中国移动 China Mobile

工业互联网产业联盟 Alliance of Industrial Internet

工业互联网典型安全解决方案案例汇编

（2023年）

牵头编写单位：中国移动通信有限公司

工业互联网产业联盟（AII）
2024年6月

工业互联网产业联盟
Alliance of Industrial Internet

工业互联网典型安全解决方案案例汇编

（2023）

牵头编写单位：中国移动通信有限公司

工业互联网产业联盟（AII）

2024 年 6 月

声　　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他文献的内容除外），并受法律保护。

如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

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。自 2018 年以来，工业互联网已连续六年写入工作报告，可见国家层面对工业互联网发展的重视程度。从 2018 年“发展工业互联网平台”首次写入政府工作报告；2019 年政府工作报告明确提出“打造工业互联网平台，拓展‘智能+’，为制造业转型升级赋能”；2020 年提到发展工业互联网，推进智能制造；2021 年提出要发展工业互联网，搭建更多共性技术研发平台，提升中小微企业创新能力和专业化水平；2022 年提出要加快发展工业互联网，培育壮大集成电路、人工智能等数字产业，提升关键软硬件技术创新和供给能力；2023 年指出支持工业互联网发展，有力促进了制造业数字化智能化。

目前，我国工业互联网已步入发展的关键时期。为了促进工业互联网产业安全的发展，2023 年国家相关部门相继出台一系列政策，保障工业互联网行业安全，但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，算力网络、5G、边缘计算、区块链、隐私计算、量子计算等新技术与工业互联网技术的融合暴露面持续增大，安全场景更加复杂，为工业互联网安全带来新的挑战；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了案例汇编工作，为工业互联网的安全建设提供样板与示

牵头编写单位：

中国移动通信集团有限公司

参与编写单位：

中兴通讯股份有限公司

杭州安恒信息技术股份有限公司

北京亚鸿世纪科技发展有限公司

中国联合网络通信有限公司研究院

中国移动通信集团广东有限公司

浙江木链物联网科技有限公司

北京炼石网络技术有限公司

中移（上海）信息通信科技有限公司

卡奥斯化智物联科技（青岛）有限公司

北京天融信网络安全技术有限公司

工业互联网产业联盟公众号

范的优秀案例。通过案例征集，组织专家评审，最终评选出 10 个优秀案例汇编入《工业互联网典型安全解决案案例汇编(2023)》。本报告汇编了有关 5G 智慧工厂、汽车制造、智慧水务等场景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。

编写组成员（排名不分先后）：

张峰、柯皓仁、陶耀东、李江力、王雨晨、于乐、马禹昇、马娟、刘晓曼、闫霞、付超、李雅璇、王国宇、徐嘉伟、仲冰、徐高峰、白小愚、古元、林飞、柳兴、贠晓雪、梁锐彬、郭文润、雷东琦、韩一名、钱晶、唐双林、王轩轩、吴天宇、符盛、宋锐、田晓扬

目 录

1. 工业互联网安全概述

1.1 工业互联网安全形势

自 2018 年以来，工业互联网已连续六年写入工作报告，可见国家层面对工业互联网发展的重视程度。从 2018 年“发展工业互联网平台”首次写入政府工作报告; 2019 年政府工作报告明确提出“打造工业互联网平台，拓展‘智能+ ’，为制造业转型升级赋能”；2020 年提到发展工业互联网，推进智能制造；2021 年提出要发展工业互联网，搭建更多共性技术研发平台，提升中小微企业创新能力和专业化水平；2022 年提出要加快发展工业互联网，培育壮大集成电路、人工智能等数字产业，提升关键软硬件技术创新和供给能力；2023 年指出支持工业互联网发展，有力促进了制造业数字化智能化。

工信部数据显示，全国“5G+工业互联网”项目超过 8000 个，相较于 2022 年的 4000 个项目，数量显著增加。我国已培育 50 家跨行业跨区域（双跨）工业互联网平台，相比 2022 年的 28 家，增长近一倍。预计 2023 年中国工业互联网产业增加值贡献规模将达到 4.69 万亿元。

近年来，国家持续重视工业互联网安全，并发布多项政策文件，其中:

2020 年 3 月，工信部印发《关于推动工业互联网加快发展的通知》，明确提出要健全安全保障体系，包括建立企业分级安全管理制度、完善安全技术监测体系、健全安全工作机制、加强安全技术产品创新等。

2021 年 1 月，工信部发布《工业互联网创新行动发展计划（2021-2023 年）》提出到 2023 年底，工业互联网与安全生产协同推进发展格局基本形成，工业企业本质安全水平显著增强。6 月，《中华人民共和国数据安全法》审议通过，明确了采用数据分类分级保护制度对数据进行安全保护，有助于工业企业对重要数据的安全防护有的放矢，消除工业企业用户对数据安全的顾虑。7 月，工信部等十部门联合印发《5G 应用“扬帆”行动计划（2021-2023 年）》，明确重点推进 5G 在工业互联网等领域的深度应用。8 月，国务院公布《关键信息基础设施安全保护条例》，明确关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重。

2022 年 5 月，工信部发布《工业和信息化部办公厅关于开展工业互联网安全深度行活动的通知》（工信厅网安函[2022]97 号），涉及分类分级管理、政策标准宣贯、资源池建设、应急演练、人才培训、赛事活动等 6 项内容。2022 年 7 月，国家互联网信息办公室公布《数据出境安全评估办法》，自 2022 年 9 月 1 日起施行，旨在落实《网络安全法》《数据安全法》《个人信息保护法》的规定，规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，切实以安全保发展、以发展促安全。2022 年 9 月，工信部印发《5G 全连接工厂建设指南》。其中，安全方面指出，结合生产安全需求，围绕设备、控制、网络、平台和数据等关键要素，构建多层级网络安全防护体系;做好安全应急预案，阶段性开展安全检测评估，提升网络安全监测水平，确保网络运行平稳，提高安全威胁发现、快速处置和应急响应能力。

2023 年 5 月，由工业和信息化部、国家标准化管理委员会联合印发《工业领域数据安全标准体系建设指南（2023 版）》，旨在推动工业领域数据安全的技术引领和规范指导，依据《中华人民共和国数据安全法》等法律法规和政策文件要求。2023 年 9 月，全国信息安全标准化技术委员会发布了《网络关键设备安全技术要求 可编程逻辑控制器（PLC）》国家标准的征求意见稿，该文件明确了将可编程逻辑控制器（PLC）纳入网络关键设备范畴的相关规定，涵盖了设备标识安全、冗余、备份恢复与异常检测、漏洞和恶意程序防范、预装软件启动及更新安全、用户身份标识与鉴别、访问控制安全、日志审计安全、通信安全和数据安全等方面的安全功能要求，以及相应的安全保障要求。11 月，工业和信息化部发布《关于组织开展 2023 年工业互联网试点示范项目申报工作的通知》（工信厅信管函〔2023〕319 号），该通知提出了工业互联网试点示范项目的申报工作，包括安全类项目。同月工业和信息化部发布《“5G+工业互联网”融合应用先导区试点工作规则（暂行）》和《“5G+工业互联网”融合应用先导区试点建设指南》，旨在指导各地积极有序开展“5G+工业互联网”融合应用先导区试点建设，推动“5G+工业互联网”规模化发展，进一步激发各类市场主体创新活力，打造具有全国、区域引领效应的产业集群。

1.2 工业互联网安全挑战

根据 CNVD（国家信息安全漏洞共享平台）和一些公开数据，2015 年至 2020 年期间，工控漏洞数量呈现显著的递增趋势。自 2021 年开始，工控漏洞数量总体呈下降的趋势。与 2020 年的 568 条漏洞信息相比，2023 年减少了 449 条，漏洞数量大幅减少，减少数量占 2020 年的 79%。2023 年与 2022 年的 96 个漏洞相比增加了 24%，漏洞数量虽有小幅回升，但仍低于 2020 年。

由于在新冠疫情期间，大量从业人员转向线上办公，导致工控产业的活力下降，攻击者的工控攻击目标数量与类型相对减少。然而随着工业系统的运作逐步恢复正常，各类设备和系统的上线运行。新的业务需求、系统升级或集成可能引入新的漏洞，导致 2023 年漏洞数量有小幅度的回升。并且，随着工控信息安全政策、体系和法规的不断完善，工控安全方面的产品体系和解决方案逐渐健全，工控厂商对其产品的漏洞管理更加严格，才使得工控漏洞没有爆发式增长，但工业互联网安全威胁依然存在。

2. 典型安全解决方案

2.1 案例一：中兴通讯滨江 5G 工厂安全建设实践——创新技术助力 5G 工厂建立主动安全防御体系

随着 5G 专网应用与终端在滨江工厂规模化部署，工业网络边界也只不断延伸，网络系统的硬件、软件及其系统中的数据更易遭受到破坏、更改、泄露，工业系统连续可靠运行、工业网络的持续服务面临越来越多的挑战。为“5G 制造”护航，成为 5G 工业互联网应用健康可持续发展的迫切需求。

中兴通讯滨江工厂依托 AII 5G 工业互联网安全实验室，在 5G+工业互联网一体化安全框架下,从 5G 工厂迫切的安全需求出发，深入分析 5G 资产面临的安全风险及安全管理问题，开发了 5G 终端安全、5G 资产安全管理等网络安全产品及方案，验证面向制造企业不同场景下的 5G 工业安全方案，为 5G 工厂的安全建设提供样板与示范。

2.1.1 方案概述

2022 年工业和信息化部发布《5G 全连接工厂建设指南》，明确了 5G 全连接工厂建设的总体要求、建设内容和建设路径。中兴通讯滨江工厂参照指南也确定了打造 5G 全连接工厂的建设目标，充分发挥 5G 网络聚合作用，形成生产单元广泛连接、信息（IT）运营（OT）深度融合、数据要素充分利用、创新应用高效赋能的先进工厂。

