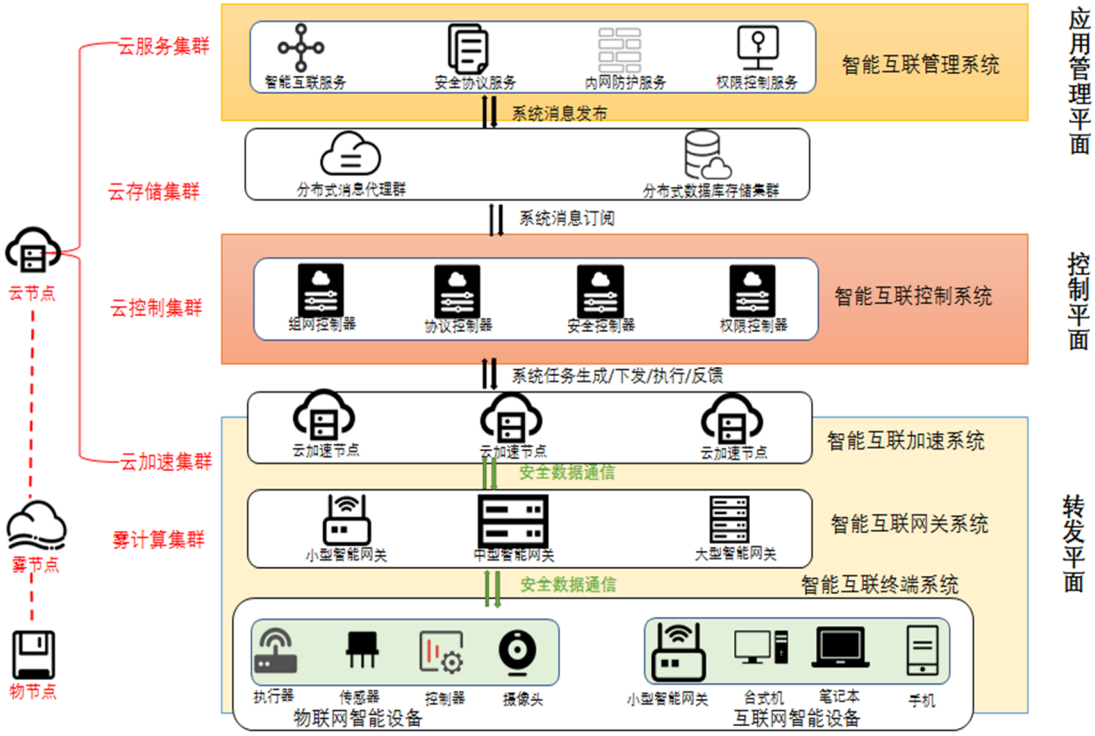


图 2 技术路线图

2.1.3.2 技术创新性和难点分析

传统的频繁项挖掘算法有 Apriori 算法和 fp-growth 算法。Apriori 算法是一个传统的数据挖掘中频繁项提取算法，由于其每次生成候选项集均需要完整遍历整个数据集，因此其大规模数据量的频繁项挖掘效率往往不高。fp-growth 算法是基于 fp-tree 前缀树的频繁项挖掘算法，fp-growth 算法通过对 fp-tree 前缀树的剪枝优化，解决 Apriori 算法的低效率问题。因此基于 fp-growth 算法，提供其并行化效率，对数据流特征进行快速频繁项挖掘。

数据通常的动态管控包含配置管理技术、规则匹配引擎技术、阻断技术。从经典的前缀扫描 AC 算法出发，根据它占用内存过大的缺点，设计了基于 AVL

树的 ACVL 高效匹配算法。同时，根据千万模式集合的特征，设计了融合改进的 DAT 算法和 WM 算法的 CDWH 算法来实现千万模式规则的匹配。在尽量保持原有匹配速度的基础上，实现了千万模式集合的匹配。

将实时安全事件(Alert)利用攻击关联度进行聚类，得到不同攻击场景的报警集合。对每一个攻击场景的报警信息与生成的攻击模式库进行关联分析，研究高效的攻击步骤关联是本项目的重点，特备是攻击关键点的准确、高效识别是进行攻击拦截的重要参考技术。

2.1.3.4 技术先进性与可行性

- **技术特点**

先进性主要体现在三个维度：管理维度上支持软件定义，服务维度上支持用户定制，安全维度上完全自主可控。

第一，采用广义的软件定义技术，改造边缘网络节点的网络架构、管理方法、配置方式、通信模式，改善边缘网络之间的安全资源共享—即通过网络虚拟化技术、软件定义安全、软件定义边界技术实现跨域安全资源的集中管理和统一调度。

第二，在传统 SDN 的管理平面和控制平面之间增加调度平面，即采用 MANO 技术、SFC 技术和 SLC 技术分别对涉及业务部分的资源、功能、生命周期进行抽象、建模、设计、编排，实现边缘网络资源的集中式、可视化、一致性管理和调度。

第三，采用自主研发、具有自主知识产权的安全通信协议套件，实现满足多元业务的可靠控制协议和安全数据协议，保障用于工业多元业务的低时延、高可靠、易扩展的安全通信。

- **先进性与可行性**

从管理维度、服务维度和安全维度分别对边缘网络的身份认证问题、计算能力问题和数据隐私问题三大核心问题给出创新性的解决方案，即采用软件定义技术提高跨域网络一体化资源（设备、系统、网络、应用、服务、安全等资源）可管理性和可维护性，采用微服务、插件化、服务链的关键技术和设计理念使得跨域网络的需求可定义、服务可定制、流程可配置，采用自主可控的安全通信协议套件、软件定义的安全防护技术和软件定义的边界控制技术保证边缘网络之间的

通信安全、内容安全和数据安全。

经过两年多对边缘计算、软件定义网络、边缘计算敏感数据保护等核心技术的调研、研发、试用，已经搭建了工业网络互联服务与管理平台已基本建成并运营良好，在威海本地企业进行了开局试用，提高了企业的信息化和智能化水平，建立了企业的网络安全保障体系。目前平台已经进入维护、推广和优化阶段。随着平台的推广，本平台必然会降低企业运营成本，缩短产品生产周期，提高产品生产效率，降低产品不良率，提高企业能源利用率，在企业新旧动能转换的过程中发挥积极作用。

本项目实施具备 SOC2Plat 服务器、核心/边缘网关、终端软件等上线产品，丰富储备边缘计算敏感数据保护安全体系的理论基础和关键技术，下一步重点突破归一化管理方法、工业级通信协议、智能化控制模型和插件式平台服务四项关键技术，对已有软硬件、管理平台进一步集成、调试、优化、完善，提供自主可控、安全可靠的边缘网络智能互联、安全防护、动态调度和综合管理的边缘计算敏感数据保护解决方案。

2.1.3.5 功能、性能指标

- **硬件指标**

核心/边缘网关硬件指标如下：

表 1 指标列表

序号	硬件指标	指标范围
1	外观	2U 高度，机架式安装并配置安装导轨
2	主板	Intel C612 高性能芯片组
3	处理器	Intel E5-2600V4 系列处理器*2
4	内存	64G 内存
5	硬盘	2T*2 硬盘
6	网卡	4 个万兆网卡，2 个千兆网卡
7	电源	1400W 服务器（1＋1）冗余电源。
8	功耗	额定功耗 500W，实际功耗 300W。
9	处理能力	单机最高 DPI 处理能力达 10G

➢ **功能指标**

1.支持用户和边缘计算设备端到端双向认证机制，以及边缘计算设备对接入用户的群组认证、跨域认证等。

2.可抵御终端侧非授权侵入、流量拦截攻击、敏感信息窃取等数据安全威胁。

3.适用于多类网络边缘侧终端设备的应用运行场景。

➢ **性能指标**

1. 终端设备的平均接入认证时间不超过 3 秒。

2.1.4 小结

本产品主要价值体现在三个方面：

首先，在面向工业级、具有自主知识产权的安全通信协议套件方面，提供安全通信协议软件 SDK，具备支持设备身份认证、用户统一认证、认证加密传输、密钥主动更新、心跳保活机制等安全通信能力，支持 C、PYTHON、JAVA 等主流开发语言，并提供国密加解密及认证接口。

其次，在核心/边缘网关设备的装置设计方面，支持丰富的终端设备接入方式，如 Wi-Fi 接入、网口、串口、并口等；支持常见的工业控制协议解析，如 MODBUS、DNP3、S7、OPC 等；且系统内置国密安全芯片及信息安全算法，如 SM1、SM2、SM3、SM4、DES、AES 等。

再次，在 SOC2Plat 服务器的平台设计方面，支持工业级的机理模型、微服务，支持面向需求定义和流程定制的插件式、可扩展的平台，支持用户和边缘计算设备端到端双向认证、个体认证、群体认证、跨域认证等多种认证方式的按需定义，实现安全功能的轻量化资源需求，能够抵御终端非授权侵入、流量拦截攻击和敏感数据窃取等数据安全威胁。

2.1.5 单位基本信息

北京微智信业科技有限公司成立于 2003 年，注册资金 5 亿元，2016 年被北京东方通科技股份有限公司（股票代码 300379）收购为全资子公司，属国家高新技术企业和双软企业。

公司专注于信息安全、网络安全、通信业务安全三大业务方向产品的研发、生产、销售和服务。公司以自主研发技术为核心，致力于大数据采集、大数据分析及处理、文字识别、图像识别、视频识别、语音识别、信息检索与过滤技术、多媒体过滤技术、网络业务质量分析等研究，是国际标准化组织 ISO/IEC MPEG 成员，技术水平始终保持国际领先水平。

微智信业凭借强大的研发能力，为用户提供网络安全、信息安全、通信业务安全三大产品，并通过三条产品线，结合十六年的行业经验，为用户提供高质量的安全服务。公司产品在三大电信运营商、政府、海外等客户得到广泛应用，产品运行稳定，性能指标优异，拥有较高市场知名度，为用户获得了良好的经济效益和社会效益。

2.2 案例二：某新能源发电企业旗下电厂监控系统安全解决方案

2.2.1 方案概述

电力系统的自动化和信息化不断提高且二者相互依赖程度也在不断提高，这对于信息安全提出了更高的要求。国家有关部门也更新了电力行业相关的信息安全要求。《电力监控系统安全防护规定》（国家发改委 2014 年第 14 号令），《电力监控系统安全防护总体方案》（国能安全[2015]36 号文）等一系列的文件的发布都使电力行业的信息安全防护更加全面、具体。与此同时，在国家倡导节能减排的环境下，风能、光伏等清洁能源技术发电的占比将逐渐升高，其将成为我国电能组成不可或缺的一部分，其网络环境的安全性对于整个电能供应的安全也起着至关重要的作用。

在本例中，我们将对某公司下属光伏、风能电站中电力监控系统中信息安全方面进行整改，使其符合电力监控系统安全规范要求并且提升系统及网络运维效率。整改前，各电厂电力监控系统部署的安全防护设备经查已总体满足“安全分区、网络专用、横向隔离、纵向认证”等基本要求，但公司电力监控系统目前尚未部署入侵检测装置、安全审计装置、防恶意代码装置，且纵向加密设备也有欠妥之处。本项目完成该公司旗下四家风电厂、四家光伏电厂安全系统、设备的供货及实施，及相关的技术培训、人员赋能和后续技术服务，实现电厂综合安全防护能力与运维人员的运维能力的全面提升。

2.2.2 典型安全问题

1.缺乏安全审计手段

运维人员或其他人员违规通过远程运维操控自动化系统等关键系统，使生产环境受到极大潜在危险。同时，生产环境并没有对关键运行数据进行审计，如关键操作系统、数据库、业务应用的重要操作及运行日志。

2.缺乏入侵防范措施

一旦有入侵发生，无法及时发现并采取相应的干预措施。

3.缺乏恶意代码防范手段

各电厂普遍缺乏恶意代码防范手段，或者防护系统特征库无法有效更新，使各电厂生产控制大区和管理信息大区的应用系统服务器和各终端计算机均面临恶意代码威胁。

4. 纵向加密装置不符合有关要求

有个别的电厂纵向加密装置未按照有关部门相关要求部署，未能部署经过国家指定部署检测认证的电力纵向加密装置。

2.2.3 安全解决方案

针对存在的信息安全问题，本方案旨在健全该公司各电厂网络安全防护体系，补足安全运维审计、入侵防护、恶意代码检测与防护、加密合规等方面的短板，使电力系统生产监控系统安全性得到进一步提高。

整改前，该公司旗下电厂拓扑示意图如下：

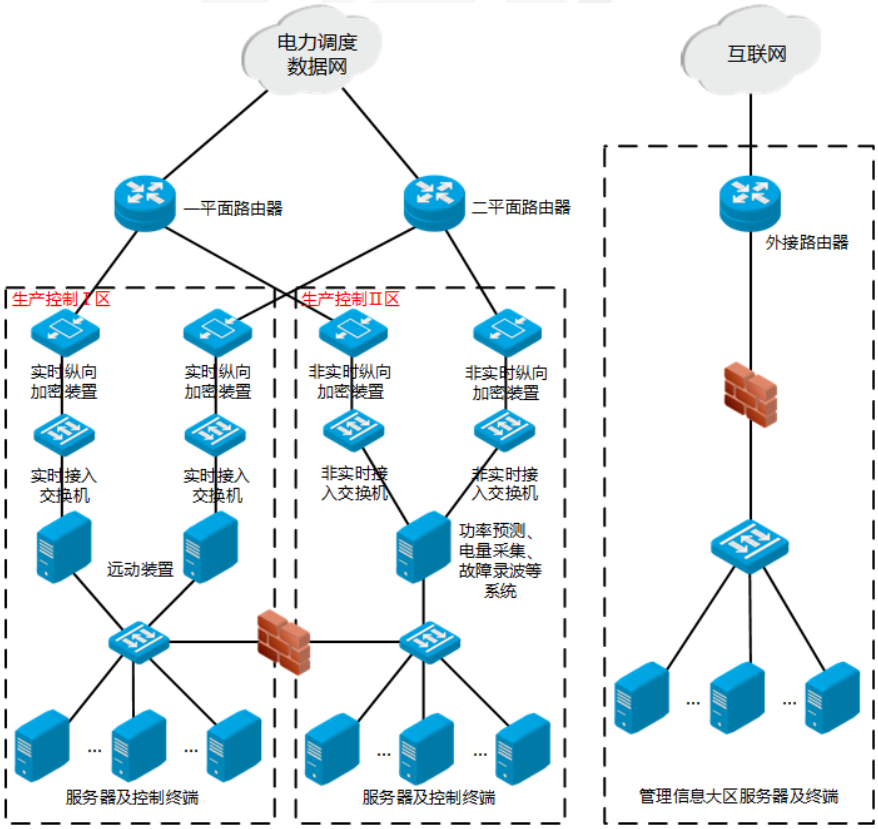


图 3 整改前电厂拓扑图

这些电厂中统调电厂存在管理信息大区，地调电厂无管理信息大区。其中有一地调电厂的生产控制 II 区没有使用专用的纵向加密装置，而是使用防火墙替代，这不符合有关部门的相关要求。其网络拓扑示意图如下：

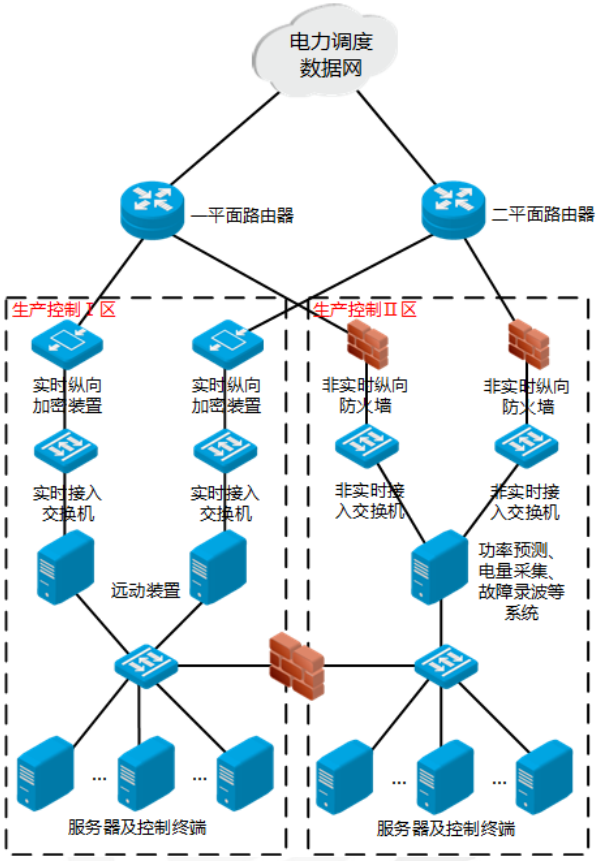


图 4 网络拓扑图

整改后，拓扑示意图如下：

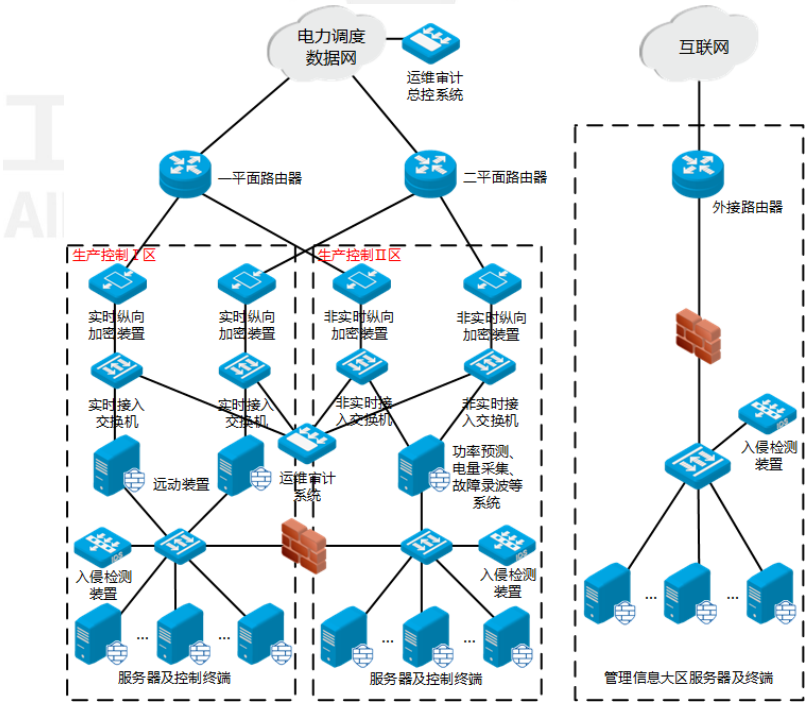


图 5 整改后拓扑示意图

针对存在的问题，我们给出以下解决方案：

- 运维审计方面

在安全运维审计方面，我司以国能安全 36 号文为基础，结合该公司电厂的实际情况，在各电站生产控制大区部署安全审计系统，对网络运行日志、操作系统运行日志、数据库重要操作日志、业务应用系统运行日志、安全设施运行日志等进行审计；对操作系统、数据库、业务应用的重要操作进行记录、分析，及时发现各种违规行为及攻击行为，并接受调度主站实时检测；对相关资产管理进行授权，并且对相关授权的权限进行管理。

另外，出于对堡垒机的性能考虑，堡垒机系统缺少对于用户和资产的授权关系的非常清晰的分析呈现，这时需要通过部署运维审计总控系统，进行统一的安全审计系统监控、和一些基础管理。运维审计总控系统采用旁路方式，部署在数据中心一平面Ⅱ区平台，接入下级堡垒机，通过对堡垒机的运维用户、设备、授权管理、告警管理等信息做同步采集、然后做统计关联分析分析形成报表，组合来查看这些授权之间的相互关系，进行维护，为删除清理等操作提供数据支撑，使堡垒机授权更加合理。

- 入侵检测方面

根据上文提及的 36 号令，生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规范，及时捕获网络异常行为、分析潜在威胁、进行安全审计。此外，根据该公司所属省份的相关规定，对统调电站的管理信息大区也需要单独部署入侵检测装置。

因此通过各电站生产控制大区和管理信息大区的核心接入域各部署一台入侵检测设备，在交换机上设置端口镜像，对流入的数据进行探测与检查，由安全管理系统统一管理，对网络违规行为及时检测、报警、记录。

- 恶意代码防护方面

相关要求规定应当及时更新测试验证过的特征码，查看查杀记录。禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。

因此在各电站生产控制大区和管理信息大区应用系统服务器、终端计算机均全面部署安全软件，并保证恶意软件特征码每天自动更新，并且特征码经过验证，以及接受调度主站的实时监测。同时，在生产控制大区中对安全性要求更高且工控系统的应用系统相对单一的特点，我们通过该软件实现了进程与应用程序白名

单，只允许可信的应用程序运行。此外，还通过此软件实现了 U 盘管理、补丁管理、防病毒管理、主机安全审计等功能。

- 纵向加密改善方面

相关监控系统防护方案中规定发电厂生产控制大区与调度数据网的纵向连接处应当部署经过国家指定部署检测认证的电力纵向加密装置，实现双向身份认证、数据加密和访问控制。

此次改造电厂中有电厂生产控制大区 II 区与调度数据网采用的防火墙，不符合要求，需将现有的 2 台防火墙更换成 2 台纵向加密装置。

2.2.4 小结

本方案帮助该公司旗下电厂符合国家等级保护及电力行业相关规定，补足安全运维审计、入侵防护、恶意代码检测与防护、加密合规等方面的短板，使电力系统生产监控系统安全性得到进一步提高。在符合要求的基础上，实现了工控主机防恶意代码及关键数据审计分析的统一平台化管理，实现了集中安全运维，有效提升了运维效率及生产网络环境的安全性。