中兴通讯滨江 5G 工厂重点围绕基础设施建设、厂区现场升级、关键环节应用、网络安全防护 4 个方面建设 5G 全连接工厂。其中网络安全防护部分在充分分析 5G 工厂面临的安全风险基础上，结合过往安全事件回溯，形成包含终端安全、网络安全、云安全、数据安全及安全管理的 5G 工厂纵深安全防御体系。特别是采用创新安全技术解决了 5G 终端安全、5G 专网安全管理面临的棘手安全问题。

1.方案背景

中兴通讯滨江 5G 智能制造基地，秉承“用 5G 制造 5G”理念，打造云、网、业、端四位一体的智能制造标杆，生产制造全方位数字化、智能化转型升级并与 5G 技术深度融合，探索 5G+工业互联网切实降本增效场景，攻克工业现场高要求 5G 网络技术难题，志在打造“5G+全连接”数字化工厂，实现生产、运营、管理全面极致优化的智能工厂。依托厂区与车间的 5G 全覆盖，滨江 5G 工厂梳理了整个生产管理流程，完成了整个工厂的 5G+全连接规划。5G+全连接当期落地了 16 大类、40 余项 5G+工业融合创新应用。

目前包括国际范围内，工业互联网在 5G 网络时代的安全体系尚未完善。亟需解决 5G 工厂在实际运营中的安全需求，尽快推进 5G+工业互联网相关安全研究及方案落地。

2.方案简介

滨江 5G 工厂已部署了包括：5G 云化 AGV、5G 视频监控、园区巡逻机器人、云化 PLC、机器视觉摄像头等 5G 行业专网应用，实际使用终端逾千台，出现过多起与终端有关的安全威胁事件。堵上终端安全这个缺口，消除 5G 终端引入的安全威胁，是建设滨江 5G 工厂安全防护体系的重中之重。

5G 工业终端种类繁多、数量巨大，伴随多样化 5G 终端的的接入，边界网络和终端自身的漏洞也带来了更多的安全风险，业界还没有成熟的 5G+工业终端安全解决方案。为此，中兴通讯协同合作伙伴在中兴南京滨江工厂进行安全产品开发及测试工作，成功开发出 5G SIEM 系统、5G 终端安全管控系统。相关产品的开发验证，补充了 5G+工业互联网安全体系在终端安全、5G 资产安全管理部分的方案，解除了企业对 5G 终端安全的后顾之忧，有利于加快 5G 向工业的推广使用，推动智能制造高质量发展。

3.方案目标

1、开发基于 5G 终端的安全防护产品，填补 5G 安全防护体系在端侧的空白。

根据有关机构统计结果，5G 网络相关的安全事件 80%与终端有关。在业界就曾发生过黑客通过 5G 终端入侵网络，实施数据窃取和破坏，导致 5G 专网大规模失陷的安全事件。

传统安全产品无法应用在 5G 终端上，设备受限于计算资源有限等现实因素，较难将为传统终端设计的安全机制直接配置到终端上，如安全策略、加密算法等，

导致5G终端自身安全能力较低，易被利用安全漏洞开展入侵、攻击等行为，且较难抵御。

为此，需要开展终端安全开发及验证测试工作，从而形成面向全行业推广的5G+工业互联网终端安全解决方案。

2、开发5G资产安全管控系统，实现行业5G专网一站式安全运营监测。

5G与工业互联网的融合，信息安全涉及到工业互联网与5G的各个层面，传统的安全管理系统不能满足5G+工业互联网的信息安全的需要。只有通过构建统一的5G资产安全监测运营保障体系，较为全面覆盖5G CT资产、IT资产、OT资产，提供5G专网全局资产视图和安全态势呈现，针对资产和业务进行威胁分析，产生告警和处置建议，协同安全组件迅速进行响应和处置。才能够有效的保障5G智慧工厂的安全运营管理。

2.1.2 方案实施概况

中兴通讯在南京滨江制造基地建设5G智慧工厂，通过几年的发展，滨江工厂已部署了包括5G云化AGV、巡逻机器人在内的16大类、60余种创新5G工业应用，伴随应用与终端的增多，安全问题随之而来，其中大多数威胁来自终端侧。

为了消除5G终端的安全威胁，构建5G专网一体化安全管理，我们遵循相关标准规范，以5G终端为主要切入点，通过部署创新安全产品，构建一套完备的网络安全保障体系，为“5G制造5G”护航。

1. 项目总体架构和主要内容

本项目以5G终端安全管控为核心底座，通过部署5G SIEM等各类安全系统，从终端安全、网络&边界安全、边缘云安全、数据安全这四个角度保障5G工业互联网的安全，搭建5G工业互联网安全防护体系，为5G+工业互联网保驾护航。5G智慧工厂方案体系框架如下图所示。

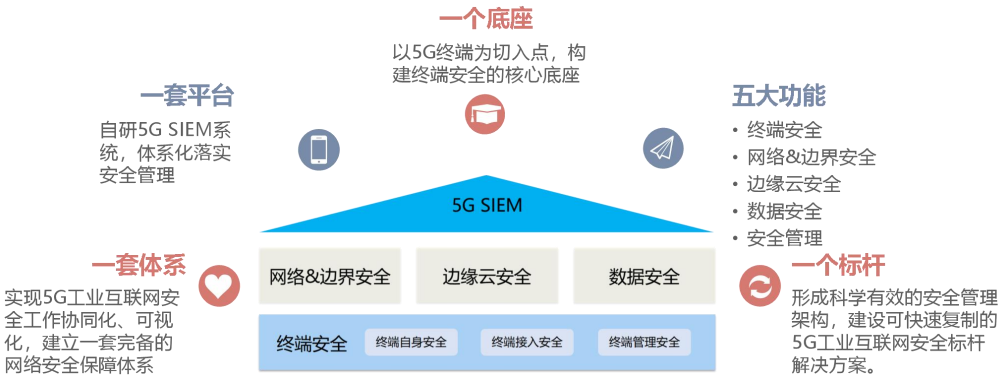


图 1-1 滨江 5G 智慧工厂安全方案体系框架

2. 基于 5G SIEM 的“端网一体”安全管控

本方案基于 5G 终端系统安全监控防护技术，采用自学习的网络、进程安全防护策略，可针对 5G 终端系统进行威胁感知、安全防护、数据加密。通过在终端资产上安装增强型安全 Agent，并由 Agent 将终端资产与安全信息采集并上报至 5G SIEM 中内嵌的 Agent 管理系统，再通过 5G SIEM 基于大数据、知识库和威胁分析能力，实现终端的 5G 资产安全管理、终端资产异常行为检测、安全事件与资产的关联分析等功能，保障 5G 工业终端安全。

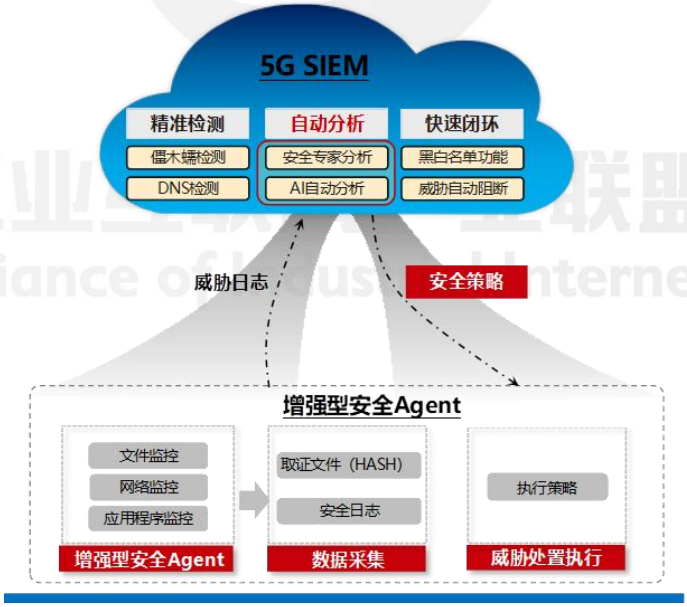


图 1-2 基于 5G SIEM 的“端网一体”终端安全管控架构

（1）5G 终端安全管控

通过对滨江工厂进行安全风险分析，发现终端主要面临包括非法外联、系统漏洞、弱口令、非授权访问等安全风险，这给 5G 工业互联网带来了病毒攻击、内网入侵、数据泄露等安全问题。

因此，我们制定了5G智慧工厂终端安全防护机制，以“攻击免疫”技术为核心，对终端进行安全加固，保障终端自身安全和可信执行；通过机卡绑定、二次认证、电子围栏等方式保障终端接入安全；通过在管理平台上进行资产安全管理、异常行为检测、事件关联分析，实现终端安全管控。

增强型安全Agent安装在5G终端上，可全面监视终端系统中所有进程活动，准确识别并拦截新型恶意程序。与传统安全防护补丁修复的解决方案相比，本方案采用创新的虚拟补丁技术可以实现“不拔网线、不打补丁、不封端口”也能有效防护漏洞，避免黑客利用漏洞进行攻击。引擎基于内存指令层的漏洞攻击检测技术，融合了机器学习等AI技术，脱离了对具体漏洞特征、文件特征、行为特征的依赖，即使在断网情况下，也不影响效果。该引擎基于的原理并不依赖于特定操作系统，而是采用指令级别的监测，这种方法同样适用于其他操作系统，而目前市面上的加固工具都是依赖操作系统本身的能力。在面对 0Day 漏洞、可信程序被恶意利用、以及后门的检测方面，都有显著的防护效果，减少了误判，极大降低了对人工的依赖，从而大幅降低误报率和运营成本。安全Agent具体功能如下:

- 僵木蠕检测与防御
  - ✓ 实时检测与阻断僵木蠕网络通信
  - ✓ 从源头阻止DDoS攻击事件
- 设备隐身
  - ✓ 设备网络端口服务全面隐身，避免被攻击者发现
  - ✓ ICMP协议过滤
  - ✓ 只有收到正确秘钥才可访问设备服务
  - ✓ 全面免疫外部网络攻击
- 网络扫描检测
  - ✓ 实时发现外部网络扫描行为，及时发现外部威胁
  - ✓ 实时发现内部网络扫描行为，及时定位内部失陷主机
  - ✓ 暴力破解行为阻断
- 欺骗防御
  - ✓ 能够在网关内网中开放多个虚假端口服务

- ✓ 诱导攻击者，及时发现潜在威胁
- ✓ 及时发现网络侦查行为
- ✓ 及时发现蠕虫、病毒内网传播行为

（2）5G SIEM

5G SIEM 支持资产安全数据的采集、处理、分析、关联、安全调查和安全态势展现等。通过对 5G 资产和业务的梳理和理解，对上报的多种安全事件与资产的分析，将资产与业务域进行可视化，呈现资产的威胁信息，形成全局资产视图和安全态势呈现。通过大数据分析技术将安全事件与资产进行关联，针对资产和业务进行威胁分析产生告警和处置建议，协同安全组件迅速进行响应和处置。

5G SIEM 系统支持终端资产异常行为检测，通过对资产进行分域划分管理，设置域之间的访问策略，及时发现非法跨域访问与域间业务异常访问，基于流量基线、流量异常访问等检查功能识别和检测终端的异常访问行为和异常流量行为。

其中，5G SIEM 内嵌的 Agent 管理系统通过接收部署在终端设备上增强型安全 Agent 采集上报的数据信息，可实现业务概览，安全概览，漏洞概览，终端概览，终端列表，基础信息，高级信息，设备信息，无线信息，安全基线管理，无线信息，漏洞管理，程序可信管理，文件可信管理，网络可信管理，未知威胁管理，威胁告警以及系统管理等，5G SIEM 具体功能如下:

- ➢ 多精准检测
  - ✓ 僵木蠕检测: 实时检测拦截，超高阻断率;
  - ✓ DNS 检测: 云端基于 DNS 日志，结合大量实时威胁信息，实现挖矿、勒索、恶意站点 C&C 远控等威胁深度分析（五元组、域名 URL）;
- ➢ 威胁秒级判定
  - ✓ AI 分析判定: 云端 10+专家模型结合 AI 算法大量日志的智能聚合分析，威胁秒级判定，用户零分析投入;
- ➢ 自动溯源处置
  - ✓ 关联分析溯源: 5G SIEM 基于海量实时威胁信息和用户网络模型，多维度关联分析，自动判定威胁内外网，实现攻击精准溯源;
  - ✓ 自动处置闭环: 内部失陷主机实时告警，外部攻击源秒级封禁，准确率 99.9%。

3.具体应用场景和安全应用模式

基于 5G SIEM 的“端网一体”安全管控主要包括 5G SIEM 系统、5G 终端安全 Agent、各类安全防护设备、5G 行业专网、工业应用系统及网管平台。5G SIEM 系统收集来自 5G 工业终端、安全设备的日志、告警等信息，实时全网终端的网络安全与异常事件安全风险态势，呈现终端与安全事件关联关系，快速发现安全事件，快速定位问题资产，统一安全管理策略下发与风险事件处置。

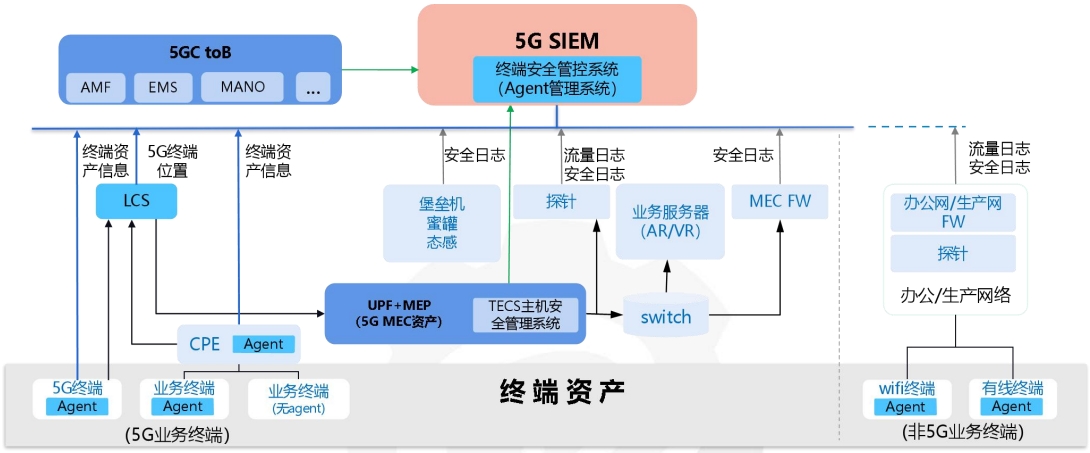


图 1-3 基于 5G SIEM 的“端网一体”安全管控

本方案集设备自动发现、基线漏洞探知、接入自动甄别、行为自动分析、违规自动阻断等多种安全功能于一身，建立纵深防御体系。在加强安全运行管理同时，轻松实现批量设备统一管理、攻击行为实时报警、安全风险实时掌控、非法入侵及时阻断等能力，全方位解决 5G 工业终端设备安全运行问题。

4. 安全及可靠性

本方案从设备管理、运行监测、主动防御三个维度进行设计，集设备自动发现、基线漏洞探知、接入自动甄别、行为自动分析、违规自动阻断等多种安全功能于一身，建立纵深防御体系。在加强安全运行管理同时，轻松实现批量设备统一管理、攻击行为实时报警、安全风险实时掌控、非法入侵及时阻断等能力，全方位解决 5G 工业终端设备安全运行问题。

2.1.3 下一步实施计划

1、继续拓展 5G SEIM 的应用场景，对接工控网络流量审计等工业安全设备，将 CT、OT 等各层级资产进行关联，根据资产关联关系来定位漏洞、脆弱性与攻击事件等威胁事件对业务的影响，追踪攻击链定位威胁发生的源头。

2、5G SIEM、终端安全系统适配国产化服务器、操作系统、数据库，基于自有平台开发适用于工业互联网特定场景的安全监测系统。

2.1.4 方案创新点和实施效果

1.项目先进性及创新点

本 5G 智慧工厂方案采用自主研发的 5G SIEM 与增强型安全 Agent，基于终端系统安全监控防护技术，采用自学习的网络、进程安全防护策略，可针对工业终端系统进行威胁感知、安全防护、数据加密。

本方案具有 5G 设备管理、运行监测、主动防御三个方面的创新。

（1）5G 工业终端管理

本方案中 5G SIEM 系统支持终端的 5G 资产安全管理，通过对终端信息的采集、统计、查询及风险评估，终端在网络拓扑中的位置和业务访问关系，对终端的属性、位置等特征进行检测，发现异常设备接入。

（2）5G 工业终端运行检测

5G SIEM 系统支持终端资产异常行为检测，通过对资产进行分域划分管理，设置域之间的访问策略，及时发现非法跨域访问与域间业务异常访问，基于流量基线、流量异常访问等检查功能识别和检测终端的异常访问行为和异常流量行为。

（3）5G 工业终端主动防御

首先，本方案中增强型安全 Agent 采用创新的“虚拟补丁”技术，颠覆了查漏洞打补丁的传统安全防护思路，即使不打补丁，也能有效抵御攻击。本系统不基于已知漏洞载荷特征进行保护，而是从原理上识别漏洞攻击行为，能够在攻击链路的任一环节进行阻断拦截，无论是 0day 漏洞还是 Nday 漏洞，都能快速阻止入侵行为，为主机提供更有效、精准、便捷的安全防护。

（4）自研 5G SIEM,实现 CT、OT 资产一体化安全管理

本方案中 5G SIEM 系统支持包括 5G 基站、UPF、MEC、及 5G 工业终端的一站式安全管理，真正打通了 5G 专网中的 CT、OT 资产安全统管。通过对各类资产信息的采集、统计、查询及风险评估，终端在网络拓扑中的位置和业务访问关系，对终端的属性、位置等特征进行检测，发现异常设备接入。

2.实施效果

（1）5G SIEM 和终端安全管控系统在滨江上线，截至目前累计发现 1 万多条威胁事件，确认发现 80 多条有效安全事件，处置了多个失陷终端。

图 1-4 安全管控系统

（2）中兴通讯南京滨江 5G 智慧工厂通过国家网络安全等级保护三级测评，等级测评结论达到优，为后续 5G 智慧工厂安全建设打下坚实基础。本次等保测评首次纳入 5G 网元作为测评对象，为 5G 专网等保标准技术要求的编写提供了参考建议和依据。

等级测评结论

测评结论和综合得分			
被测对象名称	中兴通讯 5G+智慧工厂核心网络系统	安全保护等级	第三级（S3A3）
扩展要求应用情况	☑云计算 ☑移动互联 ☐物联网 ☐工业控制系统 ☐大数据		
被测对象描述	中兴通讯 5G+智慧工厂核心网络系统通过 5G 网络将车间生产设备参数接入工业互联专网平台，结合 MEC 等在生产流程上部署云化 AGV、机器视觉、云化 PLC、智能仓储、工业穿戴、数字孪生、生产现场监测等十多个典型 5G 应用，全面覆盖了实时工业控制、设备环境监测、物料供应		
安全状况描述	中兴通讯（南京）有限责任公司中兴通讯 5G+智慧工厂核心网络系统核心网络系统在网络安全等级保护第 3 级（S3A3G3）保护要求中综合得分 90.74，测评结论为优。		
等级测评结论	优	综合得分	90.74

图 1-5 等级测评报告

（3）方案获得欧洲 Telecoms 颁发的“Glotels 奖”