2.2.5 单位基本信息

东软集团面向全球市场提供 IT 驱动的创新型解决方案与服务，致力于推动社会的发展与变革，为个人创造新的生活方式，为社会创造价值。以软件技术为核心，东软为客户提供行业解决方案、智能互联产品、平台产品及云与数据服务。

东软网络安全事业部成立于 1996 年，以业务驱动安全为核心，致力于业务安全的技术研究，为客户提供基于业务安全的网络安全防御体系。面对云计算、移动互联网、物联网、大数据、关键基础设施等新技术应用的快速发展和市场需求的不断变化，160G 数据中心防火墙、虚拟安全网关、桌面型无线安全网关、云安全支付网关、自主可控国产芯片网关、预警威胁管控平台等系列产品。

东软 NetEye 网络安全业务在未来将通过自身行业安全积累，凭借 IT 技术优势和经验，融合云计算、大数据、人工智能等新技术，积极适应网络安全市场新需求，引领网络安全市场新变化。

2.3 案例三：南京港华燃气安全解决方案

2.3.1 方案概述

燃气行业工控网络设计初始为单独组网的物理隔离环境，但随着信息化与工业化深度融合以及工业互联网的快速发展，工控系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工控系统扩散，工控系统信息安全问题日益突出。主要存在问题：

1. 控制设备安全防护手段还不完善;

2. 网络区域边界访问控制手段缺失;

3. 无线组网方式存在较大安全风险;

4. 安全管理制度及人员配置还不完善。

此方案设计参考国家等级保护模型，基本安全保护能力将通过选用合适的安全措施或安全控制来保证，根据等级保护要求，可以使用的安全措施或安全控制依据实现方式的不同，分为技术要求和管理要求两大类。

技术要求与管理要求是确保信息系统安全不可分割的两个部分，两者之间既互相独立，又互相关联，在一些情况下，技术和管理能够发挥它们各自的作用；在另一些情况下，需要同时使用技术和管理两种手段，实现安全控制或更强的安全控制；大多数情况下，技术和管理要求互相提供支撑以确保各自功能的正确实现。

亨通工控以等级保护的制度为依托，借鉴最新的等级保护思想，分别从技术和管理两大体系来规划南京港华燃气的工控安全体系建设方案，提升信息安全保障能力与水平。

2.3.2 典型安全问题

一、操作系统安全漏洞

目前所有厂站控制系统的主机操作系统都是 Windows，考虑到系统运行的稳定性，通常不会及时更新操作系统漏洞补丁。厂站监控中心采用的操作系统普遍是 Windows（Winserve2012、Winserve2008），高中压、中低压及 LNG 厂站 DCS

采用的操作系统也大部分是 Windows（winXP、win7），存在着安全漏洞威胁。

二、病毒与恶意代码

基于 Windows 平台的 PC 广泛应用，病毒也随之而泛滥。全球范围内，每年都会发生数次大规模的病毒爆发。目前全球已发现数万种病毒，并且还在以每天数十余种的速度增长。这些恶意代码具有更强的传播能力和破坏性，例如蠕虫，从广义定义来说也是一种病毒，但和传统病毒相比最大不同在于自我复制过程。

它能够通过端口扫描等操作过程自动和被攻击对象建立连接，自动将自身通过已经建立的连接复制到被攻击的远程系统，并运行它。

南京港华燃气基于工控软件与杀毒软件兼容性问题的考虑，在操作站上未安装杀毒软件，但即使是有防病毒产品，其基于病毒库查杀的机制在工控领域使用也有局限性，主要是网络的隔离性和保证系统的稳定性导致病毒库对新病毒的处理总是滞后的，工控系统每年都会大规模地爆发病毒，特别是新病毒。在操作站上，即插即用的 U 盘等存储设备的滥用，更给这类病毒带来泛滥传播的机会。

三、拒绝服务攻击和网络风暴

拒绝服务攻击是一种危害极大的安全隐患，它可以人为操纵也可以由病毒自动执行。南京港华燃气工控网对于此类威胁，主要产生于办公网用户电脑主机，当办公网主机遭受病毒后，对工控网毫无防备的设备、工控机发起攻击将变得轻而易举。常见的流量型攻击如 Ping Flooding、UDP Flooding 等，以及常见的连接型攻击如 SYN Flooding、ACK Flooding 等，通过消耗系统的资源，如网络带宽、连接数、CPU 处理能力、缓冲内存等使得正常的服务功能无法进行。拒绝服务攻击非常难以防范，原因是它的攻击对象非常普遍，从服务器到各种网络设备如路由器、等都可以被拒绝服务攻击。控制网络一旦遭受严重的拒绝服务攻击就会导致严重后果，轻则控制系统的通信完全中断，重则可导致控制器死机等。

网络风暴经常是由于 ARP 欺骗引起的 flood 攻击，或者因工控信息网络环路故障造成的网络风暴，这种攻击往往发生在同一网段的控制区域中，占用大量的带宽资源，工控系统疲于处理各种报文，将系统资源消耗殆尽，使工业系统报文无法正常传输。目前南京港华燃气采用总线型网络架构，所有厂站同属一个网段，对此网络风暴基本没有防范能力，往往容易造成严重后果。

四、黑客入侵与应用软件安全漏洞

黑客入侵和工控应用软件的自身漏洞通常发生在远程工控系统的应用上，另外，对于分布式的大型的工控网，人们为了控制监视方便，常常会开放外网方式接入，同时也不可避免的给黑客入侵带来了方便之门。

南京港华燃气工控网入侵风险，仍然是来自于办公网。办公网与工控网之间通过一台前置数据库服务器作为纽带，将工控网数据传输至办公网，但如果此服务器被黑客入侵成功，黑客将打破纽带夺取工控网的控制权限，从而控制所有厂站的工控设备。

五、高级持续性威胁

高级持续性威胁的特点是：目的性非常强，攻击目标明确，持续时间长，不达目的不罢休，攻击方法经过巧妙地构造，攻击者往往会利用社会工程学的方法或利用技术手段对被动式防御进行躲避。而传统的安全技术手段大多是利用已知攻击的特征对行为数据进行简单的模式匹配，只关注单次行为的识别和判断，并没有对长期的攻击行为链进行有效分析。因此对于高级持续性威胁，无论是在安全威胁的检测、发现还是响应、溯源等方面都存在严重不足。

南京港华燃气工控网络与信息网存在着逻辑上的连接，信息网又存在着对外网发布的服务，并且在工控网络边界也未有任何隔离手段，攻击者在突破信息网的防护后，能够轻易拿下工控网络的控制权限。

2.3.3 安全解决方案

一、设计策略

1、纵深防御体系

通过梳理南京港华燃气工控网络架构，并针对燃气工控系统，部署边界访问控制、流量监测审计、漏洞扫描、终端防护、数据认证与加密等防护管理设备，形成安全监测、安全检查与评估、安全预警通报等纵深防御体系，提升南京港华燃气工控网络整体防御能力，并满足工控网络安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理等需求。

2、统一管理平台

在生产控制网络中部署工控网络安全统一管理平台，为运维管理人员提供全面了解资产安全现状，管理网络安全防护设备的平台的集中统一管理平台，实现

安全防护设备的政策下发、运维管理、资产盘点等功能。

3、态势感知平台

针对南京港华燃气面临的工业设备和控制系统、现场物联网设备等资产安全、工业互联网平台安全、数据安全等问题，部署工业网络安全威胁预警及态势感知平台，建设完成包括在线监测网络、基础数据平台、安全态势感知多级安全保障基础设施，提升南京港华燃气工控网络安全综合保障能力。通过在内网部署多个工控系统蜜罐、探针，诱捕 APT（高级持续性攻击）攻击，防护真实工控系统不会受到黑客攻击。

二、纵深防御体系

1、安全通信网络建设

高中压厂站原有数据传输为自铺设总线型网络，从总线初始节点（2#阀室、东阳门站、亚东站），新增共计 3 条数据链路至 4#阀室，形成双链路传输的冗余架构；在 4#阀室新增汇聚交换机，避免汇聚层的单点故障；在中央路新增两台工控网核心交换机，把工控网从办公网核心上剥离出来单独组网。具体架构如下：

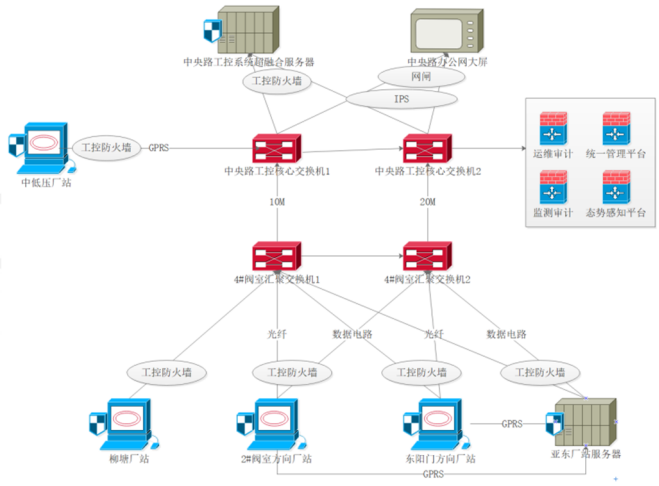


图 6 安全通信架构

2、安全区域边界建设

（1）工业防火墙

部署于被保护单元（PLC、DCS 等）和工程师站之间，可以采用黑、白名单的安全策略，过滤一切非授权访问，保证只有可信任的数据才允许通过，为控制网与管理信息网的连接、控制网内部各区域的连接提供安全保障。部署方式如下：

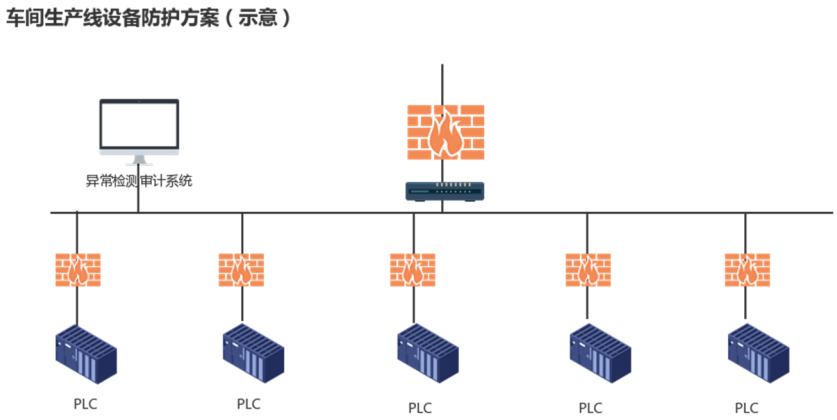


图 7 部署方式

本次设计在南京港华燃气各高中压厂站 PLC 上端部署导轨式工控防火墙，在中央路及亚东站的 GPRS 接受 VPN 设备下端部署机架式工控防火墙，防护 PLC 不受攻击。

（2）工业安全网闸

在工控网与管理网络边界部署工业安全网闸实现逻辑隔离与数据的安全传输，取代目前通过前置机的方式抓取数据，系统采用专用信息摆渡机制，解决了由于网络隔离引起的数据交换问题，既保持了网络之间隔离的特性，同时又提供了一种安全、有效的数据传输途径，采用非标准协议构成安全隧道，保障了数据传输的安全性，彻底杜绝了因办公网络的接入使业务系统感染病毒、木马的可能，消除了安全隐患。

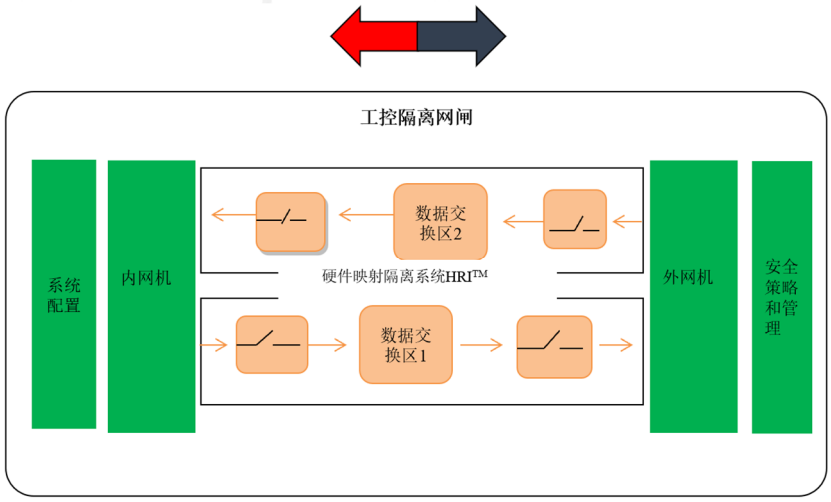


图 8 工业安全网闸

（3）入侵防御

入侵防御部署在中央路中心服务器上端，提供主动的、实时的防护，具备对2到7层网络的深度检测能力，同时实现跟防火墙的联动并及时更新攻击特征库，即可以有效检测并实时阻断隐藏在网络中的病毒、攻击与滥用行为，也可以对分布在网络中的各种流量进行有效管理，从而达到对网络架构防护、网络性能保护和核心应用防护的作用。

（4）工控安全监测审计系统

亨通工控自研的工控安全监测审计系统是针对工业控制网络数据通信进行安全审计的平台。部署在南京港华燃气工控网络交换节点，抓取网络中的所有数据，通过实时动态分析、数据流监控、网络行为审计等技术，快速识别工业控制网络中存在的异常行为。主要功能如下：

- ◆ 网络监测
- ◆ 安全审计
- ◆ 核心安全规则库
- ◆ 流量异常告警
- ◆ 自动化网络行为分析

3、安全计算环境

（1）主机安全

通过主机卫士与杀毒软件的结合从主机层面进行安全防护，同时可以配合基线检查、漏洞扫描、恶意代码监测等其他手段配合的方式，全方位的对生产控制层主机进行防护。

（2）工控运维审计系统

工控企业网络庞大、设备种类和数量较多且分散，维护需要记忆各种设备的IP地址和账号口令，对运维人员的工作提出很大挑战；同时运维人员对服务器、网络设备、工控设备的补丁升级、管理配置等所有重要操作行为都缺乏审计措施，出现问题后无法进行追溯；如通过第三方厂商进行维护，还必须提供账号和口令，存在敏感信息外泄的可能，在管理上存在安全隐患。通过部署工控运维审计系统，单点登录功能可避免记忆复杂口令，同时可将整个操作过程进行录像记录，以备后期审计取证，通过给第三方人员分配临时账号，可避免敏感信息外泄。

4、安全管理建设

（1）工业控制系统安全制度管理

根据工控安全制度管理的基本要求制定各类管理规定、管理办法和暂行规定。从工控安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

（2）工控安全机构管理

根据基本要求设置工控安全管理机构的组织形式和运作方式，明确岗位职责；设置工控安全管理岗位，设立工控系统管理员、工控网络管理员、工控安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理工控信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；制定文件明确工控安全管理机构各个部门和岗位的职责、分工和技能要求。

（3）人员安全管理

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。一般单位都有统一的人事管理部门负责人员管理，这里的人员安全管理主要指对关键岗位人员进行的以工控安全为核心的管理，例如对关键岗位的人员采取在录用或上岗前进行全面、严格的安全审查和技能考核，与关键岗位人员签署保密协议，对离岗人员撤销系统帐户和相关权限等措施。

（4）工控系统建设

工控系统建设管理的重点是与工控系统建设活动相关的过程管理，由于主要的建设活动是由服务方，如集成方、开发方、测评方、安全服务方等完成，运营使用单位人员的主要工作是对之进行管理，并按照管理制度落实各项管理措施，完整保存相关的管理记录和过程文档。

（5）工控系统运维管理

建立环境和资产安全管理制度、设备和介质安全管理制度、日常运行维护制度、事件处置与应急响应制度、灾难备份制度、工控安全监测制度。

三、统一管理平台

统一安全管理平台是对工业网络中的安全设备及数据进行统一管理。全面提高南京港华燃气工控设备、工业互联网平台和工业企业物联网设备的发现能力以

及安全管理能力。通过对控制网络中的边界隔离、网络监测、主机防护等安全产品进行集中管理，实现对全网中各安全设备、系统及主机的统一配置、全面监控、实时告警、流量分析等，降低工业企业运维成本、提高事件响应效率，满足安全管理中心需求。

四、态势感知平台

本次建设在南京港华燃气内网服务器上部署态势感知平台，安全态势感知与威胁预警平台的整体架构分为：用户端、数据采集层、数据存储分析层、基础应用层、安全中心功能层，如下图所示：

图 9 态势感知平台

2.3.4 小结

针对市政燃气行业的特点和网络现状，同时结合行业工控系统网络结构和安全需求，对目前燃气管网系统存在的安全威胁提出相应解决策略。希望通过燃气行业工控系统安全解决方案，帮助燃气企业建立工控系统安全保障体系，增强安全风险防范能力，促进工控系统安全、稳定运行，降低燃气行业工业控制系统网络安全风险。

2.3.5 单位基本信息

江苏亨通工控安全研究院有限公司（简称亨通工控安全）是亨通光电与国家信息安全工程技术研究中心江苏分中心合资共建企业；是国家中小型科技企业，江苏省双软企业，江苏省民营科技企业，江苏省高新技术企业，入选江苏省工业控制系统信息安全三年行动计划、智慧江苏重点工程、江苏省和苏州市工业互联网服务资源池；是工业互联网联盟会员单位、工业信息安全产业发展联盟会员单位、江苏省网络安全协会常务理事单位、中关村智城军民融合信息安全工程技术联盟理事单位、江苏省 AK 联盟成员单位；苏州市相城区智能制造产业联合会轮值会长单位；江苏省网络安全先进单位；是国家高技能人才培训基地、苏州市职业大学＂双师型＂教师培养培训基地、苏州市职业大学高技能人才实训基地、相城区亨通工控公共实训基地；认定为江苏省院士工作站、苏州市新型研发机构；工控防火墙系统、安全运维审计系统、工控检测审计系统、工控主机防护系统以及抗拒绝服务系统获得公安部销售许可证，工控防火墙系统获得电科院产品检测报告；信息安全、网络安全业务已入围移动、电信、联通运营商供应商名录；自主研发的工控安全产品已在市政燃气、智慧水务、智能制造和电力行业应用。

2.4 案例四：某城市轨道交通信号系统网络安全解决方案

2.4.1 方案概述

随着 2017 年《中华人民共和国网络安全法》的正式实施，我国正式进入网络安全建设新时代。安全法明确提到：“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，实行重点保护”。

城市轨道交通信号系统作为关键信息基础设施，是否能够持续安全运行，直接关系到广大乘客的生命安全，一旦遭到破坏，会对国家秩序造成重大隐患。目前信号系统网络安全并未受到高度重视，即便为了合规做了网络安全防护建设，但是业务现场仍处于传统的安全防护阶段，主要采用“封、堵、查、杀”的方式筑起一道安全防线。面对新形势下有目的性的新型网络攻击，传统的被动的防御就好比空手对大炮。因此，必须调整安全建设思路，从传统被动防御转变为主动防御，构建安全可靠的工业网络环境，才能保障城市轨道交通信息基础设施的运行安全。

当前轨道交通信号系统按访问对象划分为三大安全区域，包括控制中心、设备集中站（含车辆段、停车场）、非设备集中站，其中业务系统包括 ATS 子系统，ATC 子系统，DCS 子系统和维护网子系统等。按照实际建设需求，目前信号系统的等级保护只覆盖到 ATS 子系统和维护网子系统。网络结构示意图如下图所示：

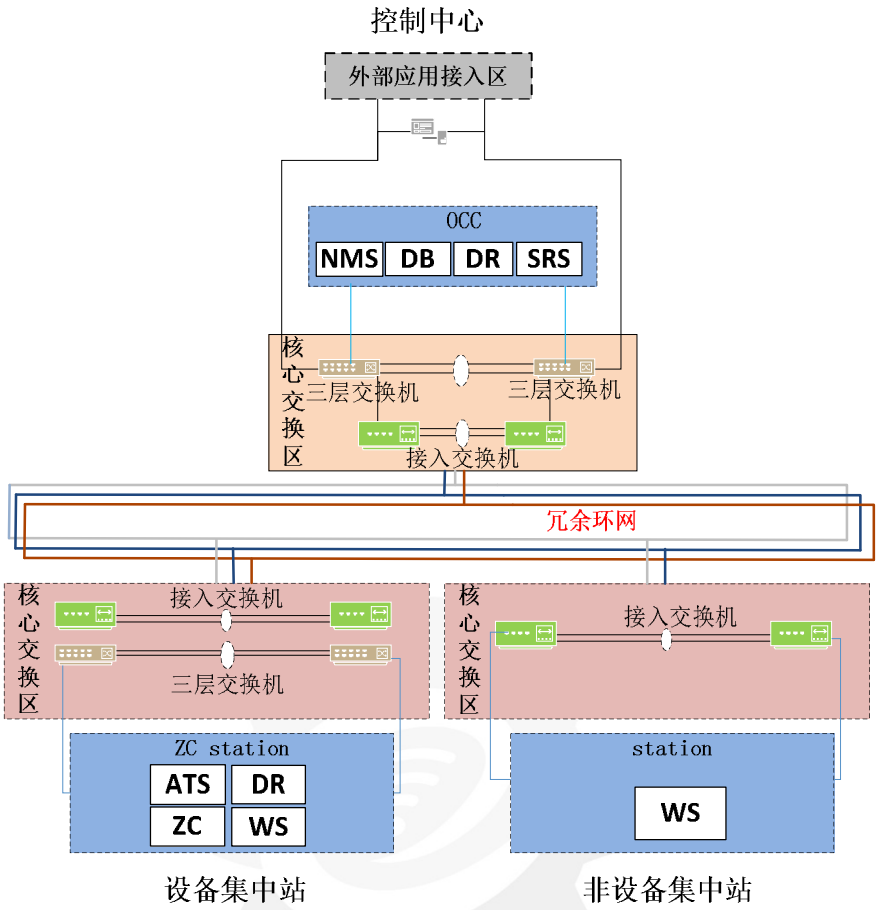


图 10 信号系统网络结构示意图

2.4.2 典型安全问题

当前轨道交通信号系统网络安全防护存在两类情况：

一、部分既有信号系统仅采用传统防火墙和杀毒软件。传统防火墙主要进行逻辑区域隔离控制，具有访问控制、安全域管理、网络地址转换等功能，但是传统防火墙未装载工业协议解析模块，不能解析工业控制协议。终端防护主要通过杀毒软件来实现，但是杀毒软件需要定期升级病毒库，而工业控制系统网络环境不允许病毒库实时更新。另外，杀毒软件有时会误杀工业软件。