图 1-6 Glotels 奖

2.1.5 单位基本信息

中兴通讯是全球领先的综合通信信息解决方案提供商，为全球电信运营商、政企客户和消费者提供创新的技术与产品解决方案。公司成立于 1985 年，在香港和深圳两地上市，业务覆盖 160 多个国家和地区，服务全球 1/4 以上人口，致力于实现“让沟通与信任无处不在”的美好未来。坚持以持续技术创新为客户不断创造价值，在美国、瑞典、中国等地设立全球研发机构，同时进一步强化自主创新力度，保持在 5G 无线、核心网、承载、接入、芯片等核心领域的研发投入，研发投入连续多年保持在营业收入 10%以上。截至 2023 年，中兴通讯拥有 8.65 万余件全球专利申请、历年全球累积授权专利约 4.4 万件，连续 9 年稳居 PCT 国际专利申请全球前五。同时，中兴通讯是全球 5G 技术研究和标准制定的主要参与者和贡献者。据 2021 年，投资管理公司仲量联行发布《中国通信行业及知识产权市场报告》显示，中兴通讯的专利技术价值已超过 450 亿元人民币。在中国专利奖评奖中，累计获得 10 金 2 银 38 铜的优秀成绩。2019 年第二次入选富时社会责任指数系列(FTSE4Good Index Series)，位列中国企业 300 强社会责任发展指数前 100 名。中兴通讯致力于构建 5G 时代自主创新核心竞争力，将凭借领先的 5G 端到端全系列产品与安全解决方案，加速推进全球 5G 在工业互联网领域的规模部署。

2.2 案例二：某大型汽车制造集团-生产基地综合管控系统建设项目——推动“汽车制造集团-生产基地”工业互联网安全数字化安全冶理新思路

某大型汽车制造集团通过建设生产基地综合管控系统，进一步提升和加强对各生产基地的工控网络安全的安全管控能力，实现工控网络安全工作“一盘棋”管好“一张网”思想。

2.2.1 方案概述

1.方案背景

为贯彻落实《中华人民共和国网络安全法》、《国务院关于深化制造业与互联网融合发展的指导意见》、《工业控制系统信息安全防护指南》、《工业控制系统信息安全事件应急管理工作指南》、《工业控制系统信息安全防护能力评估工作管理办法》、《关于促进工业信息安全产业发展的指导意见》等国家和行业指导文件要求，提高生产信息系统的安全性和管理质量，消除或降低当前存在的安全风险，提供良好的基础设施支撑环境和安全的系统环境；为了进一步推动和加强各生产基地工控网络安全工作，某大型汽车制造业集团公司（以下简称集团）生产信息化基础设施在加速建设完善，集团推动建设生产基地综合管控系统（以下简称“集团系统”），树立工控网络安全工作“一盘棋”管好“一张网”思想，建立协同联动、及时快捷、高效运转的一体化网络安全工作格局，实现安全监测、预警、防护、通报、响应和追溯工作的一体化、实时化，全面提高生产基地网络安全态势感知、监测和防护水平，为网络安全监管工作提供决策依据和技术手段。

2.方案简介

集团生产基地综合管控系统建设总投资为千万级，安恒信息召集工业网络安全咨询规划、解决方案、产品设计、研发和安全服务等人员参与集团系统建设工作，为集团设计了集安全合规管理、安全运营维护和安全服务赋能于一体的系统。

集团系统整合各生产基地生产基地级网络安全态势感知类系统数据，实时掌握各生产基地关键信息基础设施和重要工业系统的网络安全态势；建立安全合规

监督检查机制，形成安全合规闭环管理；发现问题或风险及时通报预警重大网络安全威胁；建立跨地域、跨部门的应急指挥协同机制，构建各方参与的网络安全综合防控体系。

3.方案目标

（1）总体目标

通过建设集团系统，实时掌握各生产基地关键信息基础设施和重要工控系统的网络安全态势，及时了解辖区内重要系统、重点部门、核心网络节点和违规在线工控系统的网络安全威胁、风险和隐患，监测其安全漏洞、僵木蠕毒传播和网络攻击情况；整合各生产基地已建成生产基地级网络安全态势感知数据，及时通报预警重大网络安全威胁；形成集团和各生产基地相关部门协调联动的网络安全监测预警处置工作机制，构建各方参与的网络安全综合防控体系；建设跨地域、跨部门的应急指挥协同机制；最终实现“看得见网络、防得住攻击、控得住网情、抓得住敌手、止得住危险”，为集团工控网络安全监管工作提供有效技术支撑，从而推动工控网络安全监管协调工作向深层次发展，提升辖区内网络安全防护水平，保障辖区内业务平稳安全运行。

（2）项目分项目标

建设集团生产基地工控安全态势感知能力。目前集团缺乏对各生产基地工控网络安全态势感知、分析能力，难以实时掌控工控安全动态，在发生工控安全事件时，也无法进行精准研判。为实时掌握各生产基地工控安全情况及动态，在发生安全隐患时可以进行快速、精准研判，需依托大数据技术建立集团全国工控安全感知分析能力，实现精准匹配、重点分析，并提供多个维度可视化的大数据分析结果，为研判、决策工控安全保障工作提供有效支撑。

建设集团生产基地工控安全预警与信息通报机制。当发生网络安全事件、漏洞、隐患、恶意木马病毒时，有针对性地发出通报预警，信息通报是下发重要信息、强制性要求的信息发布途径，结合实时监测系统监测数据、上级安全事件通告、第三方情报来源进行安全事件通报预警。同时，对外发布重大网络安全漏洞报告、病毒通报、相关网络安全事件、安全分析报告等资讯，提供处置措施与建议，为集团提供网络安全服务。

建立集团生产基地应急响应协同管理体系。除了事前监测、事中通报以外，发生问题第一时间的快速处置，针对影响较大的安全事件，建立多级协同应急处置机制和流程；针对各类工控网络安全应急事件，制定一体化的应急预案，建设应急预案库，积累历史应急预案、典型案例、实战演练等知识，为后续网络安全事件应急指挥和重大保障活动提供指导依据；并在事后提供日志分析、数据恢复、线索检索、攻击验证等技术手段。

建立重大活动安全保障机制。在重大活动保障期间，制定重大保障任务，确定保障时间范围、管理范围、负责人及参与者、制定检查工作计划、制定保障演练计划，制定应急预案和制定保障驻场值班表等。

建设集团生产基地工业安全中台。为避免安全数据的信息孤岛，将威胁分析所需的各类安全数据进行统一采集、处理和存储，需要建立工控安全数据中台，从而建设安全大数据高效处理能力。工控安全数据中台需要对采集到的多源异构数据进行处理，包括数据的清洗、过滤、提取、标准化、标签化等方式，提升数据质量、规范数据处理流程、优化数据服务水平，构建安全资源库，产生数据关联信息，实现数据融合，进而挖掘数据价值。并通过安全数据场景化分析模块，提供关联规则、统计建模、场景关联分析建模、情报建模以及机器建模等安全分析能力，提供支撑上层应用的数据。同时，工控安全数据中台可形成与上级监管部门以及各生产基地的数据交换共享功能，为协同工作提供基础数据共享能力。

2.2.2 方案实施概况

1. 总体技术架构

本项目同步建设集团系统与生产基地安全监测分析系统(以下简称生产基地系统)，本项目建设目标是安全管理“自上而下”；安全运营“自下而上”；同步建设，协同管控。

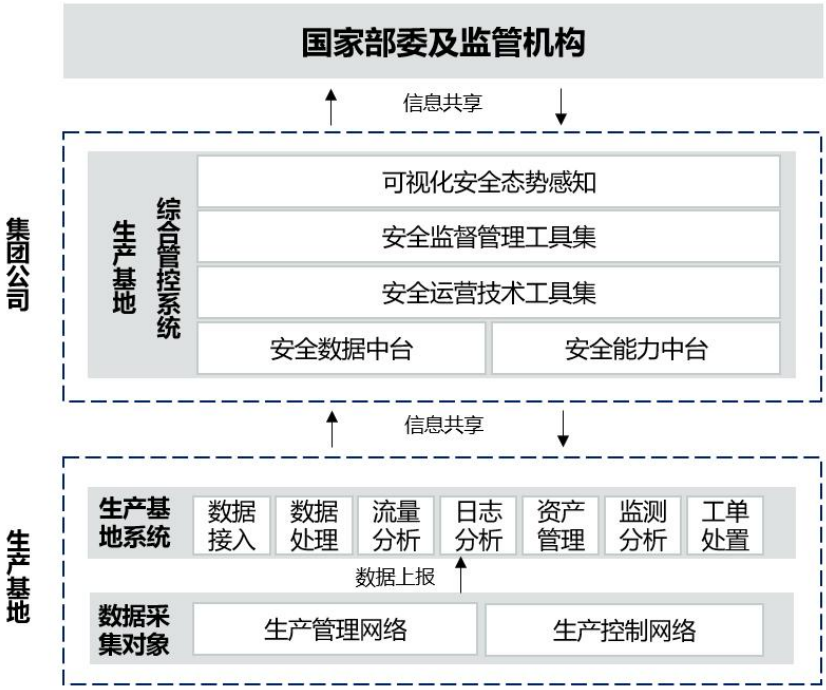


图 2-1 总体架构图

“自上而下”：安全业务管理采用“自上而下”工作方法，以网络安全法、工业互联网安全分类分级为建设指南，结合集团生产基地网络安全管理办法，通过安全监督管理工具集将日常的安全业务管理工作数字化、流程化和服务化，以安全合规为基础，运用组织管理、通报预警、协同应急和考核管理等综合管控手段，开展对各生产基地网络安全管理工作。

“自下而上”：安全运营管理采用“自下而上”工作方法，通过采集各生产基地安全数据，实现对各生产基地的统一安全运营管理，及时发现生产基地威胁信息，按应急管理流程及时上报、审核、发布通报预警和响应处置等，形成安全运营管理闭环。