二、部分信号系统依据等级保护 1.0 标准做了相对完善的安全防护，主要体现边界防护、主机防护、入侵检测、日志审计等方面。各设备部署情况：

1.信号系统与外部接口的网络边界部署工业防火墙，工业防火墙除了传统防火墙具备的访问控制、安全域管理等功能外，还增加了针对工业协议的协议过滤模块和协议深度解析模块，可做到对信号系统应用层协议内容的过滤，防止应用

层协议被篡改或破坏。

2.对关键主机的配置进行加固、补丁管理、漏洞修复等措施，部分通过部署白名单软件对可疑程序进行有效阻止。

3.在核心区域交换机旁路部署入侵检测系统。对各级交换系统间的通信流量进行深度分析，检测病毒、蠕虫、木马、间谍软件、可疑代码、扫描等网络威胁，一旦发现攻击及时告警。

4.对信号系统网络中的安全设备、网络设备、主机等进行集中安全监管，同时对各类安全日志进行收集汇总分析，并生成报表。

以上安全防护手段虽然可以抵御大多数常见类型的威胁和攻击，但仍存在局限性：

1．缺少整体安全防护管控设计，设备功能单一孤立，缺少动态关联分析，单点防护和静态防御缺点突显；

2．缺少主动网络安全防御能力，利用“查”“杀”“封”被动防护措施，安全防控能力滞后，未知威胁和新型网络攻击检测能力薄弱。

2.4.3 安全解决方案

信号系统的网络安全防护在做好顶层设计构建安全防护体系的基础上，重点在工业互联网安全要求上展开安全防护新思路，信号系统安全框架从防护对象、防护措施及防护管理三个视角构建。针对不同的防护对象部署相应的安全防护措施，根据实时监测结果发现网络中存在的或即将发生的安全问题并及时做出响应。同时加强防护管理，明确基于安全目标，持续改进的管理方针，保障轨道交通信号系统的持续安全。主要体现在新型网络攻击防护，预知安全态势以及组建专业的安全管理团队，提高安全防护保障能力等方面。

（一）做好顶层安全设计

构建信号系统网络安全防护体系需要从信号系统业务流程及系统安全需求分析为基础，保证信号系统所有用户访问、操作都经过授权，保证信号系统运行环境安全可靠，保证各种安全机制不被旁路，因此必须以控制安全为基础，以细粒度的访问控制为核心，构建信号系统网络安全纵深防护体系。

构建结合设备安全、网络安全、控制安全、应用安全、数据安全五大方面，

构建以安全管理中心为核心，构建以安全计算环境为基础、安全区域边界和安全通信网络为保障的信息安全整体防护体系。信号系统安全防护体系如下图所示：

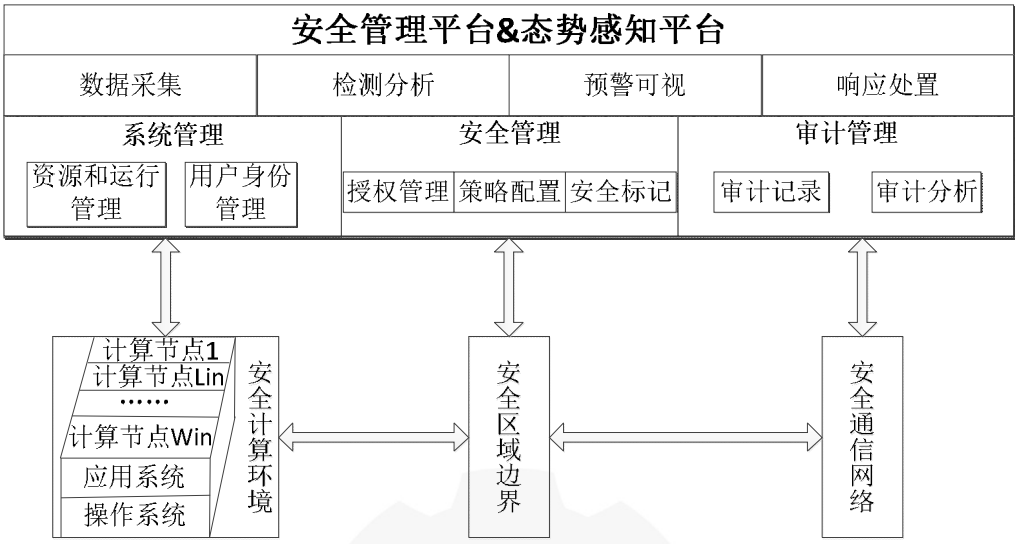


图 11 安全防护体系

安全管理中心是一个集合的概念，核心是实现所有安全机制的统一集中管理，是三层防护体系的控制中枢。安全管理中心由安全管理平台实现，基本功能包括系统管理、安全管理、审计管理，同时建立全局统一可控的态势感知平台，共同为信号系统的安全可靠运行提供重要支撑。

安全管理平台采用“三权分立”，权利最小化原则。系统管理主要功能是对信号系统的整体运行情况进行管控，确保系统稳定高效运行。对计算环境内的工作站、服务器等主机类设备，路由器、交换机等网络设备以及网络流量和用户行为进行监测，对管理人员以及用户身份进行集中管理和授权等；安全管理主要功能是对信号系统安全策略实行统一配置、参数设置，安全标记，对设备的安全性和可用性实时监控，设置告警阈值；审计管理用于采集和处理整个信号系统中各个节点的审计信息，包括终端用户的登录、文件的读写、入侵日志、网络访问行为等，通过对审计信息的关联分析，分析出信号系统可能存在的安全风险。

在安全管理平台基础功能上，建立全局统一可控的安全态势感知平台，通过采集信号系统内 IT 基础设施数据，利用关联分析、机器学习、数据建模等方法对数据进行统一分析，实现对网络攻击行为、安全异常事件、未知威胁的告警和响应。

安全计算环境是信号系统安全的核心和基础，是授权和访问控制的源头。一

方面计算环境安全通过主机、服务器操作系统、应用系统和数据库自身的安全服务机制，保障应用业务处理全过程的安全。另一方面设置以强制访问控制为主体的系统安全机制，通过对用户行为的控制，来防止非授权用户访问和授权用户越权访问，同时限制终端设备相关端口的使用。

安全区域边界是信号系统与外部系统进行数据交互的区域，安全区域边界重点对进入和流出计算环境的信息实施控制和保护，允许安全策略内的信息流经过边界。为满足访问控制、边界完整性检查，入侵防范等基本安全要求，一般通过在信号系统与外部系统连接处，部署工控网关类设备进行安全防护。

安全通信网络是计算环境之间实现信息传输功能的载体，信号系统通信网络主要是安全区域之间的网络通道，安全通信网络需要确保用户信息传输过程中不被窃听、篡改和破坏，需要对通信流量实时监控，对异常流量和操作及时告警和记录。

（二）应对新型网络攻击

在工业互联网安全中明确规定，应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。在对应互联网安全要求部署抗 APT 攻击系统、网络回溯系统和威胁情报检测系统或相关组件，并验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

以 APT 攻击为代表的新型网络攻击愈演愈烈，APT 攻击是一种高级复杂的，持续性，目标针对性很强的攻击。这种攻击一般采用 0day 漏洞实施攻击，目的是收集和窃取高价值的数据，控制破坏重要信息系统，不达目的不罢休，成为了不法分子、敌对势力恶意攻击惯用的手段。APT 攻击过程如下图所示：

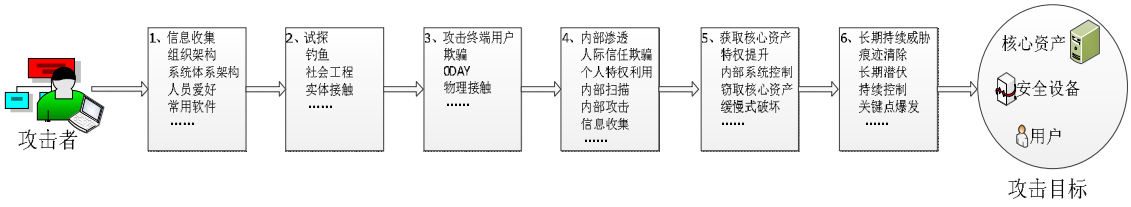


图 12 APT 攻击过程

应对 APT 攻击前提是能有效的检测到安全威胁的存在，能够动态实时检测，捕获到 APT 攻击数据。结合 APT 攻击过程，解决 APT 攻击主要有三个环节：

首先，采用大数据存储以及异常流量检测技术识别异常流量，从数据流中提取文件或样本；

其次，采用深度沙箱检测技术将传统检测无法检测出的未知恶意样本进行深度检测，通过虚拟机技术模拟用户执行环境，激发样本行为，让可疑文件在模拟环境中运行，监控可疑行为判断未知恶意文件。同时采用全流量回溯分析技术，保存原始全流量数据包，通过当前攻击行为和历史数据的关联分析，实现 APT 攻击过程的溯源，确定 APT 攻击行为；

最后，提取恶意行为的特征，形成特征库或策略库，将安全策略下发到检测设备，对相应规则进行拦截，形成整体防御体系。

（三）感知未来安全态势

习总书记在 419 座谈会上提出：“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力”。随后网络安全法、国家网络安全战略、互联网安全等政策标准的出台，对未来安全态势的感知被提升到了战略高度，安全态势感知技术应需迅速崛起。态势感知的最终目的就是能够基于环境、动态的、整体的识别安全风险，依靠大数据的支撑，从整个系统视角发现识别安全威胁，进而理解分析预警，最终响应处置落地。

信号系统的态势感知目标就是要为信号系统 IT 资源及其业务系统穿上一件保护外套，部署一套全方位的安全保障体系，态势感知网络示意图如下图所示：

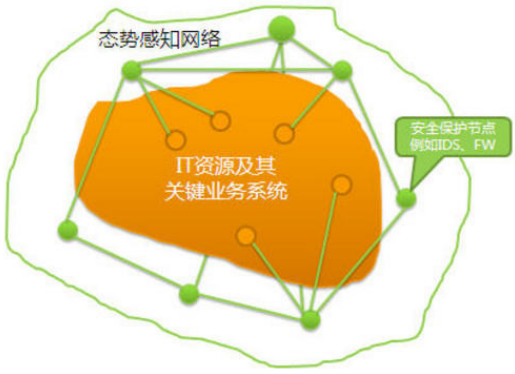


图 13 态势感知网络示意图

安全态势感知系统相当于人体的神经系统；防火墙、入侵检测系统、漏洞扫描系统等安全设备以及服务器、网络设备作为态势感知信息来源的基础，相当于神经元；安全分析相当于神经中枢——大脑，每个安全事件的处理过程就相当于神经传导和处理过程。从这个角度来看，态势感知系统处理数据、将数据分析建模的过程与人脑的对外界信息的感知过程是类似的。

传统的态势感知仅是通过采集安全设备的审计信息和扫描结果，进行总结归纳，以图表的形势展示出来，主要针对已知网络攻击行为进行监测和评估，评估结果单一，也没有实现网络安全态势感知的预测功能。随着安全技术和大数据技术的融合，态势感知需要采集多个维度信息源的数据，然后采用数据分析技术识别海量数据中有用信息，通过机器学习、威胁情报分析等自动生成分析模型，由已知威胁来推演未知威胁，对未来安全趋势进行风险预警和协同防御。态势感知框架如下图所示：

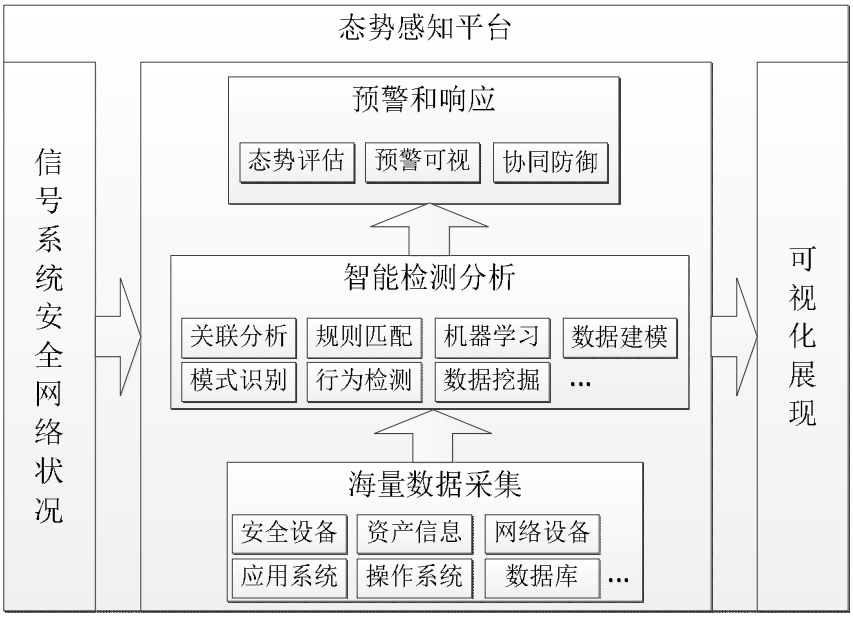


图 14 态势感知框架

1.海量数据采集：态势感知需要有大数据的支撑，应具有主动采集能力。数据来源至少应该包括 IT 资产信息、拓扑信息、弱点信息、IT 资源性能和运行状态信息、各种告警、警报、事件、日志等等。

2.智能检测分析：通过智能化分析，从海量数据中分析出有效的安全问题。智能分析不仅仅是匹配静态特征库进行安全威胁分析，要基于流量特征、行为分析建模、机器学习、数据关联等进行深度智能数据分析，从而具有解决未知威胁的能力。

3.预警和响应：智能分析结果都可以送入预警与响应模块，一方面借助态势可视化进行预警展示，另一方面，送入流程处理模块进行流程化响应与安全风险运维。做到及时、高效的响应处置动作完成，才算真正解决了安全问题。

（四）组建安全管理团队

“三分技术，七分管理”，技术是安全防护的必要手段，人是安全防护的核心

和尺度。信号系统运营人员普遍存在安全意识不高，安全知识缺乏，安全能力不足。面对日益严峻的网络安全现状，需要组建专业的安全管理团队，来提供网络安全保障服务。安全管理团队可以运营单位自己组建，也可通过专业的第三方安全团队来提供安全管理。安全管理团队主要职责有：

1. 做好系统风险监测、预警通报工作，及时向有关部门通报可能影响系统的重大漏洞和风险。

2. 做好应急预案，定期开展攻防演练，在攻防过程中通过发现大量现实存在的网络安全问题，找到安全防护体系的安全短板，及时弥补持续优化，提升安全防护能力。通过攻防演练提高面对突发网络攻击的应急响应和应急处置能力。

3. 负责突发安全事件的响应和处置，攻击过程的分析和处理，以及事件的调查与溯源，做好事后的总结工作。

2.4.4 小结

随着工业互联网深入发展和应用推广，企业面临新的安全威胁，网络安全越来越引起国家和重要行业部门的重视。城市轨道交通信号系统传统的防御措施已经无法应对 APT 等新型网络攻击。工业互联网时代构建一个事前态势感知、事中应急响应、事后追踪溯源的整体、主动和动态的安全防御体系，全面提升信号系统网络安全感知能力和防护水平。

2.4.5 单位基本信息

中国电子信息产业集团有限公司第六研究所（ 工业控制系统信息安全技术国家工程实验室)以工控系统及安全为引领，依托工业控制系统信息安全技术国家工程实验室，开展网络安全技术研究，支撑政府网络安全工作，承担国家网络靶场任务，提供工控安全检测认证服务，全面布局全国产化金融设备、轨道交通、先进智能制造三大重点产业，保障国家关键信息基础设施网络安全。致力于工业控制系统信息安全关键技术研究和重要技术标准研究制订，建设工业控制系统信息安全技术产业化平台，提升我国工控安全核心竞争力，培养工控系统信息安全专业人才队伍，集智攻关、联合创新，打造产业链上下游同发展的良性生态圈，实现工业控制系统“可发现、可防范、可替代”的安全目标。

2.5 案例五：风电场电力监控系统网络安全解决方案

2.5.1 方案概述

电网作为我国最重要的关键基础设施，如何针对清洁环保的新能源关键信息系统设计安全有效的防护方案，以保障新能源安全的并入电网，是一项比较大的挑战。风力发电因环保、能量储蓄大、资源丰富等特点，受到全球各国的广泛重视。随着大量的风力发电并网技术的成熟，风力发电不仅解决了日益增产的能源需求，同时有效的保护了我国的自然生态环境。

国家电网作为我国最重要的关键基础设施，大量风力发电的并网的同时，给电网的信息安全保障工作在管理和技术上同时提出了更高的挑战，国家能源局于2015 年出台的《电力监控系统安全防护总体方案》（国能安全【2015】36 号)以“安全分区、网络专用、横向隔离、纵向认证”的纵深防御原则，提出了省级以上调度中心、地县级调度中心、发电厂、变电站、配电等的二次系统安全防护方案，综合采用防火墙、入侵检测、主机加固、病毒防护、日志审计、统一管理等多种手段，为二次系统的安全稳定运行提供了明确的技术指导方案。

本方案基于纵深防御的工业安全防护理念，结合风电场监控系统网络安全的案例实施，在项目过程上从现状分析，安全设计——包括网络边界的隔离和加密、上下位主机安全防护以及外设管控等技术层面，方案实施以及安全方案实施后的攻防验证，进行了一体化、一致性的安全设计。

2.5.2 典型安全问题

从网络相关性来看，风力发电分成两部分，一部分是发电生产相关的生产过程控制和监控系统以及相关的企业运营和决策系统，另外一部分为和电网并网业务关联的控制 I 区，控制 II 区和电力调度系统。

虽然风力发电和输、变、配、用电由不同的公司运营，且各自的网络大小、规模和使用人群面等复杂度和专业均有不同，但均涉及传感、控、调和生产调度、办公运营各部门组成，故从整体上看，不管是风电场还是电网公司的网络业务系统，均能参照工控系统普渡参考模型对具体业务间的逻辑来进行分层理解。

控制网络的生产区间系统由风场内控制系统和风场集控中心电力监控运营决策组成的典型的跨物理区域的分布式工业监控系统组成，与电力并网的电力调度并不直接存在网络耦合关系（简称非涉网区域）。和电力调度并网相关的系统包含远动子站、AVC 子站、保信子站等和电网中变电站相关的子系统，属于国家能源局《电力监控系统安全防护总体方案》所定义的控制大区范畴（简称涉网区域）。相关元素详见下表。

表 2　涉网区域典型网络元素

网络元素名称	是否属于控制大区	物理归属地
远动子站	是	风电场
AVC 子站	是	风电场
保信子站	是	风电场
测控装置	是	风电场
风力预测	是	风电场
工作站	是	风电场
其他二次装置	是	风电场
纵向加密装置	是	风电场
横向隔离装置	是	风电场
对时装置	是	风电场
交换机	是	风电场

表 3　非涉网区域典型网络元素

网络元素名称	是否属于控制大区	物理归属地
缓存服务器	否	集控中心
数据库服务器	否	集控中心
历史服务器	否	集控中心
工作站	否	集控中心
工程师站	否	集控中心
终端服务器	否	集控中心
应用服务器	否	集控中心
运营分析服务器	否	集控中心
前置机	否	集控中心
GPS 时钟/授时装置	否	集控中心
PLC	否	风电场
仪表	否	风电场
升压监控	否	风电场
风机监控	否	风电场/集控中心
振动监测	否	风电场/集控中心
风功率预测	否	风电场/集控中心
电能计量	否	风电场/集控中心
多功能电表	否	风电场

视频监视	否	风电场
VPN	否	集控中心
交换机/路由器	否	集控中心/风电场
打印机	否	集控中心

2、 风力发电网络安全防护的常见的问题

风力发电因生产占地区域广，具备涉网和非涉网两大功能网络，同时，非涉网区域存在大量的互联网接入引入了安全风险，在分析问题前，可对安全脆弱性电力行业工业控制系统风险评估工作流程进行工业控制系统的威胁分析，经过现场调查，监控系统常见有如下安全问题：