同步建设，协同管控：集团生产基地综合管控系统与生产基地安全监测分析系统同步建设，保证两系统的级联管理与数据信息共享，为集团系统与生产基地系统提供协同管控的基础条件。

2. 安全数据中台

安全数据中台实现对所有监管数据、威胁情报库数据的整合、归档、应用并对上层提供数据的服务能力。主要提供安全数据集成、安全数据处理治理、安全数据计算等，形成安全数据服务资源目录，统一为上层提供数据服务。

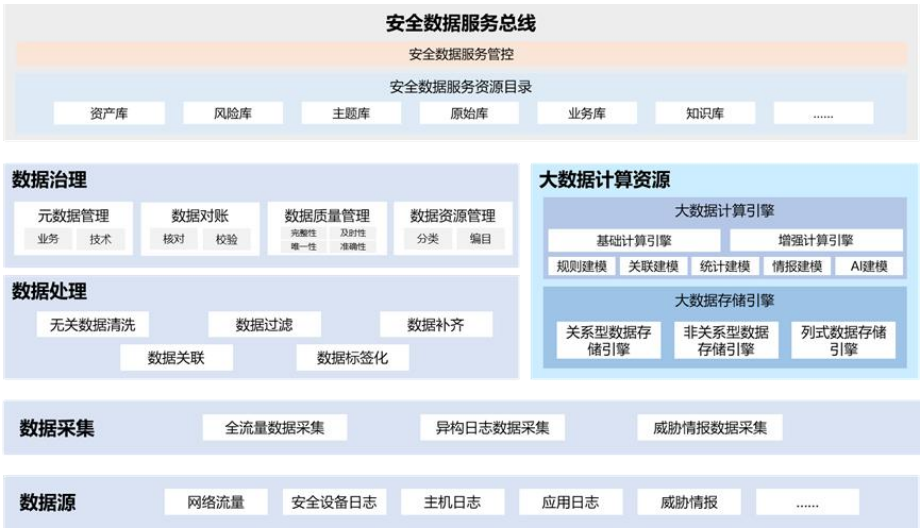


图 2-2 安全数据服务总线

3. 安全能力中台

安全能力中台遵从安全能力服务化规范，聚焦各维度的安全需求，将各种安全能力服务化，形成安全服务目录，实现安全资源的灵活调度，将能力目录、能力接口、能力编排等方面进行有机结合，为用户应用场景提供安全能力服务中心。

图 2-3 安全能力服务总线

4. 应用系统设计

（1）安全态势感知

安全可视化能够对集团态势进行展示，支持自定义的可视化设计与展示，主要在全局监测数据、检测数据、智能分析数据等多维数据的态势分析之上，形成综合态势、攻击态势、威胁态势、预警态势等多种态势感知能力。从整体视角展示集团总体的安全情况，包括网络安全情况、系统安全情况、资产安全情况、安全威胁情况等。

从网络攻击维度进行态势分析和可视化。支持图形化方式展现对网络攻击情况、网络异常流量情况、恶意程序传播情况等的统计分析结果，统计周期包括天、周、月等。支持实时展示网络攻击情况、网络异常流量情况、恶意程序传播情况、恶意网址访问情况等分析维度的告警数据，告警内容包括但不限于：告警时间、告警类型、告警级别、告警内容、攻击源 IP、攻击目的 IP、攻击次数等，支持查看告警详情。

从资产脆弱性维度进行态势分析和可视化，包括漏洞、弱口令等。支持实时展示资产安全风险情况分析维度的告警数据，告警内容包括但不限于：告警时间、告警类型、告警级别、告警内容、资产 IP 等，支持查看告警详情。

可视化应用为此项目建设的重要应用，通过可视化图表、综合态势大屏、运营报表三种方式实时展示集团安全态势情况，并对威胁事件进行统计，通过可视化实时展示整体安全态势，方便安全运营人员及时感知到集团安全风险。

建设态势大屏来展示不同维度的风险情况，从弱口令、资产信息、失陷资产、安全事件、风险等级等维度对安全数据进行统计，并通过不同的图表形式展示，产出涵盖外部攻击态势、横向威胁态势、资产失陷态势、信息系统态势、资产威胁溯源、系统运行监测等态势大屏以供纵览全局风险，组建两网（工控网、管理信息网）融合态势感知大屏。

（2）安全管理工具集

安全管理工具集为集团安全管理人员提供安全管理应用，主要包括如下应用功能：

✧ **安全服务门户**

安全门户面向该汽车制造集团和生产基地用户提供统一的业务服务，主要包括工作资讯和支撑保障。

■ **工作资讯**

为了让集团管理部门和生产基地用户快速、简洁的了解最新工作要求和相关工作开展情况动态，工作资讯整合了集团系统的工作待办信息。

■ **支撑保障**

支撑保障是提供相关工业安全政策规范、专家信息及服务机构等信息，各生产基地可通过集团系统获取相关信息，为开展工业安全工作提供基础的支持保障。

✧ **组织管理**

组织管理以树结构形式管理集团的组织架构，组织架构节点可以选择“单位”或“部门”。

■ **组织管理**

组织管理支持按照组织架构树进行增加、编辑、删除单位节点，并且支持多级组织架构树。

■ **级联管理**

集团生产基地综合管控系统的告警、漏洞、资产数据均可基于组织架构进行单位数据权限隔离，生产基地系统向集团系统进行组织架构信息同步，下属单位组织架构由本单位维护，其中集团生产基地综合管控系统仅可查看二级单位组织架构，不可编辑修改二级单位组织架构信息。

■ **数据关联**

下属单位账号可根据组织架构查询所选单位的告警、漏洞、资产数据。

■ **组织架构本级与下级区分**

组织架构包含集团系统本部单位及下级单位，本部可根据组织架构查询本部与下级单位的告警、资产、漏洞数据。

✧ **合规管理**

合规管理是该汽车制造集团定期开展检查工作的主要机制，主要包括现场检查、安全自查两个部分，通过集团系统管理检查工作、收集检查数据、评价检查结果。检查调查系统支持与网络安全检查工具箱、工业控制系统安全检查工具箱实现数据对接和业务管理闭环。

✧ **通报预警**

当监测到工业系统存在重大风险隐患，或发生重大安全事件时，集团系统会及时进行通报，被通报的工业网系统、管理信息网系统需按期反馈处置结果。通报预警模块实现安全事件通报、安全隐患通报的进度跟踪及信息通知发布，对上述基础数据进行分级、分类归纳分析，自动形成通报报告，按照不同情况分别进行通报、提醒和限期整改等业务流程。

✧ **档案管理**

档案管理统一管理包括终端、监控、工控、在线业务系统等在线网络资产的资产分布、漏洞和指纹信息，摸清各生产基地资产底数，形成统一的资产立体化管理，具备更加细化的信息系统资产数据：可按所属行业、机关横向分类；可按所属地域、行政归属横向分类；可按工业互联网企业类型、等级纵向分级；可按信息系统重要、敏感程度纵向分级；可按信息系统脆弱程度、可用程度纵向分级。

✧ **考核管理**

为了有效开展工业信息安全管理工作，项目通过管理评价系统，实现以查代促、以查促改、以查促管、以查促防，达到有效推动各生产基地落实网络安全建设工作的目标。

✧ **协同应急**

协同应急功能主要在发生较高风险的安全事件时，或在重要会议或重大活动期间，全方位全天候掌握与活动相关的网络安全状况，及时通报预警网络安全隐患，高效处置网络安全事件；对重点对象的监控、应急人员管控、调度指挥、应急处置以及活动情况总结归档；对应急指挥期间各职能部门、重要行业部门、技术支持单位进行综合指挥，协同多家技术支撑单位、第三方安全厂商、网络安全专家以及其他职能部门保障整个重大活动期间的网络安全。协同应急主要包括活动管理、组织管理、应急制度、通报管理、值守管理和指挥调度等功能。

（3）安全运营技术工具集

安全运营技术工具集为集团和生产基地安全运营技术人员提供安全运营过程中使用的应用工具，主要包括如下功能：

✧ **资产管理**

资产管理作为态势感知的最基础功能，确定了安全管理的对象和目标，将所有业务系统的网络设备、工控设备、安全设备、服务器及其之上承载的操作系统、数据库、应用系统、接口方式、硬件属性、使用维护人员等信息均作为资产管理的内容，提供资产录入、管理、变更等管理功能。可通过流量监控开放端口、主动外连行为等。

✧ 安全监测

■ 事件感知

事件感知以威胁模型能力为基础，对全流量审计行为分析、Web 攻击监测行为、邮件攻击监测行为、文件攻击监测行为、DNS 异常流量监测、挖矿行为、勒索病毒行为等进行监测，还提供了工业网络场景下的安全监测能力，帮助集团用户快速定位在工业网络安全场景下的安全事件。

■ 资产感知

以资产为核心视角，直观了解自身网络环境中存在的风险资产。资产感知通过攻击链形式展示，剖析从扫描探查阶段到资产破坏阶段资产失陷过程。感知失陷、异常资产，从海量的日志中提取有价值的资产溯源路线。集团系统简单易用，支持一键全方面钻取，降低运维成本，提高运维效率。

■ 安全热点

安全热点是结合用户实际需求，支持用户自定义设置安全热点问题，可选择内置安全事件作为安全热点，也可以通过自定义威胁模型定义安全事件后再设置成安全热点。安全热点可帮助用户快速排查重点问题，发现最重要的事件，发起快速处置。

■ 检索中心

检索中心是集团系统的日志搜索入口，提供关键字组合输入功能，实现日志快速检索，包含原始日志搜索、标准化日志搜索、自定义搜索模板和历史搜索快照。

✧ 安全分析

■ 威胁模型

威胁模型展示了基于工业互联网场景下各类内置模型管理功能，模型支持自定义。同时为了方便用户快速上手，提供了五大建模管理方式，主要包括规则建

模、安全事件关联建模、安全事件统计建模、威胁情报建模和 AI 学习建模，利用分析引擎进行数据深入分析，提升安全威胁检测准确率。

内置工业威胁模型。集团系统内置工业威胁模型，帮助用户快速发现工业网络场景下的各类威胁和异常行为，主要包括：写事件、程序上装、程序下载、启动与停止、不合规行为、工控扫描行为、工艺参数值异常、访问关系异常、异常流量行为和资产基线异常等。

■ **指标管理**

集团系统支持自定义分析指标，以便于更灵活的开展威胁建模工作，指标管理支持原始日志、异常记录和安全告警等多种数据来源，同时提供 COUNT、AVG、SUM、MAX、MIN、DISTINCN_COUNT 等多种统计方式，并提供不同场景下的指标定义。

■ **资产画像**

工业资产画像以采集到的各种数据为依据，通过安全建模分析，提供可视化工业资产画像，主要包括：资产基本信息、风险信息、访问关系、行为画像、服务端口、访问端口、脆弱性等。

工业资产画像可以快速分析重点资产的安全防护效果与威胁情况，为资产风险评估、安全加固和安全保护建设提供依据。

■ **追踪溯源**

追踪溯源旨在确定攻击事件后，回溯所有攻击相关的网络数据包，对集团系统近期的所有行为进行串联，确定攻击事件的整个事件周期，展示整个攻击事件的所有攻击路径。以互访流量关系为纽带，将攻击者的所有攻击动作列举出来。集团系统简单易用，支持一键全方面钻取，降低运维成本，提高运维效率。根据资产安全告警分析所处安全状态，集团系统会对资产进行状态标记，帮助用户清晰了解全局资产状态。

✧ **安全运营**

■ **安全工作台**

为集团网络安全运维人员提供安全事件处置工作界面，包括工单管理、通报情况、最新安全动态等视图，并为用户提供代办工单状态工作台，方便用户快速处理安全工单。

■ **工单管理**

提供工单管理视图，可以通过工单管理界面新增工单、通报详情页面新增工单、安全告警页面新增工单，并将工单指派给相应的处理人，经过各个环节的处理，工单记录状态包括未处理、处理中、已解决和已关闭，便于监督工单及时处理完成闭环。提供包括工单查询、工单新增、工单处置、工单删除、工单跟踪以及工单批量操作等功能。

■ **运行报告**

通过对安全态势数据进行周期性归纳总结、统计分析，形成全网安全态势分析报告，帮助用户管理全网安全态势变化。集团系统目前支持自动导出集团系统运营简报、安全分析运营报告、深度威胁分析报告、资产风险报告，并提供自定义编辑能力，WORD、PDF 或 HTML 多格式导出能力，报告导出后，支持订阅与推送，集团系统可选择向指定邮箱定时推送订阅报告，报告内容、报告形式、推送时间、推送周期等支持自定义选择。

■ **安全自动化编排与响应处置**

基于安全分析能力和应用能力，通过剧本编排，对复杂的分析、处置流程进行集成整合，实现从静态事件响应到动态工作流跟踪的转变，提升整体的协调及决策能力。

剧本以原始数据或安全事件作为输入，结合统计模型、情报模型、关联模型、规则模型进行威胁分析，并实现联动阻断、通报预警、人工查验等响应动作。

2.2.3 下一步实施计划

1. 形成标准化安全数据采集方案

实施目标为实现全域生产安全基础数据采集，建立标准化数据采集方案和接口规范。目标分为前、中、后三期开展实施:

前期:

- 应急响应处置流程阶段性固化
- 建立安全运营考核指标
- 安全运营报告阶段性固化
- 以自查或第三方检查等方式，开展对试点工厂的安全合规评估

中期：

- 建立各试点工厂资产业务模型
- 建立风险处置知识库
- 发布安全运营管理要求

后期：

- 资产业务模型标准化
- 风险处置知识库持续优化
- 安全运营管理要求系统化，打通三级管理机制（集团-基地-车间）

2. 场景化威胁分析模型优化

实施目标为优化风险监测规则，建立集团场景化威胁分析模型，统一风险告警策略。目标分为前、中、后三期开展实施：

前期：

- 部署并应用安全监测规则
- 对已接入的第三方安全设备数据误报信息分析
- 当前误报信息分析与规则调整
- 对高风险或有价值的告警信息数据进行重点监测

中期：

- 评估当前安全监测规则有效性
- 针对当前监测规则进行有效性整改
- 结合客观环境，制定高风险威胁分析模型

后期：

- 形成标准化的威胁分析模型
- 更新集团系统数据对接标准规范中威胁事件的监测内容

3. 安全态势内容优化

实施目标为完成全域安全态势可视，实现安全考核指标标准化，达成风险可控、可见、可溯源。目标分为前、中、后三期开展实施：

前期：

- 总体安全态势可视化
- 试点工厂的安全态势可视化
- 集团工控安全通报预警安全态势可视化
- 集团资产安全态势可视化

中期:

- 总体安全态势优化
- 集团和试点工厂的安全运行态势优化
- 以考核指标内容为标准，进行各工厂的考核评价可视化

后期:

- 业务与安全的可视化调整
- 考核评价的可视化调整
- 固化各工厂安全态势可视化内容

4.安全运营赋能

实施目标为安全风险应急处置流程标准化，建立安全知识库，完成集团-基地-车间三级联动。目标分为前、中、后三期开展实施:

前期:

- 应急响应处置流程阶段性固化
- 建立安全运营考核指标
- 安全运营报告阶段性固化
- 以自查或第三方检查等方式，开展对试点工厂的安全合规评估

中期:

- 建立各试点工厂资产业务模型
- 建立风险处置知识库
- 发布安全运营管理要求

后期:

- 资产业务模型标准化
- 风险处置知识库持续优化
- 安全运营管理要求平台化，打通三级管理机制（集团-基地-车间）

2.2.4 方案创新点和实施效果

1. 项目先进性及创新点

（1）数字化、集约化和服务化的公共服务技术创新

利用集团系统建立集约化安全支撑服务资源队伍，同时面向总部集团和生产基地提供“一站式”SaaS 化安全服务，以安全中台为数字化技术底座，为集团提供对生产基地的日常安全监测预警、研判分析能力，提升响应处置效率。帮助各生产基地提高安全防护意识，显著提高安全防护水平。降低集团网络安全部门的管理成本。同时，利用集团系统制定对安全服务供应商和生产基地的考核规则，并通过定期考核，使两者不断优化安全服务能力与安全防护能力，形成良好的生态体系。

（2）工业互联网安全场景安全数据采集与融合分析技术创新

集团工业网络场景具有网络结构复杂、业务系统和设备类型多的特点，因此需要具备可更多应用场景的安全数据采集能力，以及大数据智能分析能力。

数据采集能力：通过在设备、控制、网络、数据、平台、应用的安全数据采集，覆盖包括 5G、标识、平台、物联网、工控网、信息网、工业云等全场景应用。

大数据智能分析能力：对各场景下的用户、系统、设备、网络和操作行为进行融合分析，将各场景可能发生的安全现象进行总结分析，形成工业互联网专有的威胁分析模型，同时可根据用户实际业务场景自定义模型，更贴合用户业务，为安全生产提供稳定、可靠的威胁发现与分析能力。形成集团工控网络安全在各场景的安全分析与追踪溯源能力。

（3）数字化工业企业安全合规管理技术创新

集团生产基地综合管控系统的企业安全合规管理业务应用，以集团工业网络安全合规相关要求为基准，对各生产基地开展定期安全合规检查，该应用结合总部集团、生产基地和生产车间三大用户角色，提供“任务管理、合规自评估、现场检查、安全整改、检查验收”五大流程化管理功能，帮助集团实现数字化、流程化的安全合规闭环管理机制。

（4）基于闭环安全管理机制的多级协同响应处置技术创新

集团生产基地综合管控系统的监测预警与协同响应业务应用以安全中台为数字化技术底座，结合集团《生产基地应急响应管理办法》，具备集团-生产基地-生产车间三级应急响应协同机制，实现安全事件和风险隐患的实时发现能力，并提供多元数据安全研判分析工具，为安全分析人员提供详细的调查取证工具，从而实现高效率、精准的安全预警与信息通报功能。当发现不同安全级别的事件或风险隐患时，可启动不同的响应流程，协同响应总部集团、生产基地、生产车间和安全支撑机构等，有效提高应急响应与处置效率。

2. 实施效果

（1）建立集团集约化工业网络安全公共服务体系

一是加强对集团工业互联网安全公共服务能力，通过对集团资产梳理、安全隐患监测、安全事件分析研判、应急响应支持、安全态势感知服务、安全运营服务等，提高集团提供网络安全公共服务的能力。

二是针对信息安全意识、安全技能、热点安全事件等定期组织安全培训，辐射整个集团，对集团各级单位进行网络安全业务培训，形成常态化工业信息安全人才队伍建设与培养机制，增强各级各部门网络安全意识和防护水平。

（2）提升集团多方协同管理能力

依托大数据技术建立集团工业互联网安全感知分析能力，对集团建立监测、预警、多方协同管理机制，形成面向集团-生产基地-生产车间三级长效协同工作机制，全面提升集团多方协同作战能力，提升整体安全态势感知和分析能力，实时掌握集团工业互联网安全态势。

（3）建立集团安全合规管理机制

以《网络安全法》、行业标准、指南等为依据，建立集团安全合规管理机制，打造精细化、差异化的科学管理方式。开展现场安全检查和信息调查，针对集团进行定期及不定期的巡视检查，通过建立集团工业网络安全检查机制，借助线上监测加线下检查来形成管理合力，摸底各下属单位的网络安全状况。