- **涉网区域常见的安全问题**

1）缺少信息加密手段

调度数据网和非实时控制区（II 区）之间采取纵向防火墙进行防护而缺乏纵向加密装置，存在网络传输过程被窃听和篡改的可能。

2）控制 I 区缺乏安全防护和逻辑隔离措施

远动系统(控制 I 区)与风功率预测系统（控制 II 区）连接，并没有安全防护和逻辑隔离措施。

3）控制 I/II 区存在缺少隔离装置或装置故障

风功率预测服务器出口反向隔离装置故障。

4）未采取入侵检测措施和安全审计设备

5）缺乏防范恶意代码的技术设备

6）上位机缺乏病毒管控措施

控制区大量上位机系统暂未安装防病毒软件，部分主机已感染病毒和木马。

7）上位机外围接口缺乏监管

现场的上位机 USB 端口存在无有效监管。

- **非涉网区域常见的安全问题**

因非涉网区域独立运营的特殊性，风电场和集控中心在非涉网区域，除了涉网区域提到的上述问题，还存在如下的问题：

1）工作站和服务器缺少有效的监管。

2）与外网存在广泛交互，且缺少相关安全措施，存在跨网攻击的可能。

3）纵向加密装置普遍缺失。

2.5.3 安全解决方案

本方案以2015年出台的《电力监控系统安全防护总体方案》(国能安全【2015】36号)以“安全分区、网络专用、横向隔离、纵向认证”的纵深防御原则，引入工业系统在线集中管理和监测平台精准的通知企业整改，在企业的纵深防御中加入相应防护，防患于未然。

1、网络安全防护方案

1）网络分区

划分控制区和非控制区，在非涉网的区域内，增加工业防火墙进行逻辑分区隔离。

2）纵向加密

网络至调度的上行边界处，部署支持国密加密算法的纵向加密装置。

3）横向隔离

在控制区域内，部署正反向装置进行横向隔离。

4）入侵检测

风电场内部旁路部署工控入侵检测审计一体化设备，实现基于业务行为和流量白名单的常见恶意攻击行为和异常流量检测告警，并且能够实现网络行为和流量审计，提供异常行为和流量日志回溯。

5）日志管理

搜集并存储日志，用于安全事件追溯还原，以及业务运维和预警。

6）安全集中管理监测

部署统一管理平台，相关安全设备的统一管理和安全策略的统一下发集中管理、分析设备运行状态，提升安全管理效率，降低运行维护成本。

2、主机安全防护方案

1）主机加固

主机安装工控专用的主机和服务器防护软件，抵抗病毒，木马等恶意程序攻击。

2）外设管控

主机安装对USB端口进行防护和监管的软件，抵抗U盘、外设摆渡攻击。

3、整体防护方案一览

首先，按照控制 I 区、控制 II 区，以及管理大区对风电场场内和集控中心网络系统进行分区，其次，基于方案设计阶段，对整体网络进行的脆弱性分析，结合前两节所述的安全防护方案，分别部署正反向隔离装置，工业防火墙、工业监测审计系统、工控主机卫士，和统一安全管理平台，达到监控系统网络纵深防御的效果。整体如下图所示。

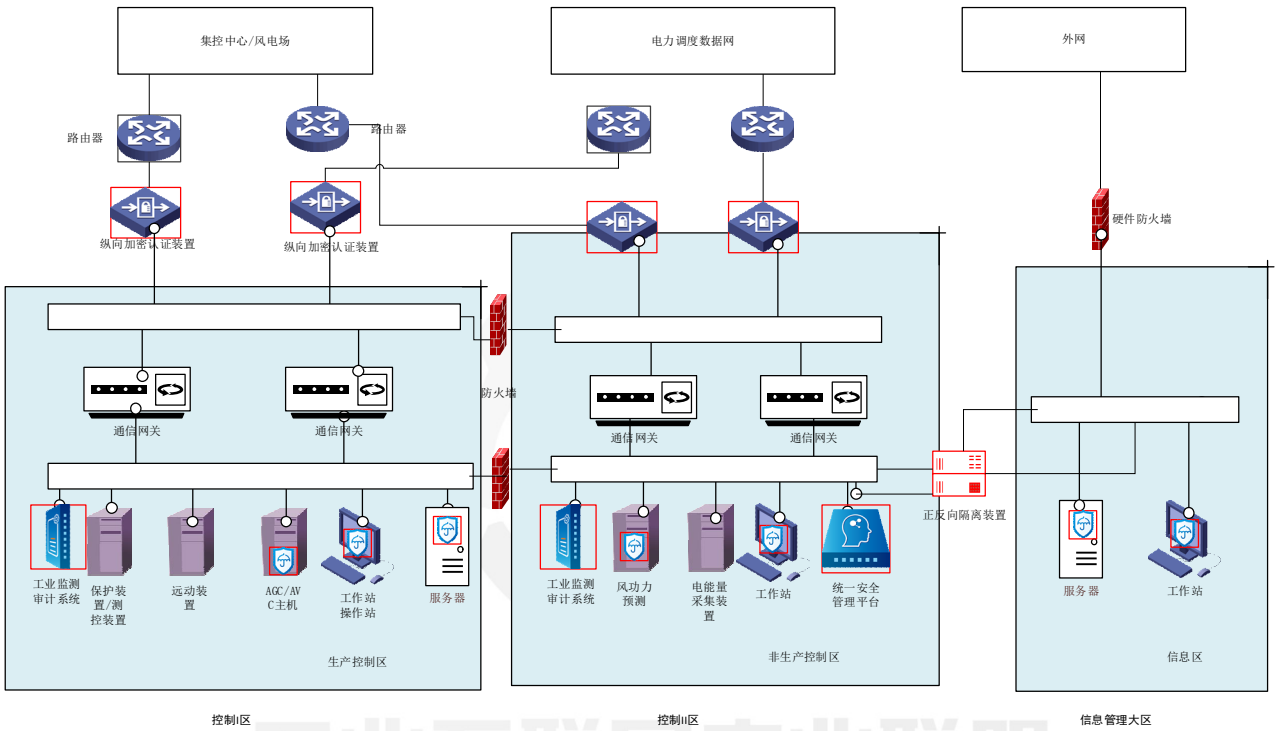


图 15 风电场电力监控系统整体防护方案

4、安全设备部署说明

本项目配置关键安全设备如下表所示：

表 4 安全设备配置列表

序号	类型	主要功能	部署依据
1	工业防火墙	基于安全规则精准行为控制，工控网络攻击特征分析与拦截。	**国能安全【2015】36 号文附件 4《发电厂监控系统安全防护方案》** 控制区与非控制区之间应当采用具有控制访问功能的设备或相当功能的设施进行逻辑隔离 5.1 入侵检测：生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜

序号	类型	主要功能	部署依据
			在威胁并进行安全审计。 5.4 安全审计:生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析、及时发现各种违规行为及病毒和黑客的攻击行为。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。
2	工控主机卫士	操作系统及监控软件安全加固	国能安全【2015】36 号文附件 4《发电厂监控系统安全防护方案》 2.5 综合防护:综合防护是结合国家信息安全等级保护工作的相关要求对电力监控系统从主机、网络设备、恶意代码防范、应用安全控制、审计、备份及容灾等多个层面进行信息安全防护的过程。 5.2 主机与网络设备防护:发电厂厂级信息监控系统等关键应用系统的主服务器、以及网络边界处的通信网关机、WEB 服务器等，应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专用强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安全应当经过测试。
3	纵向加密认证装置	风电场安全 II 区与调度之间进行数据传输加密	国家发展改革委第 14 号令《电力监控系统安全防护规定》第十条:在生产控制大区与广域网的纵向联接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施。
4	横向隔离装置	用于风电场安全区 I/II 和安全区 III 的单向数据传递	国家发展改革委第 14 号令《电力监控系统安全防护规定》第九条:在生产控制大区与管理大区之间必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置
5	杀毒电脑	用于风电场上位机和服务器不受病毒的侵犯	**国能安全【2015】36 号文附件 4《发电厂监控系统安全防护方案》** 5.7 恶意代码防范：应当及时更新特征码，查看查杀记录。恶意代码更新文件安装应当经过测试。
6	安全审计网关	用于风电场安全区 I/II 安全监测和审计	**国能安全【2015】36 号文附件 4《发电厂监控系统安全防护方案》** 5.4 安全审计:生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析、及时发现各种违规行为及病毒和黑客的攻击行为。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。

5、关键设备功能参数

1）工业防火墙

性能指标：

表 5 性能指标

序号	技术指标项	技术规格
1.	变量处理点数	10 万点
2.	吞吐量	900M
3.	并发	50 万
4.	新建	6000 个每秒
5.	时延	满负荷运行的时延时间≤100μS

表 6 功能指标

序号	技术指标项	技术规格
1.	部署方式	★支持无 IP 透明方式部署，路由方式部署。
2.	工业协议支持	★支持超过 **12 种工控协议的深度解析和指令集控制**（包括但不限于 Modbus/TCP，OPCDA，DNP3，S7，IEC104，MMS，Profinet ，BACnet, GOOSE，SV，Ethernet/IP, OPCUA_TCP 等）。 ★实现指令级控制，对 Modbus 协议实现某个功能码或寄存器地址上的数据进行解析和控制;对 S7 协议实现 PDU 类型和功能操作的解析和控制;对 OPC-DA 协议实现读写操作的解析和控制。 ★支持 OPC 断线重连功能。
3.	实时监控	★事件实时监控，包括事件总数、未读事件数以及事件发生的高峰时段，将事件信息分为安全事件和系统事件两类分别监控，并支持将事件导出为 excel 格式。 日志监控功能，包括用户登录日志，用户操作日志，防火墙报文日志记录功能。 ★未知设备监测，对系统内未知的设备接入进行实时告警，迅速发现系统中存在的非法接入，并能够支持阻断功能。
4.	安全策略	★须支持黑名单规则配置，每个漏洞对应一条保护规则，用户可以选择哪些规则部署到网络中 ★黑名单特征数量不低于 900 条，并支持无扰导入。 ★支持自学习创建白名单应用规则，学习时间可配置。 支持基于网络层的基础网络安全策略。 支持 IP/MAC 地址绑定规则，同时需要支持针对特定工控设备做绑定和解绑编辑功能。 ★支持工业控制协议读写控制，包含 Modbus 协议、S7 协议、OPC-DA 协议等。支持针对单个 IP 流量的控制及针对单个 IP 会话数控制。 ★支持防 DDOS 攻击和防扫描攻击功能，用户可以开启防御来实现防 SYNflood、UDPflood、WinNuke、Land、Smurf、Ping of death 攻击。

		★能防止 TCP 扫描和 UDP 扫描攻击。
5.	运维管理	支持测试模式和工作模式等不同运行模式，以保障工控系统运行的稳定性。 ★支持单一设备自管理完成所有管理功能项
6.	集中部署	支持集中管理可由统一安全管理平台集中进行配置、监控、管理。 支持日志上报至统一安全管理平台进行统一查看。

2）工控主机卫士

表 7 工控主机卫士

序号	项目	技术规格
1	功能及技术要求	★**一键主机加固**，一键扫描并将当前操作系统的全部文件生成基准白名单，对文件进行唯一标示管理，防止被病毒、恶意程序篡改
		★支持进程白名单管理：增、删、改、查； ★对非白名单内程序的执行进行阻止； ★对阻止的信息进行审计记录，记录包括：时间、次数、程序名称、路径、结果、父进程名称、公司名、产品名、版本等详细信息； ★采用静默气泡提醒，对用户无打扰。
		★支持对单文件及文件夹的保护，防止文件被包含勒索病毒、木马等程序恶意篡改。 ★支持对注册表保护，防止注册表被恶意篡改。 ★对被保护文件及注册表的修改行为的阻止过程进行审计记录，包括：文件、注册表的完整路径、尝试修改的时间等详细信息； ★采用静默气泡提醒，对用户无打扰。
		支持 USB 管理，禁止白名单以外的非法 USB 设备连接，并产生安全事件，记录非法 USB 设备的连接企图，支持对 USB 设备操作行为审计。 支持对 USB 设备的识别与授权，支持 USB 存储设备的多种操作权限：读写、禁止等。
		★对异常的文件篡改和程序执行采用汽泡形式实时告警。
		★须支持本地图形化管理
		★程序自身防护，退出程序需要输入有退出权限操作的管理员/用户的密码。
2	性能指标	运行状态：正常运行状态 CPU 占用不超过 1%，内存占用不超过 10MB 固化过程，CPU 占用不超过 50%，内存占用不超过 40MB。

6、验收与攻防验证

不知攻焉知防，在方案设计和实施后，需要对整改后的风电场电力监测系统进行攻防验证，以尽可能的覆盖解决已知的安全威胁。攻防验证可以采用第三方的渗透测试、工控风险评估来完成，通过模拟黑客远程和内部恶意用户的入侵的手段和方法，测试并发掘该网络中存在的安全问题，主动地暴露整体系统在安全防护方案实施后可能存在的安全脆弱盲点和漏洞，进一步的进行消除和弥补，避免将来可能产生的经济上、生产上的损失。比如工控环境主机漏洞进一步的检测、工控组态软件漏洞分析和工控协议漏洞的识别和利用分析，弱口令探测和扫描，网络分区连接的进一步的排查，从而优化防护设施和装置的安全策略。

7、方案的创新性分析

1）全方位一体化工控系统信息安全解决方案

本项目针对风电场信息化建设环境下的信息安全保障需求，构建从管理、技术及考核三位一体的纵深防控体系，通过技术手段打通传统工控安全分区隔离技术造成的信息孤岛，形成一体化安全解决方案。

2）自主建设智能可控的信息安全保障体系

将智能黑白名单技术、智能网络安全审计技术等智能化信息安全保障技术和自主工控相关技术、自主容灾备份技术等自主可控信息安全保障技术相结合，从技术、管理、运维多个维度打造适用于风电场的新型智能可控信息安全保障系统。

3）风电场安全攻防测试。通过模拟黑客远程和内部恶意用户的入侵的手段和方法，测试并发掘该网络中存在的安全问题，事先地、主动地暴露网站所存在的安全脆弱点和漏洞，进而可以对其进行消除和弥补，避免将来可能产生的经济上、生产上的损失。攻防测试的范围包括工控环境主机漏洞检测、工控组态软件漏洞分析和工控协议漏洞的识别和利用。

8、方案实施效果

以具备大量风力发电的某公司的风电场安全整改为例，依据方案在该公司下辖 6 个风电场进行安全整改和实施，对涉及到的安全事项一一进行了整改，提供了该风电场建设系统整体安全运行能力的有力保障，同时提高设备自动化水平和人工使用效率，实现集团资源优化配置、保障电力监控安全稳定运行，减少因网络安全事故而带来的经济损失及社会负面影响，得到了用户的好评。

2.5.4 小结

长扬科技针对发电企业工控系统网络安全的设计思路充分考虑到电厂工业控制系统的业务连续性和工业特性，并且结合国家发改委的 14 号令《电力监控系统安全防护规定》、国家能源局发布《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》（国能安全〔2015〕36 号）及其附件，和工信部的《工业控制系统信息安全防护指南》，以及各电力企业针对电厂工业控制系统的相关技术要求，对全国电力系统包括风电场的信息安全体系化建设具有指导意义。

随着电力能源消耗的逐年增多，传统发电对生态环境带来的恶劣影响，为保护自然生态环境，光、风、地、气等各种清洁无污染的新能源面临着广泛并网的趋势，《电力信息系统安全等级保护实施指南》也将于 2019 年 7 月开始正式实行，该指南在技术和管理能力两方面均提出了更详尽的要求。本项目作为新能源板块的工控安全示范项目，不仅满足了示范性、合规性的需求，极大的保障了风电场信息系统的安全运行，具有在新能源领域复制和推广的价值。

2.5.5 单位基本信息

长扬科技（北京）有限公司是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、西安、重庆、武汉、济南等 15 个省市设置分支机构和服务中心。公司目前拥有 150 余人的团队，具备强大的技术研究和攻关能力，并在能源、电力、交轨等多个行业、领域积累了丰富的场景化应用经验，是我国工控安全防护事业第一批践行者。

公司产品及业务聚焦工业网络安全及安全大数据领域，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。已推出安全防护类、监测审计类、漏洞扫描挖掘类、安全检测工具类、工业终端安全类、安全态势感知及工业大数据等七大产品线。公司产品及方案通过人工智能技术赋予了客户在网络和业务两个层面的安全防护能力，实现空间、时间两个维度上的安全大数据分析及态势感知，为客户建设立体式工业互联网安全防护保障体系。

公司是国家信息安全漏洞库技术支撑单位；已通过 ISO9001 质量管理体系、IEC27001 信息安全管理体系等一系列管理体系认证；拥有信息安全风险评估、安全集成、应急处理、安全运维等系列安全服务资质。

2.6 案例六：智能工厂安全态势感知

2.6.1 方案概述

随着工业信息化的快速发展，工业化与信息化的融合趋势越来越明显，工业控制系统也在利用最新的计算机网络技术来提高系统间的集成、互联以及信息化管理水平。未来为了提高生产效率和效益，工业互联网网络会越来越开放，而开放带来的安全问题将成为制约两化融合以及工业 4.0 发展的重要因素。

为了应对工业控制网络发展和开放所带来的各类安全隐患，以生产运行安全规范为基础，不影响生产业务正常运行的工业互联网安全态势感知系统建设显得迫在眉睫。

2.6.2 典型安全问题

工业互联网工控安全和传统 IT 安全有着明显区别：

工控网络相对隔离；操作系统老旧，很少更新补丁；基本不安装杀毒软件；以专用软件为主，类型数量不多；信息交互多通过 U 盘实现；安全漏洞较多，易受攻击。

传统网络与互联网相通；操作系统新，频繁更新补丁；杀毒软件是标配；办公软件为主，类型数量繁多；信息交互主要通过网络实现；安全漏洞较少，防护措施完善。

相比于传统 IT 安全基于 TCP/IP 传输协议，工控安全协议众多：TCP/IP、Modbus、IEC103、ICE104、OPC、RS-232、RS-485、Siemens 7、Pofinet、Profibus、Ethernet 等。

工控安全性能是实时需求，响应时间紧迫；适度吞吐量可以接受，但是无法容忍高延迟和/或抖动。

一个典型工控系统包括办公网、生产网和控制网。办公网包括 ERP 等应用

系统，从实时数据库读取数据；生产网主要指 MES 系统区域，通过 OPC Server 从控制网中采集数据，保存到实时数据库中；控制网通过传感器等对生产现场进行控制。

当前工业互联网面临安全主要包括以下几个方面：

1）办公网和自动化系统网络通信安全风险

- ✧ 网络中攻击流量、异常流量和协议非法指令无法感知；
- ✧ 工控网络内部服务器/主机与自动化系统网络连接安全风险；
- ✧ 网络流量明文传输；
- ✧ 数据传输缺少正确性校验，数据包存在被篡改风险。

2）工控环境服务器和主机安全风险

- ✧ 操作系统系统漏洞（ DCS 服务器、MES 服务器、上位机）；
- ✧ 服务器开放服务漏洞（SSH、VNC、FTP 等）、服务器、主机开放不必要的端口和服务；
- ✧ DCS、MES 应用软件漏洞，上位机组态软件安全漏洞；
- ✧ 应用程序缺少白名单管理，存在非法进程和线程注入等安全风险。

3）自动化系统安全风险

- ✧ 自动化操作系统安全漏洞（XP、Linux、VxWorks 等）；
- ✧ SCADA/PLC 软硬件系统安全漏洞、自动化 HMI 软件安全漏洞；
- ✧ 自动化数据采集端口、API 接口安全风险；
- ✧ 自动化系统 USB 移动介质使用安全风险（病毒木马、内部违规）。

4）现场运维安全风险

- ✧ 现场运维缺少操作审计，运维操作行为风险；
- ✧ 运维操作涉及的移动介质使用安全风险；
- ✧ 相关人员安全意识匮乏。

2.6.3 安全解决方案

当前工业互联网安全挑战是多维度的，安全范畴包括网络通信安全，数据安全，控制安全和设备安全等。

网络通信安全威胁主要面向工厂内网安全，常见的通信层安全威胁包括物理

攻击、网关节点捕获，传输截获，传输窃听，传输篡改，传输伪造，Dos 攻击，重放攻击，完整性攻击，Sinkhole 黑洞攻击，Wormhole 虫洞攻击，HelloFlood 攻击等；面对通信层安全威胁，主要应对措施是边界隔离方案，包括使用 NGFW，NGIPS，ACG，WAF，LB，Anti-DDoS，工控安全网关，隔离网闸，网站安全检测中心等；

数据安全威胁主要是面向生产管理数据安全，生产操作数据安全，内外数据交互安全以及商业数据和用户数据泄漏、丢失、篡改等，经过跳板入侵、内部入侵等对系统造成侵害；针对数据及工业云安全威胁应对方案包括使用堡垒机，数据库审计，云安全整体解决方案，对网站、数据库、终端等进行漏洞扫描等。

控制安全威胁在针对控制器漏洞，控制协议漏洞，配置错误，凭证管理不足造成侵害；应对方案是深入挖掘漏洞，使用漏洞扫描，安全设备管理平台等进行漏洞的即时发现和管理。

设备安全威胁主要针对感知设备（各种仪表、传感设备等）和执行设备（生产和加工设备）进行攻击，相应措施是实施准入控制、网络授权、用户管理、视频监控等。

在新华三杭州智能工厂，针对当前工业互联安全问题，我们部署安全态势感知分析平台，在防护基础上加强网络流量/行为监测分析能力，提升安全威胁事件发现和处置水平。

方案架构图如下：

图 16 安全态势感知系统

本方案包含安全数据采集、安全态势感知系统和云端安全能力中心。

安全数据采集对象包括各安全设备、网络设备、计算存储设备和工业设备的日志数据信息，具备对网络流量数据和相关业务系统的数据采集；数据采集面向生产网和办公网，对相关设备的日志数据和以及网络流量数据进行安全、可靠、连续采集；日志数据采集器具备对异构日志过滤、归并和标准化处理能力；流量探针具备网络流量还原分析能力，包含对网络流量中协议还原、应用识别、文件还原和异常流量检测等；还具备对网络资产和服务进行发现和定义。