（4）建立数据信息共享机制

集团系统实现集团与各生产基地的数据信息共享机制，形成数据上传、下达，纵向与各级单位系统的数据贯通和业务协同，实现网络安全数据的高效上报，并且能够接收上级指派的任务与工作指令。

（5）建立跨部门协调指挥体系

根据《生产基地应急管理办法》相关要求，为积极落实责任要求，加快集团协同协作机制建设，本项目实现了集团总部、生产基地、生产车间、技术支撑服务机构等在生产基地安全层面上的协作、互通，进一步完善监测预警、信息通报、应急处置等相关机制的建设。

2.2.5 单位基本信息

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于2007年。以云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大方向为市场战略。已形成覆盖网络信息安全生命全周期的产品体系，包括网络信息安全基础产品、网络信息安全系统以及网络信息安全服务，各产品线及业务线在行业中均形成了强大的竞争力。作为国家级核心安保单位，安恒信息参与了近乎全部国家重大活动网络安保，实现15年重保零事故。2023年10月8日，安恒信息圆满完成杭州亚运会网络安全保障工作，以先进的理念和专业的服务获得各盛事主办方和监管机构的一致好评。

2.3 案例三：工业领域数据安全诊断系统——解决工业企业数据安全问题，提高企业的数据安全水平和风险防范能力

本方案在山东电力设备有限公司部署工业安全态势感知平台、工业数据安全监测与审计系统和工业网络安全监测与审计系统等安全系统，接入其办公网、生产网和集团内网网络流量，针对工业数据安全风险、网络威胁和工控异常行为，实现 7*24 小时常态化安全检测和审计，并对发现的数据和网络安全风险进行警示和预警，对存在的数据及网络安全风险进行分析、评估和汇总，并以此依据提出针对相应风险的处置建议，为企业风险控制、消除风险提供指导，提升工作效益和为安全提供保障。

2.3.1 方案概述

1.方案背景

为深入贯彻落实《国务院关于深化“互联网 + 先进制造业”发展工业联网的指导意见》（国发〔2017〕50 号），2022 年 3 月 31 日工网安函【2022】235 号关于征求开展工业互联网安全深度行活动意见建议的函，2022 年 5 月《工业和信息化部办公厅关于开展工业互联网安全深度行活动的通知》工信厅网安函【2022】97 号推动在全国范围内深入实施工业互联网企业安全分类分级管理的要求，《中华人民共和国数据安全法》第 29、30 条加强风险监测、发现数据安全缺陷、漏洞、事件等风险时应当立即采取处置措施并告知用户和向有关主管部门报告、重要数据的处理者定期开展风险评估、并向有关主管部门报送风险评估报告意见，《山东省工业和信息化领域数据安全管理实施细则》要求的建立覆盖本单位相关部门的数据安全工作体系。

本方案通过对山东电力设备有限公司 3 个网络区域的持续监测，梳理了企业工业资产情况、网络威胁和数据安全风险实时预警，掌握总体安全态势，支撑安全决策和规划。通过项目方案实施为电力企业提供分类分级全生命周期安全服务，包括工业互联网企业分类分级综合管理、企业安全防护能力建设、企业态势感知呈现，对接省工业互联网安全监测与态势感知平台，实现 IT 与 OT 的融合分析，

提供安全监测和预警通报、威胁溯源、公共安全服务技术手段，实现工业互联网相关企业安全态势可感、可知、可监管，为工业互联网发展保驾护航。

2.方案简介

随着智能化、信息化技术的不断发展，越来越多的新兴技术在电力系统中不断应用，使得电力监控系统所涉及的技术、工作量、工作难度在这个过程中大幅增长。此外，现代电力监控系统使用计算机网络技术取代了传统分布式厂站自动化设备技术，带来便携的同时也让电力行业数据资产暴露在多重网络威胁中。传统封闭的网络变得越来越开放，在提质增效的同时，也带来暴露面扩大、网络边界模糊等新的安全风险。工业数据规模化增长速度越来越快，内外网数据交互流通、海量数据集中汇聚分析等提供了更多窃取、篡改数据的路径，扩大了攻击面，网络与数据安全面临愈发严峻的风险隐患，实施工业安全分类分级、加强工业数据安全保障刻不容缓。

在 2023 年 5 月 4 日—2023 年 7 月 30 日，借助山东未来网络研究院安全团队的科研能力及安全技术手段，对山东电力设备有限公司指定网络区域进行安全监测，接入办公网、生产网和集团内网网络流量，针对工业数据安全风险、网络威胁和工控异常行为，实现 7*24 小时常态化安全检测和审计，并对发现的数据和数据安全风险进行揭示和预警。

通过对不同网络区域3个月的持续监测，发现的资产、网络威胁和数据安全风险总体情况如下:

- **资产发现**：现网识别到生产、研发、运维、管理等共22类，共7159条工业数据资产，其中重要数据7048条，核心数据9条。共发现办公网、生产网和集团内网共819台工业资产，包括工控上位机、下位机、触摸一体机，智能终端、文件共享服务器、数据库服务器等。

- **数据安全风险：**现网未授权访问、接口敏感数据明文传输、异常跨境访问、弱口令、匿名访问等5类数据安全风险，共62494条，占总体审计数据的0.51%。

- **网络威胁：**现网特洛伊木马通信、挖矿木马、僵尸网络、暴力破解、远控工具使用、WEB攻击等6类网络威胁，共440935条，占总体审计数据的3.6%。

➢ **工控异常行为：**现网发现重启接入服务器、非授权操作、发送空消息、跨安全区域通信等4类工控威胁和工控异常行为，共23254条，占总体审计数据的0.19%。

➢ **高风险主机：**监测发现32台主机存在网络威胁、数据安全风险和工控异常行为，包括：感染挖矿木马、特洛伊木马、僵尸网络等恶意程序，成为受控主机，并存在与境外IP通信、对内外网IP发起暴力破解攻击、高危指令执行等攻击行为。

因此，山东电力设备有限公司目前针对工业互联网数据安全风险发现、实时告警、防护处置等能力欠缺，主要体现在。

- 工业互联网数据安全监测与防护体系尚未建立，企业侧工业互联网数据安全监测节点部署数量较少，企业级、地区级、国家级上下联动的数据安全保障机制不完善。
- 数据安全可信交换共享不充分。
- 数据要素资源有效配置确权定价难。

因此，通过本项目实施工业互联网数据安全监测分析技术，可以对数据访问、存储、共享、披露、删除等环节进行全流程安全监控，避免非法访问、无序存储、违规共享、恶意披露与删除等问题。同时，可以实现多源数据采集、数据识别、流量监测、人工智能分析、数据安全风险分析及综合研判等一站式解决办法，形成面向工业互联网数据安全监测的整体解决方案。

工业互联网数据安全诊断系统可以解决很多工业互联网企业数据安全问题，提高企业的数据安全水平和风险防范能力。

3.方案目标

实时检测山东电力设备有限公司工控网络的网络威胁、数据安全风险，掌握整体网络安全和数据安全态势。

(1) **提升工业互联网数据的安全性：**工业互联网数据安全诊断系统能够及时发现和解决数据在存储、传输和处理等环节的安全问题，避免数据被黑客攻击或泄露，从而提升数据的安全性和可信度。

(2) **增强工业互联网的风险防范能力：**通过实时监测和防护，课题能够及时发现和应对各种数据安全威胁，有效防范黑客攻击和内部人员泄密等风

险，保障工业互联网平台的稳定运行。

(3) **促进工业互联网的发展和创新：**项目方案的研究将推动工业互联网领域的技术创新和产业升级，为工业互联网的发展提供有力的技术保障。同时，课题的研究能够提升企业在工业互联网平台上的核心竞争力和创新力，为企业创造更大的价值。

(4) **推动国家工业信息安全的发展：**项目的研究不仅涉及到工业互联网数据安全，还涉及到国家工业信息安全。因此，研究不仅有利于企业自身的利益和发展，也有利于国家层面的信息安全管理，推动国家工业信息安全的发展。

总之，本项目方案的研究对于提升工业互联网数据的安全性和风险防范能力具有重要意义，同时也有助于推动工业互联网和国家工业信息安全领域的技术创新和发展。

2.3.2 方案实施概况

本项目将工业安全态势感知系统部署在山东电力设备有限公司企业二楼机房内，共计 3 台设备，包含工业网络安全监测与审计、工业数据安全监测与审计、工业安全态势感知平台 3 个子模块。部署示意图如图 3-1 所示：

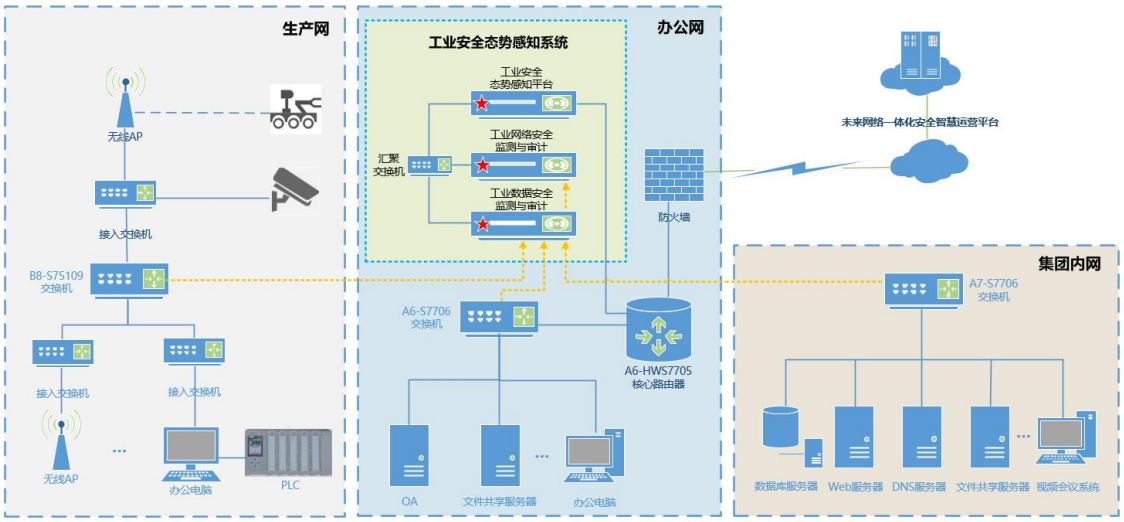


图 3-1 工业安全态势感知系统部署示意图

工业安全态势感知系统通过流量镜像方式，接入办公网、生产网、集团内网交换机，实现对 3 个网域的流量采集，运用融合探针深度解析技术，对流量中数

据资产进行识别及分类分级，对网络安全和数据安全风险事件的监测分析、研判、预警。

工业安全态势感知平台汇聚工业网络安全监测与审计模块、工业数据安全监测与审计模块的多源异构数据，通过多场景大数据安全分析引擎、安全知识库等技术，实现工业资产测绘，工业数据分类分级管理，网络安全、数据安全风险实时监测和预警，威胁溯源，安全态势感知和策略管理等功能；通过汇集网络安全和数据安全风险事件进行关联分析，呈现主机威胁画像，提高对复杂情况的判断能力，辅助安全决策，构筑电力企业内部的安全底座。