安全态势感知系统基于大数据架构的流式计算和批量计算，对预处理后数据进行实时分析和批量分析；结合系统中各个分析引擎进行分析，针对威胁信息和安全事件进行应急响应处置；从资产风险、未知威胁发现、异常流量、攻击溯源、等保合规等各个业务维度来分析和呈现整体办公和生产环境的安全态势。

云端安全能力中心提供云端威胁情报碰撞，特征库升级，提供对本地检测能力补充，并对本地安全检测进行更新和升级。

整体方案提升智能工厂综合安全能力，在安全防护基础上，对威胁监测和漏洞挖掘进行多维度监测和防护。针对性阻止网络非授权访问，阻止网络层网络攻击；发现 APT 等网络攻击，发现病毒传播，发现生产安全异常并及时处置；支持取证分析和溯源分析，防止终端病毒；深入发掘系统漏洞并提供漏洞补丁，从工业控制系统的安全生命周期角度做到对工业控制系统全方位安全监测，从边界防护深入到纵深防御，结合 AI 分析并对未知威胁检测，通过安全态势感知进行风险把控，全网协同联动处置，最终发展到全面综合预警，综合提升工业控制系统所面临的安全威胁的防护能力。

多维度展示工厂安全态势；

图 17 安全态势示例

2.6.4 小结

1）先进性及创新点：

1. 工业协议深度解析，兼容市面主流环境下通讯协议，提升工业互联网环境下的数据感知能力；
2. 黑白名单机制：智能学习生成白名单和黑名单规则，结合黑名单规则/白名单统一规则部署。黑名单包括工控设备漏洞、工控协议漏洞、工业以太网漏洞、工控系统漏洞等；白名单包括多种工控协议和传统协议白名单，建立边界通信的“白名单”、网络监测“白名单”、应用程序“白名单”、以及建立基于“白名单”的工业主机防体系；
3. 工控漏洞攻击特征库：内置千条工控安全漏洞攻击特征库；
4. 提出工业互联网环境下的智能 AI 引擎，提升对风险分析、威胁防护能力；
5. 实现云网端协同联动，提升工业互联网环境下对风险威胁的联动处置能力；

2）本方案具备以下能力：

1. 该系统在工业互联网环境下具备工业控制系统协议识别、深度分析、合规性审核能力；
2. 具备工业互联网安全审计和异常流量监测能力；具备基于大数据分析的安全态势感知能力；
3. 提供工业互联网网络安全风险的实时告警、设备运行状态实时监测，并根据生产控制网络的安全态势及时调整和部署安全策略；
4. 提供工控网络资产可视化管理，动态识别非法接入设备，直观展示工控网络安全威胁；
5. 提供网络、终端、通信、数据、运维、管理等多个层面完整安全防护与管理手段，实现工控网络全面的安全保护；
6. 最小干扰原则：所有安全组件均采用非侵入式安全监测与防护工作方式，可确保将设备对工控网络的干扰降低到最低；

3）系统价值：

价值 1：实时网络监测，保障正常生产；多厂家海量安全数据收集与解

析；多维度关联分析，快速定位风险威胁；多维度多视角实时展示安全态势；多环节协同防御，闭环安全问题；对网络数据、事件进行实时监测、实时警告，帮助客户实时掌握工业控制网络运行状况；根据监测结果，提供防御策略建议，帮助客户构建适用的专属工业控制网络安全防御体系。

价值 2：提高运维效率，降低维护成本；通过丰富的管理功能，友好的用户界面，人性化的统计报表，极大的提高企业工业互联网安全管理的效率，使企业工业互联网安全管理简单易行。

价值 3：易安装、易使用；一体化设计，旁路接入，不影响工控网络运行，提供成熟的多点部署方案，可集中监控多个网段（依赖于具体的网络架构）。

价值 4：网络安全审计，便于历史追踪；对网络中存在的所有活动提供协议审计、流量审计，生成完整记录便于客户进行事件追溯。

2.6.5 单位基本信息

紫光旗下新华三集团（简称“新华三”）是业界领先的数字化解决方案领导者，致力于成为帮助客户业务创新、数字化转型可信赖的合作伙伴。新华三拥有计算、存储、网络、安全等方面的数字化基础设施整体能力，能够提供云计算、大数据、数字化联接、信息安全、安防、物联网、边缘计算、人工智能、5G 在内的一站式、全方位数字化平台解决方案，以及端到端的技术服务。同时，新华三也是 HPE®品牌的服务器、存储和技术服务的中国独家提供商。

在数字经济新时代，新华三坚持“应用驱动，融绘数字未来”的核心技术战略，以技术创新为发展引擎。目前，新华三的研发人员占比超过 50%，截至 2019 年 7 月底，专利申请总量超过 10,332 件，其中 90%以上是发明专利。

植根中国，新华三始终以客户需求为导向，深耕行业三十余年，提供场景化客户化解决方案，支持运营商、政府、金融、电力、能源、医疗、教育、交通、互联网、制造业等各行各业数字化转型实践。服务全球，产品广泛应用于近百个国家和地区，尤其是欧洲和北美市场，客户包括沃达丰、西班牙电信、瑞士电信、可口可乐、梦工厂、法国国铁、俄罗斯联邦储蓄银行、三星电子、巴西世界杯等。“融绘数字未来，共享美好生活”，这是新时代信息技术发展的远景，也是新华

三作为数字化解决方案领导者屹立于数字经济时代的全新企业愿景。面向未来，新华三将以推动数字经济发展为目标，与合作伙伴一道共创人人悦享的美好。

2.7 案例七：智能工厂工业网络安全集中监测与态势感知

2.7.1 方案概述

制造业是实体经济的主体，是国家安全和人民幸福安康的物质基础。随着《中国制造 2025》的全面部署推进，智能制造已日益成为制造业发展的重大趋势和核心内容。以智能制造为主攻方向，推进我国信息化和工业化深度融合，成为实施制造强国战略的必然选择。

为了紧随国家战略，某集团全面启动了智能工厂建设工作，提升工厂整体技术水平和制造实力，加速全球化推动。目前，某集团完成 5 大产业线多个工厂的智能化改造，建成沈阳冰箱、郑州空调、佛山洗衣机、黄岛中央空调、胶州空调、青岛热水器等多个智能互联工厂。智能工厂集智能化生产和大规模定制化平台于一身，采用模块化、自动化、数字化、智能化为基础的全生态互联体系，包括内网互联、信息互联，外部需求信息直接互联到内部生产线，生产线根据需求进行产品生产的实时优化。

2.7.2 典型安全问题

随着智能工厂的建设，工厂的智能化自动化程度越来越高，导致工业控制系统从封闭走向开放，生产网、办公网与互联网互联互通。网络的互通互联造成了生产网络规模越来越大而复杂，因此网络威胁和安全风险也在不断增加，发生网络安全事故造成的损失也越来越大。其安全风险主要包括以下几方面：

厂区间跨地域网络互通：全国各厂区之间网络专线互通，形成一个大的“局域网”，易造成病毒在厂区间横向传播感染，而且难以定位、追溯。

厂区内各区域边界不清：不同区域的网络冗余互联，生产网和办公网边界不清晰，不同的业务、设备混在一起，风险高、难管理。

区域通信缺乏监测手段：对于 IT 网络之间、以及从 IT 网络到 OT 网络的通信流量，缺乏监测手段，当发生恶意流量时无法实时感知。

生产过程缺乏审计手段：对于工控系统生产过程中各工艺流程之间的数据交换、组态变更、协议通信、数据采集、远程维护等缺乏必要的感知监测手段，无法及时发现问题。

工控系统资产缺乏有效管理：工控系统的资产数量、工作状态不清楚。无法监测资产之间通信的流量，无法及时定位非法接入、幽灵资产、失陷主机。

因此，由于智能工厂网络互联互通、网络规模大、复杂程度高，它所面临的安全威胁是多层面、复杂多样的，安全威胁的影响范围和带来的损失也更大。仅仅依靠传统的网络隔离、访问控制、入侵检测等单一的技术，已不能满足安全需求。需要的是新的技术，即将传统 IT 检测技术和工业 OT 检测技术有机结合起来，充分理解工控系统生产业务，将传统的信息安全理念与工业安全业务相融合。做到及时发现网络中的异常事件，实时掌握网络安全状况，将之前很多时候亡羊补牢的事中、事后处理，转向事前自动监测预警，降低网络安全风险，提高生产网络整体安全水平。

2.7.3 安全解决方案

经过针对某集团全国多个厂区的调查，智能工厂网络结构大致分为核心层、汇聚层、接入层三层星型网络。核心层：由核心交换机、路由器组成。负责厂区内部各区域的数据交换以及外网出口；汇聚层：由工业汇聚交换机、无线控制器组成；负责区域内部网络分组之间的数据交换；接入层：由工业接入交换机、办公网络接入交换机、无线 AP 组成。负责网络分组内部各主机、设备之间的数据交换；工控生产所需的 SCADA 和 MES 系统部署在单独的数据中心；接入层网络由多个交换机组成的环形网络，PLC 控制器部署工业生产接入交换机，PLC 多采用西门子、三菱、欧姆龙等品牌。

综合以上信息，在厂区内部署工业安全监测系统（ISD），对工业网络中的 IT 和 OT 流量进行综合实时的监控，通过资产发现管理为主线，动态监测厂区网络的安全状况。部署方案如下：

在核心交换机部署一台工业安全监测系统，负责对办公网、生产网、数据中心以及互联网之间的数据监测；选取 PLC 分布较多、关键工艺和生产过程密集区域的接入交换机位置部署工业安全监测系统，监测工控系统生产过程的各种工控

资产、指令、操作、数据；

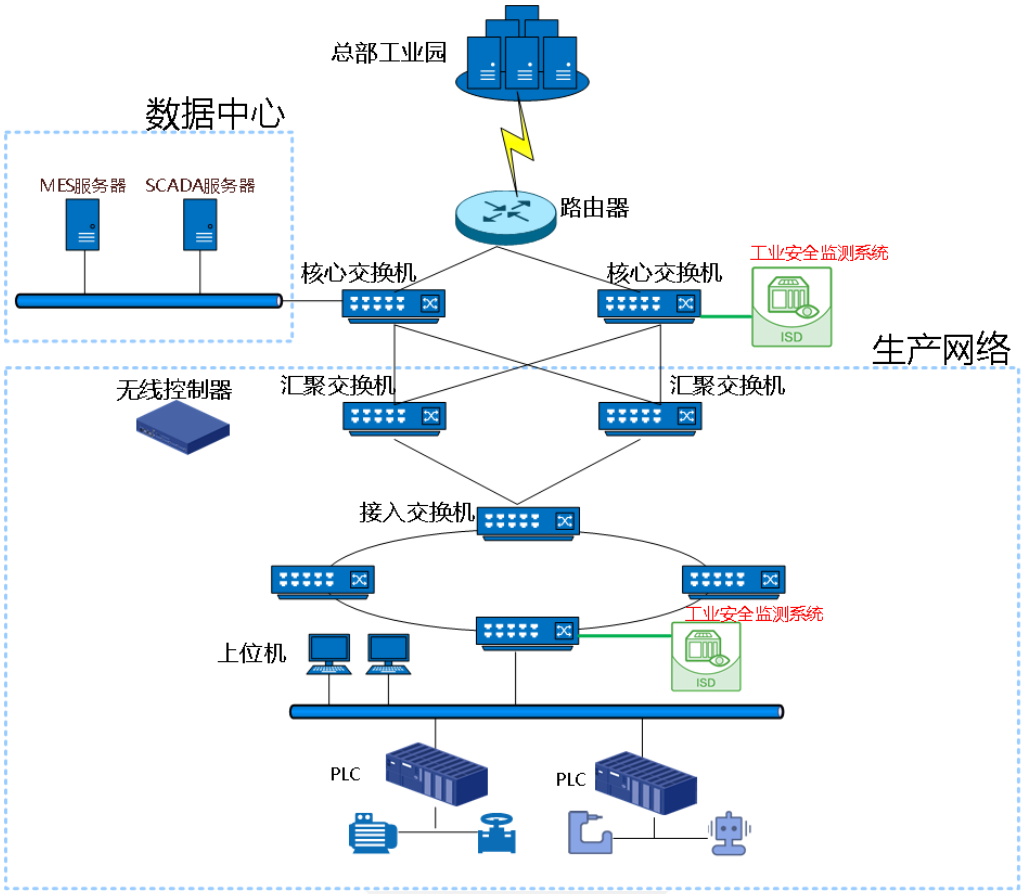


图 18 工业安全监测系统部署方案图

同时，为了满足某集团总部对各厂区集中监测、集中分析的需求，在集团总部部署工业安全监测控制平台（ISDC）。通过工业安全监测系统（ISD）数据自动上报的机制，将各厂区的监测结果实时上报集团总部，实现全面数据汇总、统一监测、集中分析。

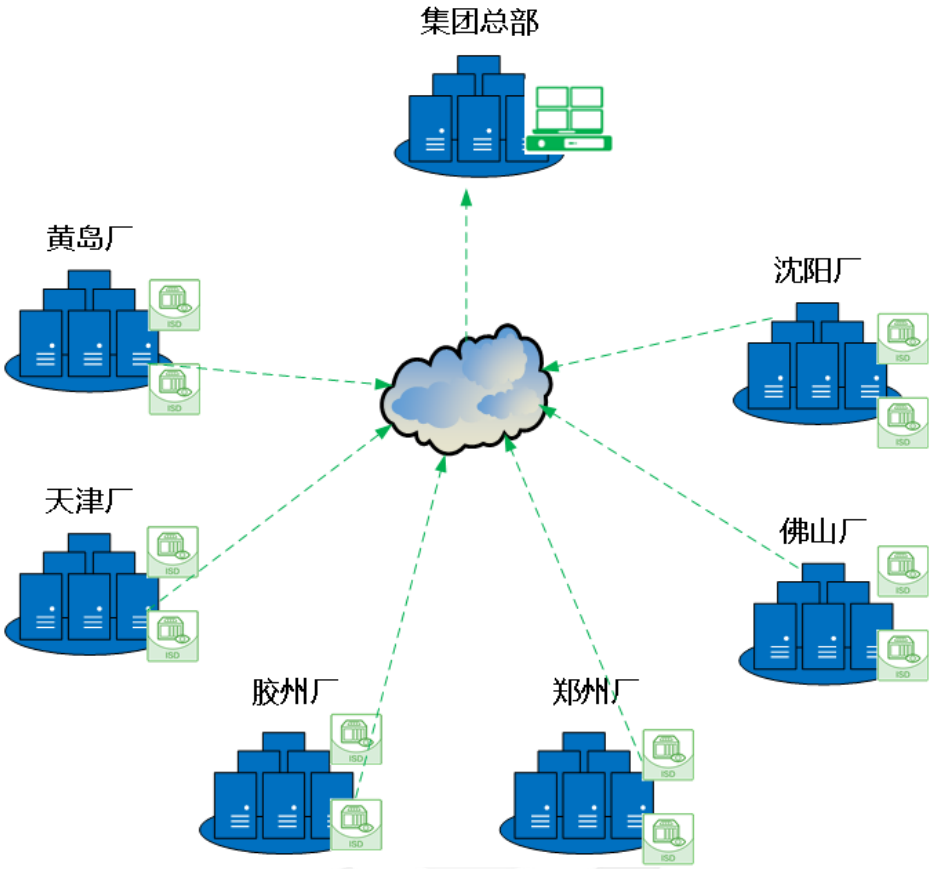


图 19 数据上报部署方案图

通过“智能工厂”工业安全监测系统及控制平台的部署和成功实施，帮助某集团实现了智能工厂内网 IT 和 OT 流量的一体化同时监测，实现集中监测与态势感知；帮助企业解决了不同区域工厂的难以进行统一安全监测的问题；为某集团提供了安全管理的抓手，帮助企业进行安全预防性维护、应急响应和事故调查。

方案创新点

（1）以“大数据分析”为核心的威胁发现和溯源技术

大数据时代的到来为工业信息安全提供了新的技术手段，对工业企业的业务数据和安全数据进行统一管理，将工业大数据和信息安全分析技术相结合，实现对数据的采集、分析并从功能维度进行汇总、查看、统计及处置。

（2）以“积极防御”为核心的纵深防御技术

现阶段大多数企业的信息安全工作都聚焦于“架构安全”和“被动防御”，对“积极防御”和“情报”则涉及较少，本方案建设以 “情报”驱动的“积极防御”纵深防御平台，提高企业的网络安全防护能力。

（3）以“人+机器”为核心的安全运营技术

新形势下的网络安全，本质是“三人”的对抗：人与人的对抗、人与机器的对抗、人工智能的对抗。人工智能时代，机器人可以替代一切，但不能替代网络安全工程师，因为网络安全是逆向思维、是不走寻常路，而人工智能是经验的决定。只有采用“人+机器”的方法，把人的知识驱动和机器的数据驱动结合起来，才能真正做到“谁进来？做什么？拿了什么？”，从而掌控全局。

2.7.4 小结

本方案采用奇安信工业安全监测系统（ISD）和工业安全监测控制平台（ISDC）对某“智能工厂”工控系统进行集中监测与态势感知，为某集团提供了可靠有效的智能工厂监测方案，降低了安全运营成本，为其它大型智能制造企业推进工业安全监测与态势感知体系建设奠定基础，同时，为制造行业工厂转型升级树立行业标杆作用。

2.7.5 单位基本信息

奇安信科技集团股份有限公司（以下简称“奇安信”）是中国最大的网络安全公司之一，专门为政府、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，已覆盖 90%以上的中央政府部门、中央企业和大型银行，已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展了安全业务。

奇安信工业互联网安全事业部基于自身在大数据、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。

2.8 案例八：智慧港口场景下的 5G SA 安全解决方案

2.8.1 方案概述

近年来我国航运业取得了历史性成就，实现了跨越性发展。港口通常包含岸桥、轮胎吊、龙门吊、集卡等在内几百台重型机械设备，密集部署，是典型的工业作业环境。港口作业的作业效率和自动化水平，是决定港口未来竞争力和经济效益的重要因素。

5G 技术提供的超大带宽、超低时延和海量连接特性，在港口业存在较大的融合前景，将对港口基础设施、运输组织模式、商业模式、治理模式等产生深远影响。5G 港口的智慧化发展不仅将降低码头用工成本，最大限度地减少人机接触，保障人员安全，同时也将实现港口的运行高效、安全生产运营。

宁波舟山港是基于 5G SA 切片安全的智慧港口创新项目，采用了 SA 组网的 5G 切片及边缘计算等先进技术，提升港口信息化水平，降低改造建设成本、提升运营效率、确保运营生产的安全和可靠性，为港口信息化、智能化、智慧化升级发挥巨大的经济效益。针对 5G 网络中新的安全风险，从网络安全架构、 业务风控能力、数据安全量化风险控制、网络安全运维等维度出发进行分析，提出安全要求，为大规模的 5G+工业互联网安全测评、安全运维提供现网实践依据和指导，建立健全工业互联网安全技术保障体系。

2.8.2 典型安全问题

5G 处在一个开放的环境中，不仅需要保障用户与网络自身安全，还需要为垂直行业与应用提供安全能力。随着 5G 网络演进、业务演进、IT 演进， 5G 网络中引入了新的安全风险点，形成了安全新需求。主要包括：

1.CU/DU 分离、无线空口、核心网、互联互通协议等引入带来的风险；

2.5G 下出现的新形态业务包括 eMBB、uRLLC、mMTC，相关业务对网络安全提出了新需求；

3.5G 提供的安全能力开放，形成新需求；

4.基于云化的 SDN、NFV、网络切片技术安全性在现网没有商用实践，安全性

能研究有待验证。

2.8.3 安全解决方案

宁波舟山港引入 5G 高性能网络技术对港口无线网络进行高速、无线化改造，通过 5G 网络的建设与平台的部署，对作业区域内的设备信息、物流信息、运转过程信息、生产调度管理信息等进行数据采集、监控和智能化分析，在此基础上进行应用示范研究，针对 5G 存在的安全风险点，制定切实可行的网络安全防护技术方案：

（1）5G 无线安全保护机制

5G 无线安全是指 5G 终端 CPE 和 5G 基站之间无线接口(空中接口)的机密性和完整性。

加密：通过对空口数据（包括信令和用户数据）开启加密保护，通过加密算法将明文数据转换为密文数据，保证数据不被泄露，并且支持 128 位加密算法。

完整性保护：5G 网络支持信令消息和用户面数据提供完整性保护，5G 终端和 5G 基站通过完整性算法能够检测信令消息和用户面数据是否被篡改。

（2）5G CPE 接入终端安全保护机制

CPE 支持网络连接时启用防火墙，使连接 CPE 的港区龙门吊、摄像头等在享受网络服务的同时，可以预防网络安全隐患的威胁，并控制网络访问权限。支持设置 MAC 地址以限制网络访问权限，防止不安全的设备接入。

CPE 和其所连接的 PLC、摄像头等，通过 AAA 服务器进行鉴权，确保合法的应用接入。

部署支持 IPsec 功能的路由器(AR651C、AR6140-9G-2AC、ATN 905-F/ETN500-F），与部署在园区内网边界的智能防火墙（含安全网关）一起，实现 CPE 与港口园区内部网络间的端到端加密。

（3）MEC 安全防护

物理安全：根据港区业务场景，MEC 节点园区站点机房，靠近用户的现场。由于处于相对开放的环境中，MEC 设备更易遭受物理性破坏。浙江移动与港口园区一起,共同评估和保障基础设施的物理安全,引入门禁、环境监控等安全措施。对 MEC 设备安全，与华为公司联合，加强自身防盗、防破坏方面的结构设计，对

设备的 I/O 接口、调试接口进行控制。

平台安全：开展平台安全加固，加强平台管理安全、数据存储和传输安全，引入可信计算技术，从系统启动到上层应用，逐级验证，构建了可信的 MEC 平台，防止 MEC 平台的软件被篡改。通过虚拟机隔离提升虚拟化安全。对于部署在 MEC 的 VM，通过微分段（Micro-segmentation）等技术，对 VM 和不同应用实施严格隔离。另外，通过实时监测 VM 的运行情况，有效发掘恶意 VM 行为，避免恶意 VM 迁移对 MEC 造成感染。

网络安全：MEC 连接了多个外部网络，在北仑港 MEC 中，使用传统的边界防御、内外部认证、隔离与加密等防护技术。从 MEC 平台内部来看，MEC 被划为不同的功能域，如管理域、核心网域、基础服务域（能力开放）、第三方应用域等，彼此之间需要划分到不同安全域，引入各种虚拟安全能力，实现隔离和访问控制。同时内置了入侵检测功能，对恶意软件、恶意攻击等行为进行检测，防止威胁横向扩展。

运维管理安全增强：为了确保 MEC 节点中资产与数据的安全，对使用 MEC 的各方的行为执行认证(Authentication)、授权(Authorization)、审计(Audit)，此外，在平台层面、网络层面、业务层面等多个维度，对数据资产的所有权、使用权和运维权进行分权分域的管理。当 MEC 与核心域之间涉及到管理、计费等关键性通讯时，充分利用 PKI 以及 TLS/IPSec 等协议，实施认证授权与传输加密。为了确保运行版本的安全，防止带毒运行，MEC 支持针对 VNF 版本包在不同交付环节之间的签名（发布方）与验签（接收方），同时需要对发布的版本包做签名校验。为了避免安全漏洞影响到 MEC 节点上其它功能域的安全，在园区其它应用引入之前，执行严格的管控流程，对其进行全面的安全评估和检测。同时通过应用注册过程对应用权限进行控制，通过审计手段对应用行为进行问责，以规范应用的运行。

（4）切片接入安全

首先，提供用户接入切片的认证。终端接入网络时由 5G 网络接入认证来保证接入 5G 网络的用户的合法性，由北仑港股、浙江移动共同完成的切片接入认证和授权，保证接入合法切片以及园区应用对切片网络及资源使用的可控性。

其次，提供切片选择辅助信息的隐私保护。切片选择辅助信息 NSSAI

（Network Slice Selection Assistance Information）可以区分不同类型、不同用途的切片。在园区终端初始接入网络时，NSSAI 指示基站及核心网网元将其路由到正确的切片网元。切片选择辅助信息对于北仑港属于敏感信息，5G 网络可对 NSSAI 进行隐私保护。

（5）切片隔离

IT 基础设施共享、网络功能按需自动编排，是网络切片的关键技术，浙江移动按需创建和维护切片，提高资源利用效率。切片之间的隔离，一方面在保持灵活性和动态性的基础上保证了切片自身安全，另一方面为向用户提供定制化、托管式安全服务做好了铺垫。

网络切片是逻辑上“独立的专网”，但从物理资源角度看，网络切片之间共享物理资源和 IT 基础设施，每个切片以“租户”形式按需使用这些资源。切片管理器 NSMF（Network Slice Management Function）根据切片的 QoS、安全策略为各切片分配对应的服务器资源，并通过资源分配策略、虚拟化隔离等多种手段保证不同租户之间不会产生 CPU、存储、I/O 资源的竞争和滥用。

针对切片应建立三级立体化安全隔离体系，如下图所示：

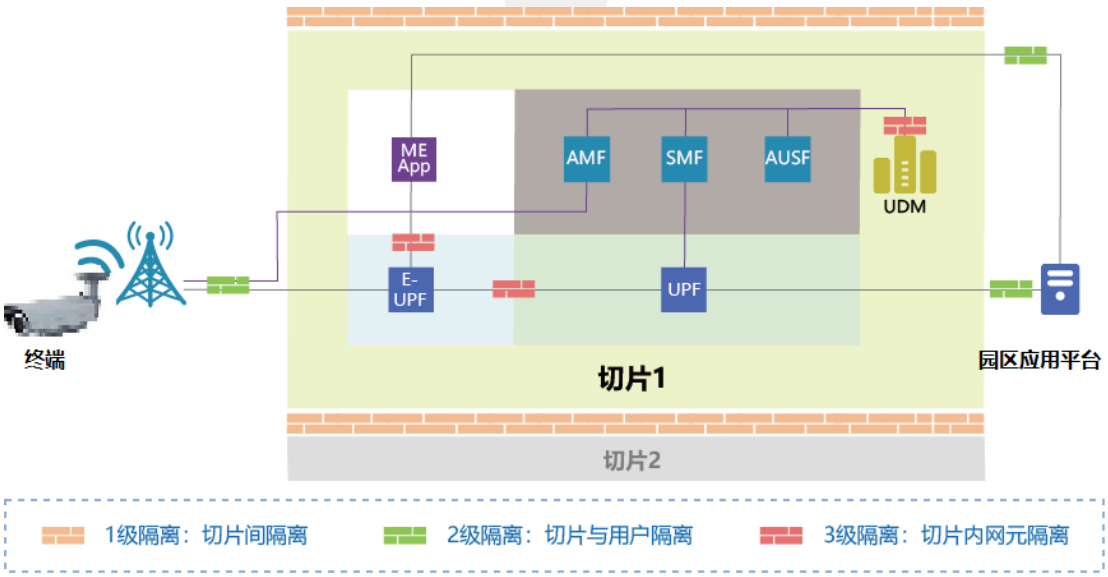


图 20 网络切片的三级立体化隔离体系示意

切片隔离体系包括：

1）切片间隔离：依据园区业务类悲哀和数据资产的重要性，进行切片间的

有效隔离，保障每个切片具有对应安全级别；

2）切片网络与用户隔离：为保障 5G 网络切片的安全、高可靠运行，在切片网络设计时，在最终用户侧、园区应用侧设置隔离机制，在按照 SLA（Service Level Agreement）向不同应用提供高可靠切片服务，保证切片网络自身安全边界清晰，确保切片网络自身的安全可控；

3）切片内网元间隔离：在切片网内划分出安全域，提供网元间安全隔离；

上述的三级立体化安全隔离体系中，每个层级的隔离实施方案均可从网元、网络、数据三个层面实施，使用成熟的虚拟化隔离方案，借助 NFV、SDN 等技术，与虚拟机编排、切片编排功能协同，实现精准、灵活的切片隔离。

（6）5G 网络和园区网络边界隔离安全

BBU 与 SA 核心网之间的安全机制。BBU 支持 ACL 访问控制策略配置，确保只有合法的信令流量才能访问北仑港园区无线接入网络。

UPF 支持 ACL 访问控制策略配置，确保只有合法的信令流量才能访问园区 UPF 网络。防火墙提供精细化访问控制策略缩小攻击面，并提供流量行为分析能力，检测恶意软件行为。

在 UPF 接入到北仑港园区内部网络的核心交换机之间部署防火墙，确保两个网络边界隔离安全。防火墙支持双机热备，对接下挂 5G CPE 设备的 IPSec 隧道，提供冗余备份能力。解密之后可以定制化提供应用感知能力，确保只有正常业务才能接入网路。防火墙还支持 APT 防御、IPS、Anti-DDoS 等功能。

方案创新点：

（1）深度融合行业基础设施开展评估实践。

宁波智慧港口是基于垂直行业的 5G 应用，深度融合园区信息化设施，5G 网络与企业内网、运营商网络互通，5G 网络安全将直接影响到行业客户的业务，对网络安全提出了更高要求。公网用户访问私网用户、运营商网络和企业网络的互相攻击和渗透，MEC 设施布置在园区，造成边缘节点增多，管理量大，安全边界多，非法物理入侵等问题都需要落实风险管控。依托 5G 智慧港口平台部署，结合 5G 网络特点及园区业务特点，开展对 5G 新功能新设施引入后面临的安全问题的探讨及评估实践。

（2）发掘新形态业务安全风险点

在保障终端安全、业务流程安全、业务内容安全、平台及软件安全、设备安全、网络结构安全的基础上，又研究了 MEC 的安全性、URLLC 的保障措施、5G 切片的安全风险、园区数据的安全保护、对公共安全的影响及应急等安全风险。此外，根据中国移动集团公司《5G 新技术新业务试点安全评估模板》对 5G 基础安全功能、5G 业务安全、终端安全、配套安全管理措施等 120 余项险识别评估，掌握安全风险点。

（3）形成总体安全防御体系

在评估实施中发现的各种安全问题，通过加强接入控制，加强访问控制等方式规避业务安全风险。在 MEC 侧部署防火墙，强制业务路由通过防火墙进行访问控制。开展机卡分离检测，将 CPE 和卡的绑定，限制 CPE 位置等方式实现 5G 网络用户接入身份认证。通过对切片的多种隔离措施实现业务端到端的安全可管可控。

2.8.4 小结

基于 5G SA 切片安全的宁波舟山智慧港口是 OCTAVE 安全框架下的 5G+工业互联网环境的业务创新。采用了 SA 组网的 5G 技术提升港口信息化水平，其平台部署为 5G 工业网络技术的应用研究与实践提供了测试和应用环境，为 5G+工业互联网环境的安全风险评估和保障提供了指导和依据，建立健全工业互联网安全技术保障体系。

2.8.5 单位基本信息

中国移动浙江公司（简称“浙江移动”）隶属于中国移动通信集团有限公司，在全省拥有 11 个市分公司，统一经营浙江省的中国移动通信网络。公司于 1997 年在全国通信行业中最早在海外（香港、纽约）上市，根据国际资本市场要求，建立和不断完善符合国际惯例的企业治理结构，成长为业绩优秀、管理出色、服务优质、行业领先的主导运营商。面向 5G 新时代，公司全力打造杭州“5G 第一城”，开通全国首个 3GPP R15 标准 5G 基站和 2.6GHz 频段 5G/4G 双模基站，建成全国首个 5G 连续覆盖体验区，打造全球首条 4.9GHz 频段 5G 网络精品线路；牵头成立浙江省 5G 产业联盟，在全国首次实现钱江潮、马拉松赛事、世界互联网大会等大型活动的 5G+8K 高清直播，开展远程医疗、无人驾驶等 5G 创新应用。

2.9 案例九：某大型能源企业态势感知系统安全解决方案

2.9.1 方案概述

某能源有限公司是某电力集团公司旗下首个产业集群，是一个集煤炭、火电、新能源、电解铝等产业一体化协同发展的大型综合能源企业。

本案例旨在研究发电厂工控系统的信息安全集中监测技术，通过对工控系统各对象流量、日志、告警的收集，基于大数据分析技术对原始安全数据的整合、分析，实现对全网整体工控安全态势的可视化展示、安全预警及知识库管理，构建电厂工业控制系统生产安全大数据分析平台，掌握电厂工控系统全网信息安全实时态势。

2.9.2 典型安全问题

目前，我国工业控制系统核心软硬件产品自主可控水平较低、安全防护能力普遍不足、网络接入控制不严格以及网络维护依赖国外厂商等问题依旧存在而且较为突出。同时我国工业控制系统的信息安全同样面临全球工业控制系统所面临的问题，包括工业控制网络设备漏洞数量仍居高位，工业控制系统安全事件呈逐年增加趋势，能源、交通运输、石化、关键制造业等成为受攻击最多的行业。电厂作为工业控制系统应用最早、最为广泛的领域之一，其生产高度依赖工业控制系统，工业控制系统安全是电厂生产安全的重要部分。

该能源公司为满足国家相关政策规定，提高自身工业控制系统安全防护水平，同时考虑到自身网络安全生产监测方面存在一定的不足，在集团侧无法有效直观的获取各厂级的网络安全态势，决定对公司及下属电厂进行安全防护建设。

2.9.3 安全解决方案

1、技术路线

采用“一个中心、三重发现”的建设理念，其中一个中心是指集团级工控安全集中监视平台，三重发现是指发现工控网络区域边界、网络通信、计算环境安全问题的能力。

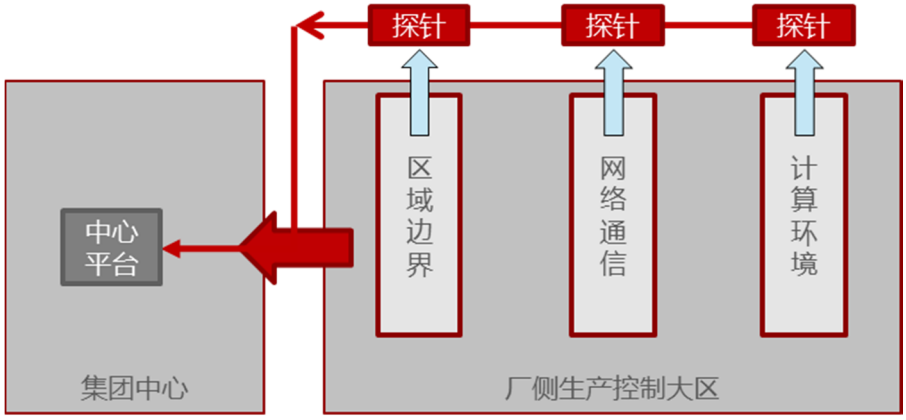


图 21 示意图

使用先进的大数据挖掘分析技术，基于各种安全数据和日志信息，通过数据分析构建工业场景的各种行为模型，实现对通用的工业控制网络和安全大数据的有效建模，构建工控安全健康指数计算方法，实现对实施安全态势的量化展示和分析。

基于对被监测对象流量、日志、告警的收集，通过多样的标准接口方式把数据上送至数据存储和分析层，基于对原始安全数据的整合、分析支撑上层应用服务如风险分析、异常检测等，最终实现对全网整体工控安全态势的可视化展示、安全预警及知识库管理。

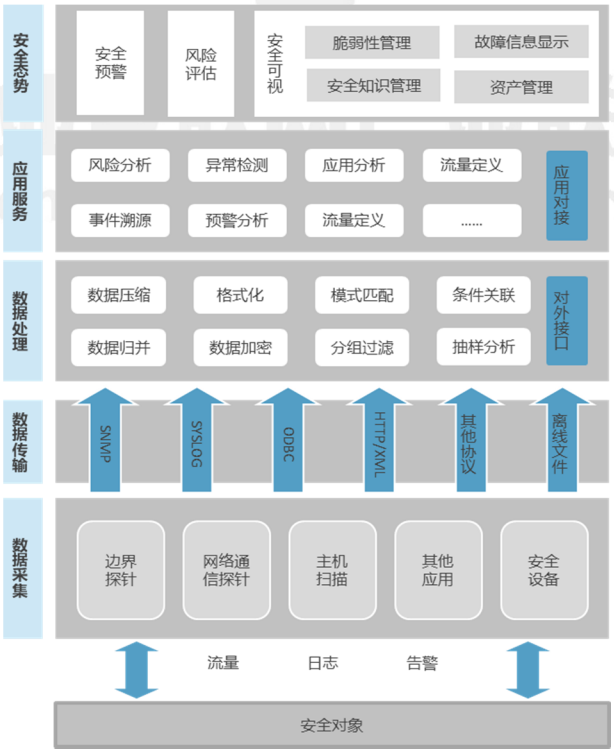


图 22 工控安全态势

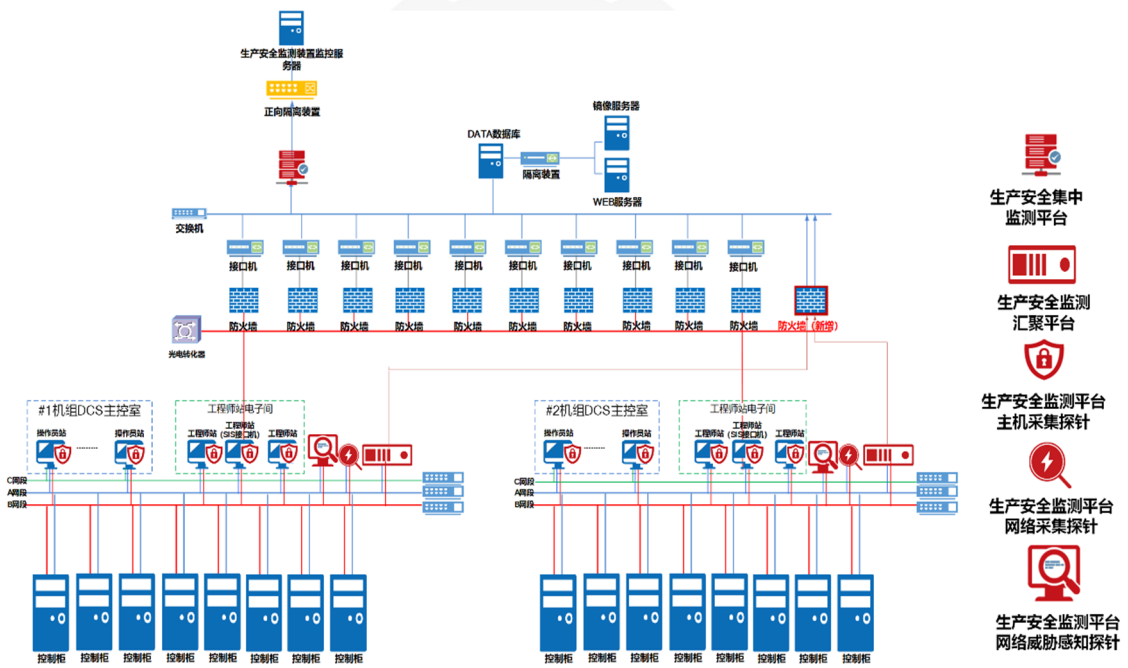
2、部署方案

部署方式：部署电力监控系统网络探针，完成区域边界和网络通信旁路监测审计。

部署电力监控系统内的探针，通过各机组 DCS 系统、SIS 系统交换机端口镜像功能旁路部署，实时采集网络内流量信息，把非法操作、非法协议、非法指令等安全事件分析结果以及后台分析的流量数据实时发送到集团侧态势感知系统内。

安全生产集中监测管理系统的采集探针逻辑架构划分为数据采集层、分析检测层。

部署示意图：



DCS 系统部署方式：

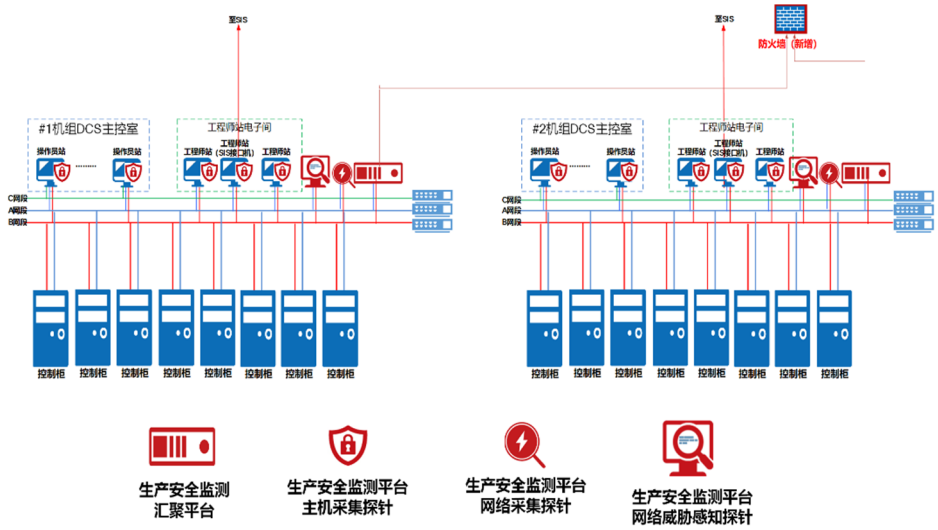


图 23 DCS 系统部署方式

通过 DCS 系统交换机端口镜像功能旁路部署生产安全监测平台网络采集探针。

在 DCS 系统的操作员站部署生产安全监测平台主机采集探针。

在 DCS 系统网络内部署生产安全监测系统汇聚平台，该平台通过新增防火墙与部署在 SIS 系统内的生产安全集中监测平台进行数据交互。

SIS 系统部署方式：

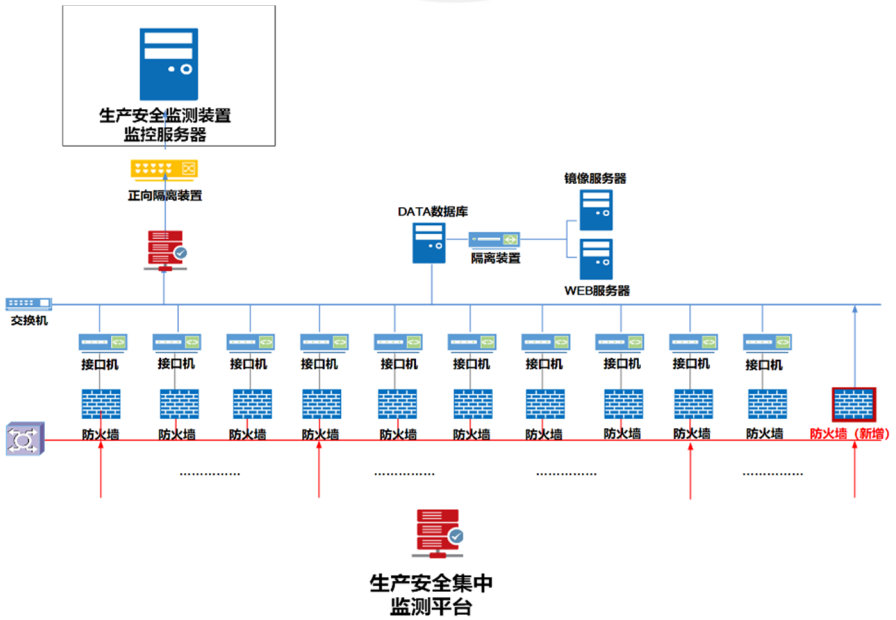


图 24 SIS 部署方式

通过 SIS 系统交换机端口镜像功能旁路部署生产安全监测平台网络威胁感知探针。

在 SIS 系统网络内部署生产安全集中监测系平台，该平台通过新增防火墙与部署在 DCS 系统内的生产安全集中监测汇聚平台进行数据交互。

信息管理大区部署方式：

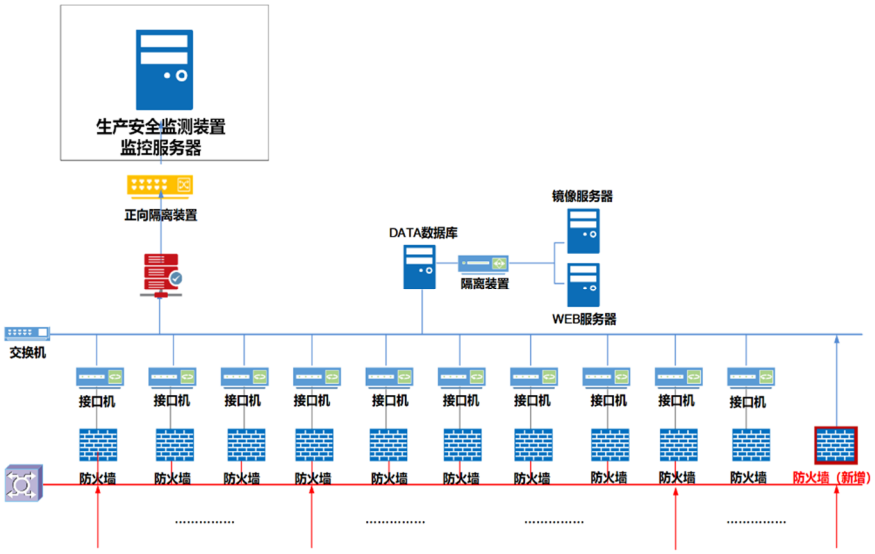


图 25 信息管理大区部署方式

部署在 SIS 系统内的生产安全集中监测平台通过正向隔离装置与部署在信息管理大区的生产安全监测装置监控服务器进行数据交换。

2.9.4 小结

结合风险分析和案例技术分析，本解决方案具备如下特点：

（1）提高工业企业生产稳定性。通过平台实施，能够有效的降低生产网络中的各种风险，提高企业生产的连续性和稳定性，有利于保障企业的安全生产。

（2）提高工业企业安全生产水平，为企业经营效益做贡献。通过平台实施，规范工控系统网络中的资产和行为，可以事前防御由病毒、入侵等导致的安全生产事故，监管集团工控系统信息安全形势，为企业安全生产做贡献，产生良好的经济效益。

（3）提高工控系统网络信息化水平。通过平台实施，能够有效的提高工业

企业网络安全任职，切实提升信息化管理水平和管理效率，使管理人员的决策更加及时、准确，使信息流通结构更加合理，增强综合竞争力。

（4）提升工业企业抵御网络安全风险能力。通过平台实施，增强工控系统网络行为的合规性识别能力，避免各种有可能出现的由网络安全引起的突发问题，避免或减少工控系统网络安全威胁。

（5）显著提升电厂工业控制系统安全防护能力，避免网络攻击事件引发电厂生产安全事件可能导致的环境安全问题，能够更好的维持电厂区域环境生态。

2.9.5 单位基本信息

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。

威努特秉承“专注工控，捍卫安全”为企业使命，以率先独创的“白环境”整体解决方案为核心，深度结合工控系统安全特点研发了覆盖工控网络安全的 4 大类 20 款自主可控产品，提供工控安全咨询、安全培训、风险评估、安全检测、安全应急、安全建设及运维等全流程服务。拥有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，智能制造及军工等五百余家国家重点行业客户提供了全面有效的安全保障，赢得客户一致好评。

威努特作为工控安全领域的领军企业，拥有多项核心知识产权，是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，多次受邀为中共十九大、两会、“一带一路”、G20 等多项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，得到了中央网信办、公安部、国安部、工信部、国防科工局等国家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，积极推动与众多主流设备厂商构建安全产业生态，为“中国制造 2025”保驾护航，为建设网络强国添砖加瓦！

2.10 案例十：油气田生产基础网络的安全防护平台建设

2.10.1 方案概述

某油气田公司集油气勘探开发、油气集输和销售以及与之配套的矿区服务业务于一体，是我国首个天然气年产量超百亿立方米的大气区，首个以生产天然气为主的千万吨级大油气田。公司协调推进油气核心、矿区服务两大业务，大力实施资源、创新、人才三大战略，不断推进科学发展上水平，进一步履行好经济、政治、社会三大责任，为建设综合性国际能源公司和区域经济社会发展做出贡献。

为保障油气田的安全生产运营，综合考虑油气田 SCADA 的特点，建立自动化生产系统的安全加固与主动预警的安全防护体系，从网络层、主机层、系统层、应用层和管理制度等多方面进行主动式威胁管理，提高油气田整体网络安全防护等级，保证油气田 SCADA 系统的稳定有序运行。

2.10.2 典型安全问题

油气田作为国家重要的关键基础设施，两化融合提高油气田生产效率的同时，也使油气田面临网络威胁：

1）通用病毒浸入：病毒通过网络、USB 口或服务商服务过程方式侵入系统。

2）黑客恶意攻击：如：敌对势力、不法分子、对企业不满者等，通过远程修改控制策略、修改测控参数等手段攻击。

3）客服恶意植入：如：敌对势力、不法分子、对企业不满者，恶意植入危险秩序，造成工艺装置发生事故，或停产损失。

4）企业信息被盗：企业重要信息被恶意窃取，影响企业经营或国家利益。

2.10.3 安全解决方案

本次生产网安全体系建设核心思想可总结为：“垂直分层、水平分区、边界控制、内部监测、全局管理”。

“垂直分层、水平分区”即对工业控制系统根据分公司生产网的业务属性垂直方向化分为四层：现场设备层、现场控制层、监督控制层、生产管理层。水平

分区指各层级单位的系统之间应该从网络上隔离开，处于不同的安全区。

“边界控制，内部监测”即对各系统边界即各操作站、工业控制系统连接处等要进行边界防护和准入控制等。对工业控制系统内部要监测网络流量数据以发现入侵、业务异常、访问关系异常和流量异常等问题。

“全局管理”即通过各层级安全信息、网络信息、终端信息的收集加强全局监控管理，提高信息的统一性、集中性。并通过收集的数据进行安全风险预警，安全事件溯源。

2.10.4 小结

1）先进性和创新点

本次项目符合当前国家对工业互联网安全市场战略发展需要，带动了工业互联网安全防护与监测产品、系统的研发与市场化，更可以带动自主可控、基于国产化组件的工业互联网安全产品的研发与市场推广应用，并形成工业互联网安全产品和服务的增值业务，也是对整个工业互联网安全产业，尤其是能源方面的基于安全运营思维的网络安全主动防御技术与研究得到了有力实践验证。

2）实施效果

本次项目的实施完成具有直接的经济效益，避免了几年行业内频发的网络安全勒索事件导致 SCADA 停产导致超过的经济损失等类似重大工控事件，本次项目的顺利建成，能够为石油石化行业的网络安全运营及其业务安全稳定运行提供了有力的安全保障，产生了巨大的间接经济效益，避免出现网络攻击事件造成直接的经济损失。

2.10.5 单位基本信息

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，是国内极具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。目前，启明星辰已对网御星云、杭州合众、书生电子进行了全资收购，自此，集团成功实现了对网络安全、数据安全、应用业务安全等多领域的覆盖，形成了信息安全产业生态圈。

2.11 案例十一：某智慧矿山工业安全运营中心解决方案

2.11.1 方案概述

随着国家对中国制造 2025 和智慧矿山的持续发力，在矿山开采建设过程中自动控制技术、信息技术、智能设备、机器人等高新科技的广泛应用，矿山网络建设从封闭走向开放，工业控制系统产品越来越多地采用通用硬件、软件和协议，以及云计算，大数据技术，并且企业以各种方式与互联网等公共网络互连。随之而来的是病毒木马、网络入侵、APT 攻击等网络安全威胁迅速向工业控制网络扩散，矿山工控网络安全问题日益突出。

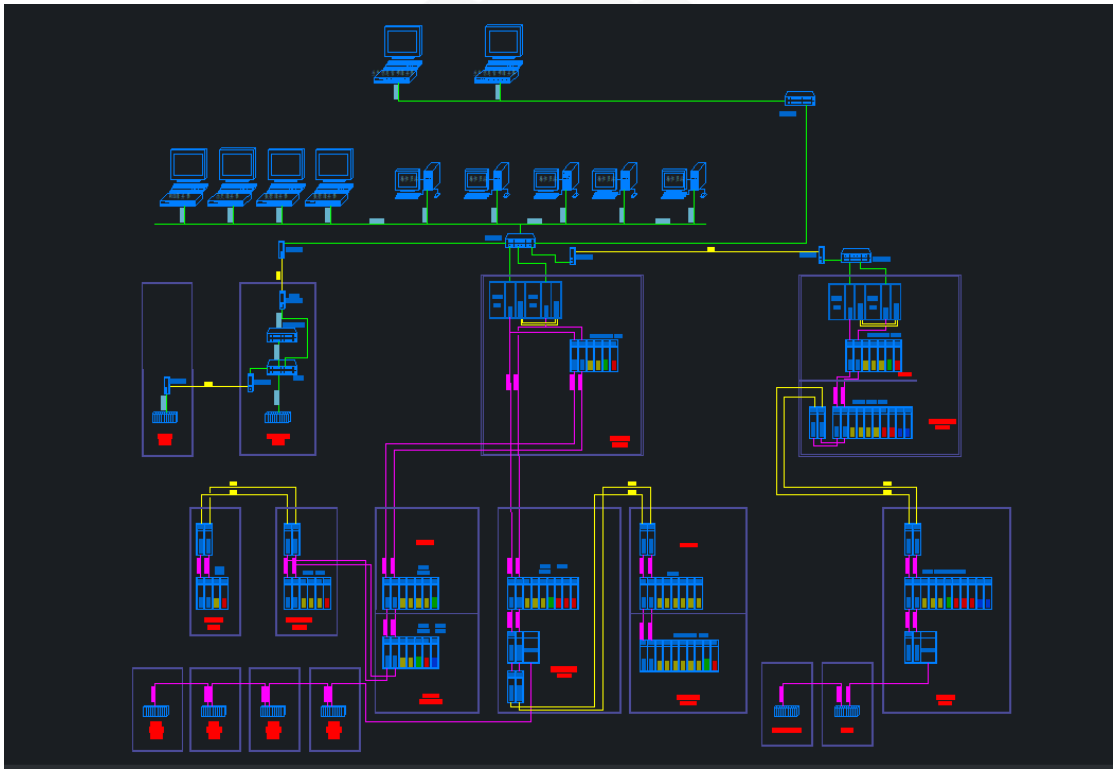


图 26 某矿山网络示意图

2.11.2 典型安全问题

1） 工控安全无管理抓手，在集团内网缺少安全分析与管理工具，难以实现资产统一管理、威胁态势呈现，及时掌握工业控制系统安全状态、风险隐患的实

时感知、精准研判和科学决策，全天候感知工业资产安全态势。

2） 工业主机安全管理不到位，存在黑客利用或病毒恶意软件感染的风险。主要体现在工业主机未封闭 USB 接口，甚至仍然存在移动存储介质使用。工业主机的账户密码以文件形式存储在主机上并向网络共享，账户密码为弱口令且为厂商初始设置，大量工业主机使用过期的、缺少补丁的 windows 操作系统。

3） 工业控制网络未做横向隔离，存在病毒或恶意软件感染痊愈风险。虽然工业控制网络与管理网之间通过部署单向网闸实施了纵向隔离防护，但工业控制网络中的各 FRR 域之间可以互相访问，未进行横向隔离。

4） 工业控制网络没有安全监测手段，难以及时发现攻击，违法操作等恶意行为。工业控制网络中未部署工业安全监测设备，不能及时发现病毒/木马传播，可和攻击引起的网络异常。

5） 重要工控设备前端未部署工业防火墙设备，一旦工业控制网络被攻破，工业控制设备可能面临直接攻击。工业主机、工控控制网络层面的防护可以在较高程度上可以避免攻击达到工控控制设备。

2.11.3 安全解决方案

根据矿山企业安全管理的需求和网络的特殊性，通过安全运营中心的建设实现信息安全的全方位保证。矿山安全运营中心主要由工业安全运营管理平台、工业主机防护设备、隔离防护设备、工业流量探针组成。

工业安全运营管理平台是支持主被动两种方式，全面感知资产和威胁的工业企业安全业务工作平台。该平台利用探针类设备、工业互联网扫描器、防护类设备等工业安全设备，收集资产、漏洞、威胁、异常行为等信息，帮助矿山企业安全管理人员进行工业资产管理、威胁分析、应急响应和统一运维。通过资产拓扑可视化进行资产拓扑画像，以资产为核心实现资产脆弱性和威胁事件态势可视化，基于威胁信息实现事件处置和应急响应，为安全人员提供安全管理抓手，降低事故风险，协助应急处置，整体提升工业企业的安全保障水平。

工业安全防护设备及隔离防护设备通过单体主机、局域网、环网、互联网多维度全面覆盖矿区安监专网、工控生产网、视频专网、管理网、办公网等网络，

全方位保证生产安全。

工业流量探针通过对工业网络数据的全面检测和分析，实现网络资产、漏洞、病毒等数据的全面管理。

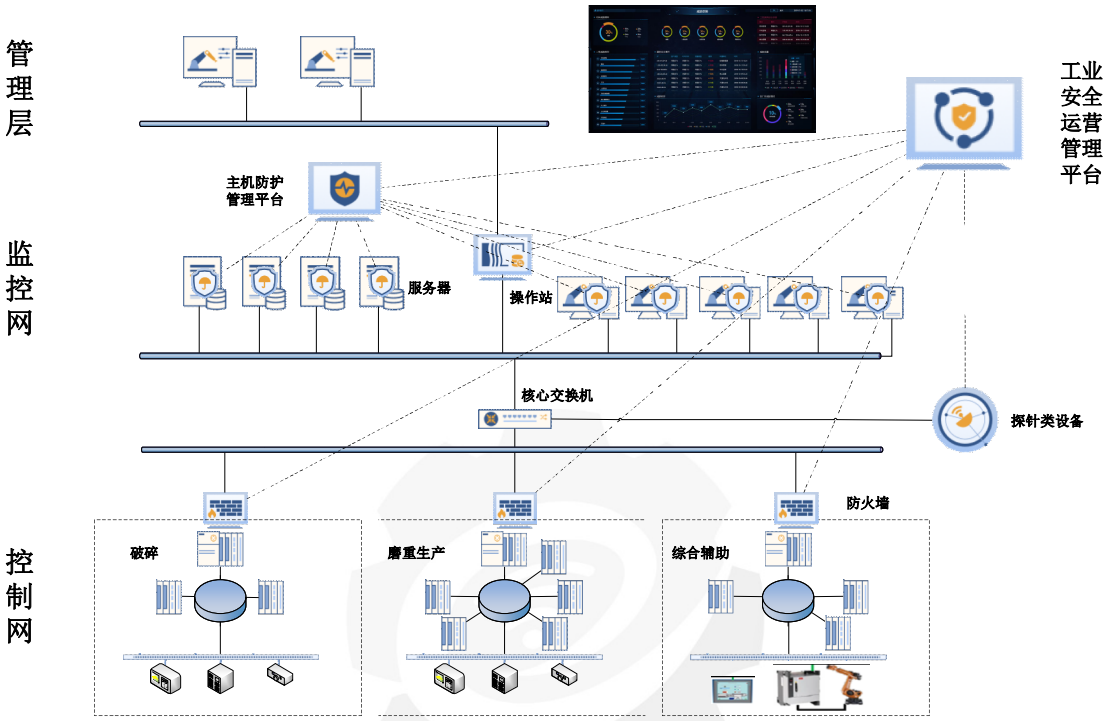


图 27 矿山工业安全运营中心部署示意图

1） 安全运营管理平台

安全运营管理平台（ISOC）部署在工业企业网络中的管理信息层，平台接各种安全设备数据，接收各层探针类设备、主机防护设备的数据，工业互联网扫描器管理节点汇总的资产和资产漏洞数据及其他工业网络安全设备上报的数据。

安全运营管理平台核心特征：

➢ 多维的数据采集与分析：资产数据、安全事件数据、 流量数据，安全设备数据

➢ 灵活的开放平台：灵活集成和快速定制，实现第三方设备数据接入

➢ 直观的可视化呈现：采用数据可视化技术，2D/3D，趋势图，关联图等对数据直观展示；

➢ 全面的资产管理：实现多源数据收集资产基本信息，行为信息，状态信息，连接关系等统一管理；

- 安全管理中心构建，确保安全设备统一管理、日志统一审计和安全合规。

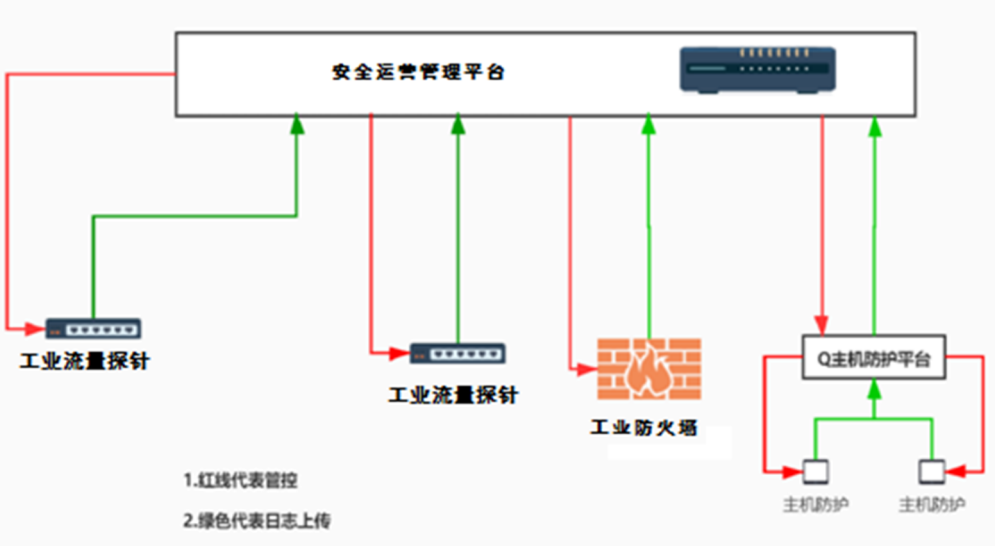


图 28 安全运营管理平台部署示意图

2） 工业主机安全防护

随着近年来针对工业控制系统的 APT 攻击增加，工业控制系统内部网络安全问题的严重性也逐渐增加。因此对控制系统内部操作员站、服务器、工程师站以及生产信息系统主机等工业主机的防护已成为工业控制系统安全的基础环节，可为控制系统提供基础的防御与保护。

工业主机安全防护核心特征：

- 白名单管控机制，为工业生产打造纯净运行环境 。
- 三重关卡拦截，全方位病毒防护。
- 资产自动发现，轻松掌控全网主机清单 。
- 主机安全加固，提升工业软件核心参数的访问权限 。
- 工业主机集中管理，降低运维成本。

3） 工业防火墙安全域划分及隔离

根据国家工控信息安全建设相关标准，对企业工业控制网络及生产信息网络从纵向、横向两个方面进行安全域分区设计。工控网络安全域分区设计的基础上，采用工业防火墙对各安全域边界进行隔离保护，对跨安全域的防护进行监控，阻止非合规访问流量通过边界。

工业防火墙安全域划分及隔离的主要作用：

- 边界防护与隔离，阻止非授权访问，防止安全事件扩散。
- 工控协议深度防护：完整性、功能码、 地址范围及读写权限、工艺参数。
- 安全规则精准发现及非法数据和异常行为防御，屏蔽未经授权访问。
- 对数控网络进行实时监控与分析，提供实时告警和阻断等多种响应方式。
- 对重点系统、重点设备制定有效的防护策略进行综合防护。

4） 工业流量探针

工业安全监测主要通过部署工业流量探针实现。工业流量探针是基于流量分析能力的全面探查工控网络威胁的探测器。采用标准接口将威胁事件数据推送给本司的工业安全管理平台，同时平台可对工业威胁探测器进行管控。

工业流量探针核心特征：

- 工业流量实时监测，及时掌握安全状况。
- 工控网络异常检测，保障生产连续性。
- 自动资产发现，监测非法外联。
- 自动匹配资产漏洞，识别安全风险。
- 网络通信记录回溯，提供调查依据。
- 网络威胁发现，及时威胁告警。
- 网络安全审计，生成完整记录。

2.11.4 小结

根据某智慧矿山企业工业控制系统现阶段的安全现状，结合企业安全运营管理的需求。智慧矿山工业安全运营中心安全解决方案，实现边界防护、主机安全、网络监测、统一管理，让工业安全管理成为一种智能的可监控、可管控、可追溯的技术化工作，真正为管理者提供方便的操作与管理手段。

2.11.5 单位基本信息

北京双湃智安科技有限公司致力于保护数字化转型时代下工业资产、运营和人员免受网络安全威胁，凭借超过 15 年的网络安全和工业领域专业知识和应用经验，为客户提供创新的网络安全服务、产品和解决方案，帮助工业互联网和关

键基础设施运营方对任务关键性网络提供 360 度全方位的防护。

2.12 案例十二：卷烟厂工控安全解决方案

2.12.1 方案概述

2011 年，国家烟草专卖局印发了《国家烟草专卖局办公室关于卷烟工业企业信息化建设的指导意见》(国烟办综[2011] 212 号)，明确了构建智能化工厂、建设信息化企业的主要任务。近几年，***卷烟厂在进一步构建一体化“数字烟草”，推进烟草行业的“两化融合”过程中，以太网技术与工业控制网络技术的融合程度逐渐加深，工业控制网络和企业管理网业务信息数据交换的关联性也越来越紧密，工业控制信息系统的机密性、完整性，特别是可用性保障问题也成为***卷烟厂目前需要解决的问题。

针对***卷烟厂的工业控制网络安全现状，通过针对工业控制系统安全风险评估和安全产品部署相结合，通过专业的工控安全防护产品以提升***卷烟厂工控系统的安全检测和防护的能力。使***卷烟厂工业控制系统安全防护能力显著提升，进而逐步实现安全技术能力、安全管理能力的全面提升，实现管、控、防一体化。

2.12.2 典型安全问题

2.12.2.1 网络与通信层面

（1） 安全域架构设计缺失

目前部分卷烟生产企业由于建厂时间较早，最初生产网网络规划设计的时候没有考虑网络互联互通产生的通信安全问题，也没有考虑安全域的设计思路，或者安全域设计不合理，导致企业管理网与生产网之间，生产网内部各生产车间中控之间，都缺失明确的安全边界的界定，内部数据的传输没有得到合理的访问控制，这可能会导致生产网及管理网的业务系统、生产系统、工业控制系统和生产数据未经授权的访问、病毒感染，生产业务拒绝式服务攻击等安全风险。

（2） 生产网与管理网之间安全隔离机制不合理。

管理网办公人员需要了解底层生产设备的运行状态信息，及时掌握生产工艺各流程的运行状况、工艺参数的变化、实现工艺的过程监视与控制；所以需要通过 MES 系统对生产控制系统进行管理。在这个过程中，多数卷烟生产企业都没有严格且有效的安全管理机制，以防止管理网对生产控制系统的非授权访问和滥用（如业务操作人员越权操作其他业务系统）、失误操作、篡改指令、违规操作等行为。

（3） 控制指令数据通信明文传输

目前多数卷烟生产企业均没有针对数据传输的加密机制。不管是管理网内部数据通讯，还是生产网内部通讯，以及管理网 PC 与生产网数采服务器之间通讯、上位机与 PLC 控制器的通讯之间都是明文数据传输。特别是目前常见的工业控制协议来控制生产设备时传输的各种指令信息都是采用明文方式（如 ProfiNet/ProfiBus、ModBus、DNP3 等），易被攻击者窃听和解析。

（4）生产网无线网络管控机制缺失或不完善

由于多数卷烟生产企业在设计网络架构的初期，并没有考虑到无线网络将在卷烟生产过程中的广泛应用，因此也没有针对于无线网络的统一部署和管控。而在车间内部通常由于生产业务需要，会采用无线网络接入技术作为现有生产网络的延伸。然而在搭建无线网络的时候，往往仅考虑生产业务的可用性，而针对无线客户端和接入点的安全认证措施往往都被忽略（甚至存在免密码直接接入生产网），这样生产网无形当中多了一条对外的不安全网络出口，安全隐患极大。

（5）网络设备安全性配置不完善

生产网的网络设备大多是由车间系统管理员管理（非安全管理员），网络设备配置基本都是保持出厂默认。存在很高的网络设备被未授权访问或被攻击的风险。甚至造成生产网络的瘫痪。

（6）工业控制安全审计机制缺失

没有对工业控制网日常运行维护人员的操作行为进行统一运维审计管理，对于人为原因造成的卷烟生产业务异常事件无法溯源，也无法找到事件发生根本原因，最终无法对事件进行定性分析。

2.12.2.2 控制器、主机及应用层面

（1）工业控制系统自身存在大量漏洞

目前烟草行业工业控制系统使用比较主流的品牌是 Siemens S7 系列 PLC、Rockwell AB PLC 以及 GE PLC，依据绿盟科技去年发布的《2014 年工业控制系统安全研究与实践报告》的描述，工业控制系统公开漏洞所涉及的工业控制系统厂商占比中，Siemens（28%）、通用电气 GE（7%）与 Rockwell（5%）三者漏洞数总共超过 40%。

（2）关键生产设备 HMI 身份认证机制不完善

部分卷烟生产企业生产车间工业控制系统 PLC 前端现场操控触摸屏 HMI 是登陆身份认证机制不完善，弱口令情况普遍存在，甚至还有无认证机制完全开放的运行状态，同时缺失监管及监控机制，导致相关联的生产设备有可能被越权操作。

（3）工程师站、操作员站和监控终端缺乏安全加固机制

一般在卷烟生产企业，工程师站、操作员站以及监控终端均为 Windows 系统，运行多年没有系统打补丁机制。由于操作员站计算机可以直接向工业控制系统下达生产指令、监控生产设备状态，系统存在大量安全漏洞有可能导致被攻击的风险大大增加（如获取权限后，可以任意下达控制指令）。

（4）关键生产设备组件、工程师站、操作员站及监控终端远程运维操作

对于关键工业控制系统 PLC 的运维、检修工作，一般都是本地化操作，但是部分生产企业安全隔离机制不完善，导致具备被远程访问操作的可能性。比如使维护工程师和厂商获得远程访问系统的能力，应该加以安全控制，以防止未经授权的个人，通过远程访问接入到生产网。

（5）工程师站、操作员站及生产网业务系统服务器缺乏恶意代码检测机制

在部分卷烟生产企业，由于工程师站、操作员站和监控终端计算机工业控制应用软件与防病毒软件存在兼容性问题，因此不安装，给病毒与恶意代码传染与扩散留下了空间。

而对于数采服务器和 Web 发布服务器，由于担心影响到生产可用性，也存在未安装防病毒软件的现象。即便部署了防病毒软件，病毒库也常年未更新。

（6）工程师站、操作员站和监控终端系统身份认证机制不完善

部分卷烟生产企业为了日常运维的便利性，中控室操作员站及监控终端都采用公用账号（甚至是系统默认账号），且系统操作界面长期处于开放状态，没有

配置登陆超时锁定功能。导致进出中控室的所有人员都可以对其进行操作，可能存在被无关人员访问操作员站进行未授权操作的安全风险。相当于对车间 PLC 控制器可随意操作，且发生安全事件无法追溯责任人。

（7）生产网 IP 地址网段划分不合理

部分卷烟生产企业生产网办公计算机与生产业务服务器规划在同一 IP 网段，导致有可能出现生产网第三方计算机 IP 地址与生产业务服务器 IP 地址冲突，导致系统中断的安全风险。

（8）生产网移动设备管控措施不完善

部分卷烟生产企业针对工业控制网络生产设备，没有采用物理封闭 USB 接口的机制，且生产网员工 USB 移动存储介质管控机制不完善，导致生产网存在被病毒感染的安全风险。

另外，不安全的移动维护设备（比如笔记本等）的未授权接入，也会造成木马、病毒等恶意代码在生产中的传播。

（9）业务系统、数据库账户权限设置不合理

生产执行系统（MES）作为卷烟生产企业核心业务系统，系统登陆账户都是根据员工岗位区分角色及系统权限。但是多数卷烟生产企业员工权限申请流程执行不好，比如车间员工电话向信息管理部门系统管理员申请，系统管理员联系厂家现场运维人员更改账号权限。缺失申请审批记录。也有车间员工直接向业务系统原厂运维人员电话申请，无需任何流程确认审批，权限即刻开通。这样对于卷烟生产业务会造成极大的安全隐患。

另外对于生产车间数采服务器，部分企业未区分登陆账号划和权限，或者登录账号和初始密码都是默认账号，并且没有设置密码保护策略。攻击者可获得数据库权限，可任意破坏、篡改生产数据库。

（10）关键设备的配置文件没有存储备份措施

对于生产网中关键设备配置文件没有进行存储与备份机制，无法防偶然事故的发生，比如防止员工误操作，或者攻击者对配置文件进行更改，造成生产业务中断或生产数据的丢失。

2.12.3 安全解决方案

当前***卷烟厂共有动能车间、卷包车间以及三个自动化库共五个车间，车间内部通过环网连接各 PLC 设备，车间汇聚均为千兆光纤网络，因此在核心交换和工业生产网汇聚之间串接部署工控安全隔离装置，实现生产网和管理网的物理隔离；在每个车间汇聚交换机和工业生产交换机之间串接方式部署工业安全网关，实现针对每个车间内部的 PLC 设备的安全防护；在工业生产汇聚交换机通过旁路方式部署工控漏洞扫描系统、工控安全审计系统、工控入侵检测系统，对工控网络主机资产进行漏洞管理和加固、工控协议的安全审计和工控入侵行为检测；详细拓扑图如下所示：

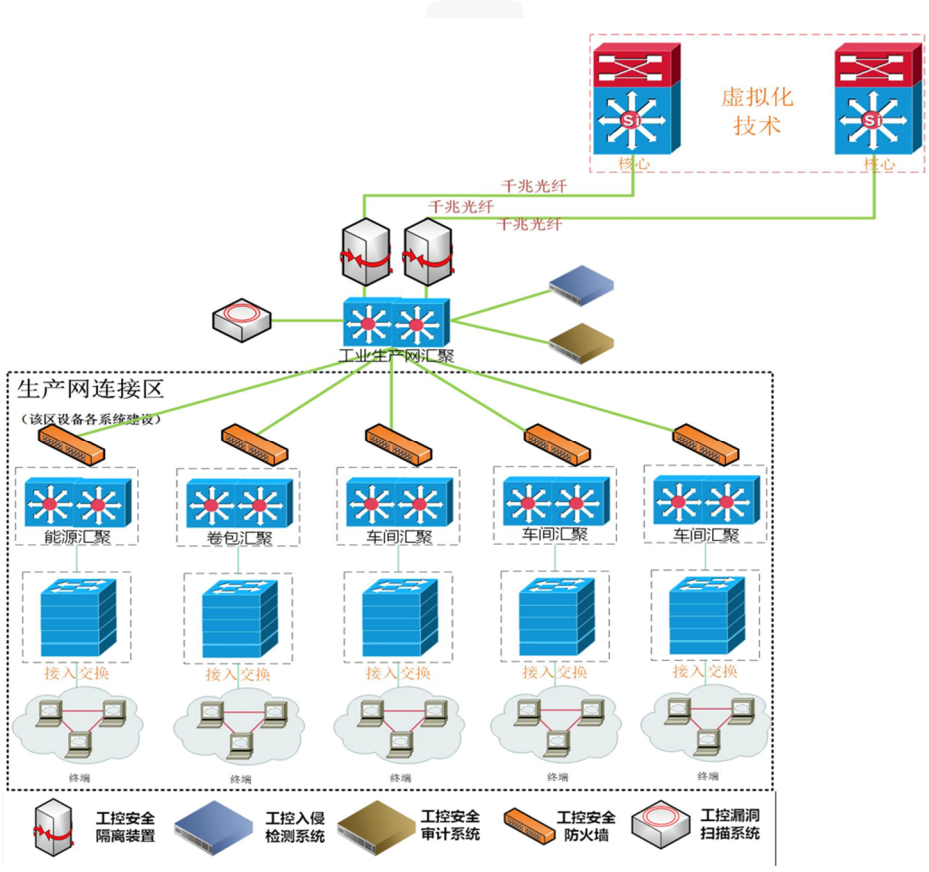


图 29 部署示意图

通过绿盟工业安全隔离装置、绿盟工业安全网关、绿盟工控入侵检测系统、绿盟工控漏洞扫描系统、绿盟工控安全审计系统的集成部署使***卷烟厂的工业控制网络能达到网络入侵检测、工控网络边界防护、工控网络纵深防御的防护效果，可以对工控安全设备进行灵活管理，对工业控制网络现状进行及时监控，对工控安全事件及时分析并采取措施，使公司运维管理人员能实时了解工控网络的

网络现状和安全现状。具体的安全防护能力如下：

2.12.3.1 工控网络边界防护

（1）管理网社生产网物理隔离

将两台绿盟工业安全隔离装置冗余部署在生产网和管理网之间，实现生产网与管理网安全隔离作用，满足了《烟草工业企业生产网与管理网网络互联安全规范》的合规性要求。绿盟工业安全隔离装置作为控制网络与信息网络之间的安全隔离设备，其核心是工业网络隔离技术的应用。工业网络隔离技术是硬件与软件相结合来完成的。工业网络隔离技术在物理层采用了两个独立高性能嵌入式主机，双主机之间采用基于总线通信的隔离卡实现两个安全区之间的非网络方式的数据交换；数据链路层和应用层采用私有通信协议，数据流全部进行 128 位加密处理，在保证安全隔离的前提下，实现数据的高速交换。通过物理硬件和软件逻辑的共同作用，彻底截断了穿透性的 TCP 连接，同时实现对工业协议数据的定向采集和转发，达到数据完全自我定义、自我解析、自我审查，传输机制具有彻底不可攻击性，从根本上杜绝了非法数据的通过，确保控制网络不受攻击和入侵。

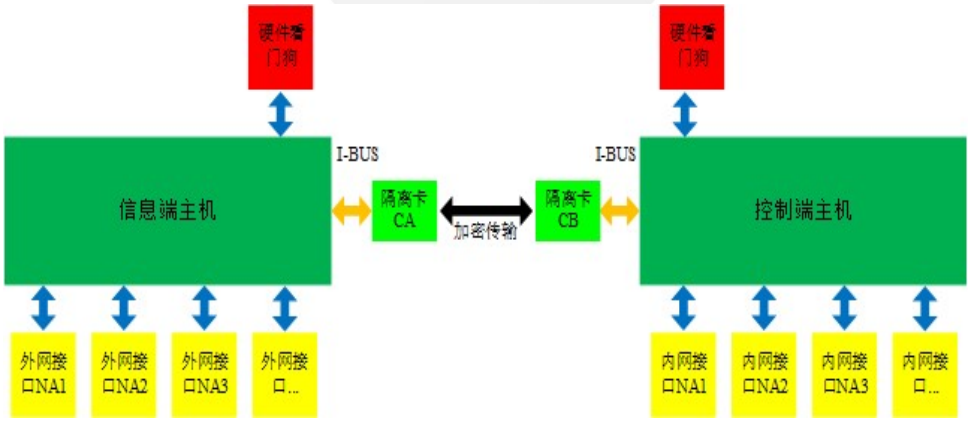


图 30 示意图

（2）双数据摆渡

通过测点管控模式和隧道管控模式两种数据摆渡模式。测点管控模式针对工业现场数据通信需要，提供测点数据的解析和安全保护；隧道管控模式使用自主开发的安全数据传输方式支持数据库、视频等常规 IT 流量等更为多样化的网络环境中的数据摆渡。

（3）工业网络通信协议的深度过滤

绿盟工业安全网关不但可以针对工业网络协议进行基本的访问控制，而且可以针对工业网络协议的内容和数据进行细致的合规性检查。例如：绿盟工业安全网关的 Modbus 协议管控模块可以针对 Modbus 协议的设备地址、寄存器类型、寄存器范围和读写属性等进行检查。通过类似的管控模块能有效的防范各种非法的操作和数据进入现场控制网络，最大限度地保护控制系统的安全。

2.12.3.2 工控网络安全监测

（1）工控协议识别

绿盟工控入侵检测系统支持 ModBus TCP、 IEC-60870-5-104、C37.118、OPC UA、profinet、DNP3 等协议的解析和识别，解析内容包括源目的 IP、源目的端口、协议名称、协议内容等。

（2）工控入侵检测

绿盟工控入侵检测系统可以对 PLC 等控制设备的拒绝服务攻击漏洞（CVE-2013-2784）、缓冲区溢出攻击漏洞（CVE-2014-0768）等典型工控漏洞的攻击行为进行有效识别，并产生告警信息。绿盟工控入侵检测系统提供基于流的应用识别技术，可准确识别非标准端口应用、以及 HTTP 协议隧道中 Web2.0 应用，发现隐藏在应用中的攻击行为。绿盟工控入侵检测系统能够基于敏感数据的外泄、文件识别、服务器非法外联等异常行为检测，实现内网的高级威胁防护功能。

（3）工控安全审计

针对不同客户在审计工控中的需求，绿盟工控安全审计系统对于基于 IEC 60870-5-101、102 和 104 协议、IEC 61850、MODBUSRTU 和 PROFINET 等工控协议的操作指令进行有效的识别，定义了其中存在的高危操作，能够及时进行报警。如对于变电站侧的 SV 报文，能够发现其中存在的采样值的变化情况，如发现采样操作超过了预定义的 3000HZ 的频率，会发出相关的告警。用户也可以根据实际的工程经验，在系统界面中进行配置。

2.12.3.3 工控资产安全管理

（1）工业控制系统拓扑自动生成

在部分工业控制系统环境中，由于系统使用者和系统管理者很有可能分属于

两个部门，所以没有相关人员对工业控制系统进行过资产的梳理，拓扑的更新等操作，并且由于工控设备大多数部署在工控现场，可能位于不同机柜甚至位于不同的地区，在进行工业控制系统资产梳理和拓扑编制的过程中存在较多困难点。针对此种情况，绿盟工控漏洞扫描系统具有工业控制系统拓扑自动生成功能，能够对所在工控系统进行拓扑的自动生成操作，并支持后期人工修改，界面美观，操作方便。

（2）基于串行总线的漏洞扫描

绿盟工控漏洞扫描系统具有对使用串行总线接口设备的漏洞扫描能力，使得漏洞扫描产品可以与基于 RS232，RS422，RS485 通讯接口的工控设备进行通讯，加上漏洞扫描产品对工控协议的支持，实现了对基于 RS232，RS422，RS485 串口的老式工业总线设备的漏洞扫描。

（3）轻量化无损漏洞扫描

为了实现对工业控制系统完全的无害评估，绿盟工控漏洞扫描系统独家采用了无损扫描技术，通过对支持的工控资产进行梳理和信息收集，绿盟工控漏洞扫描系统可以实现远程，非接触式的安全评估。在不影响业务的前提下完成漏洞扫描。

（4）可视化的工控风险展示

通过采用了更具实效性的仪表盘技术，从不同的角度展示设备风险及趋势。

- 包含资产整体的风险值、资产分析趋势图
- 包含主机风险等级分布、资产风险分布趋势
- 能够可视化的显示当前资产的风险值及过去一段时间的变化趋势

（5）工控漏洞管理流程

建立工控漏洞管理流程，包括漏洞预警、检测、结果分发、修补、验证的闭环管理流程。

图 31 工控漏洞管理流程

2.12.4 小结

本方案为***卷烟厂工业控制系统信息安全管理平台建设提供了解决方案，在保证生产运行的情况下，通过改造逐步实现生产过程的安全可控。逐步完善工业控制系统的安全防护措施，使***卷烟厂工业控制系统安全防护由安全策略的部署向安全能力的部署迁移，逐步实现安全技术能力、安全管理能力的全面提升，实现管、控、防一体化。安全能力逐步覆盖系统上线、系统运行、系统运维、系统检修等各个环节，实现工控系统安全的闭环管控。

2.12.5 单位基本信息

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技或公司），成立于 2000 年 4 月，总部位于北京。绿盟科技在国内设有 40 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。

3. 结束语

“编制优秀试点示范推广案例集”是工信部 2020 年推动工业互联网加快发展的工作方向之一。本报告从工业互联网安全的优秀实践层面，响应国家的决策部署，着眼于新技术融合带来的安全问题以及固有的安全风险，汇编了业内优秀安全解决方案，为工业企业提供安全建设参考。

本报告面向 5G+智慧港口、边缘计算等新技术场景提供优秀安全实践，同时涵盖电力、轨道交通、油气等重要行业的安全解决方案，以及安全态势感知平台、安全防护平台的建设方案，与案例汇编 1.0 和 2.0 共同丰富工业企业安全最佳实践。

未来，工业互联网这一新兴基础设施建设将向更广范围、更深程度、更高水平不断推进，助力经济发展新动能，推动产业升级。新基建中 5G 与工业互联网的融合发展乘数效应显著，5G+工业互联网也将加档提速，渐行渐近。

安全，作为工业互联网建设的重要组成部分之一，将不断面临新的挑战，新的安全解决方案也会不断诞生。唯有安全行业与工业行业互相协作，攻坚克难，深耕工业互联网安全，协同打造安全的工业互联网，才可共同促进工业互联网的繁荣与发展。