1. 方案总体架构和主要内容

（1）方案总体架构

工业数据安全诊断系统通过底层工业数据安全融合分析系统对各类型数据进行采集解析、数据还原、数据安全检测、数据安全威胁检测、数据异常跨境检测，结合多维度的安全分析研判引擎和威胁情报信息进行自动化分析，针对企业内部已知和未知威胁进行实时监测。

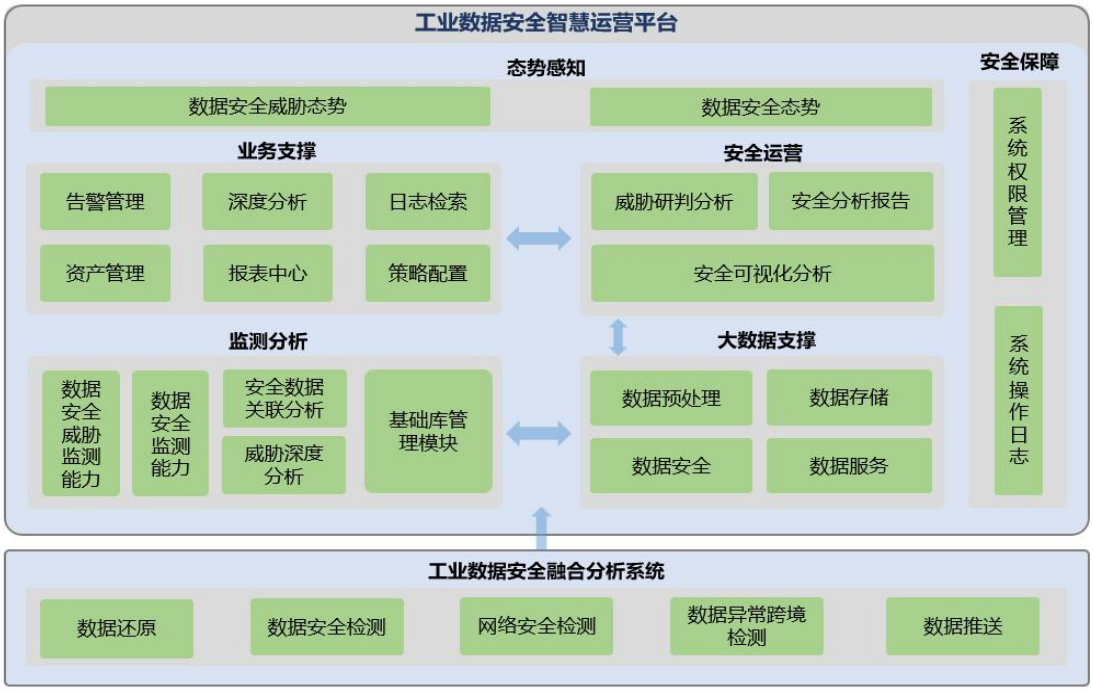


图 3-2　总体功能架构图

同时，对工业数据风险进行研判，对风险主机进行画像和威胁行为回溯和预警。通过海量安全事件关联分析结合安全知识库，实现精准实时的安全告警，极

大提升安全事件处置效率，并通过安全规则自动化提取，构建安全风险、攻击手法和威胁数据等规则模型，积累形成网络安全知识库（见图 3-2）。

（2）方案技术方案

实现平台的各种具体功能，如日志检索、深度分析、告警管理、报表分析、资产管理、策略配置等，具体如下：

1）日志检索

提供接入的原始数据查询和检索功能。同时，通过对原始数据的统计和分析，向用户展示威胁事件分布，归属区域，攻击趋势，威胁等级，失陷主机等维度的分析结果，如图 3-3 所示：

图 3-3　网络威胁日志图

2）数据资产梳理

对企业网络中的数据资产进行发现、检测、“清单式”管理，对其中重保、涉敏的网络数据资源进行集中、统一监管，做到摸清家底、资产清查、理清思路、完善管理（见图 3-4）。

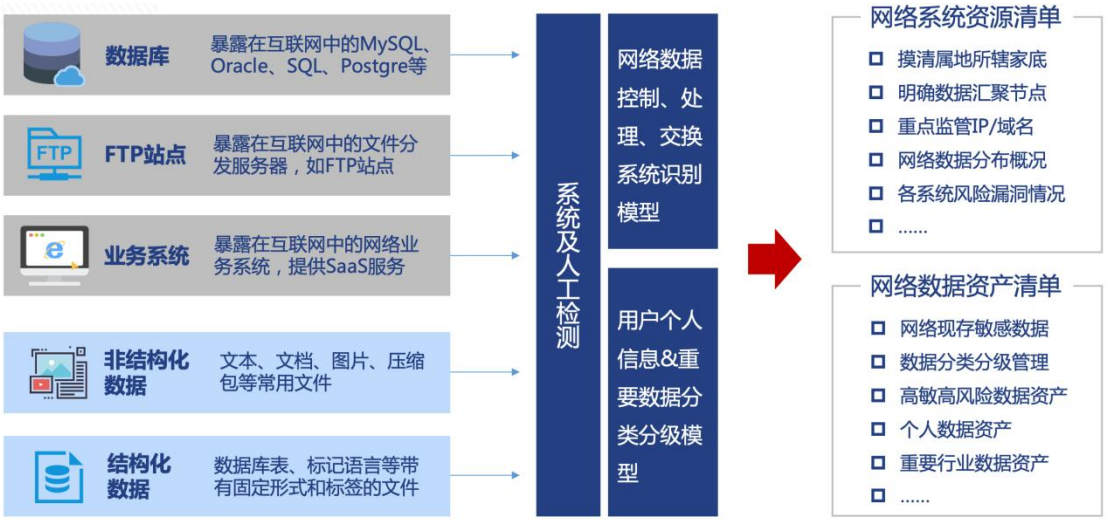


图 3-4　数据资产梳理

3）网络数据深度分析

基于 ATT&CK 安全分析模型，对威胁事件和攻击行为进行攻击链溯源和取证，如图 3-5 所示，通过对各类威胁事件基于攻防视角等多维度归类，依托安全分析模型和各攻击阶段的攻击路径和手法进行关联分析，为用户还原完整的攻击过程和攻击影响范围，并针对攻击者和被攻击者进行行为回溯和画像。

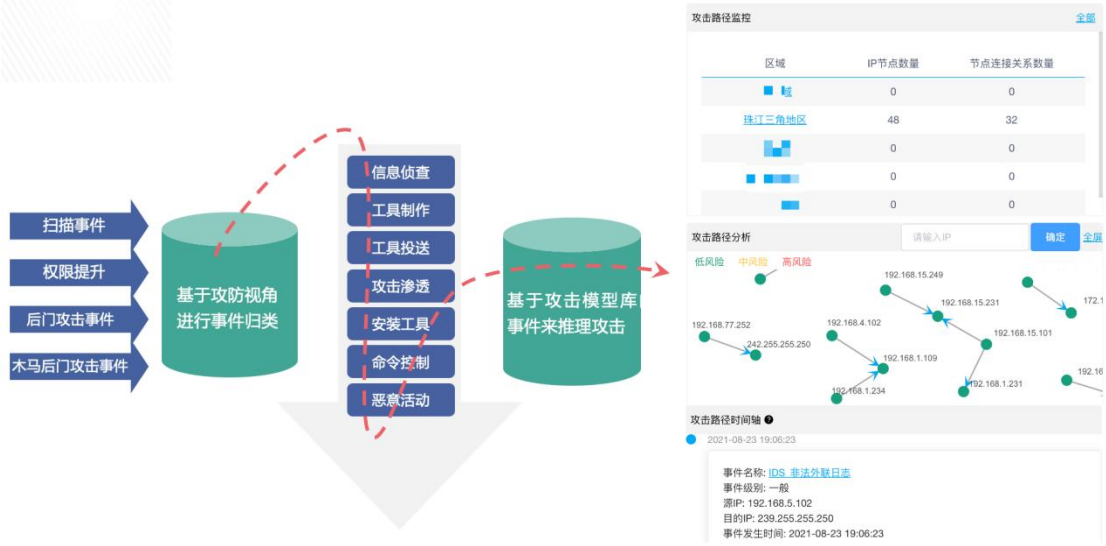


图 3-5　网络威胁深度分析模型和结果图

4）数据安全风险还原和追溯

针对数据安全风险，在发现企业内网的数据安全风险后，对风险事件进行还原和追溯，得到风险主机及系统数据安全风险的证据链，为后续分析研判、策略运营和数据安全风险处置提供支撑（见图 3-6）。

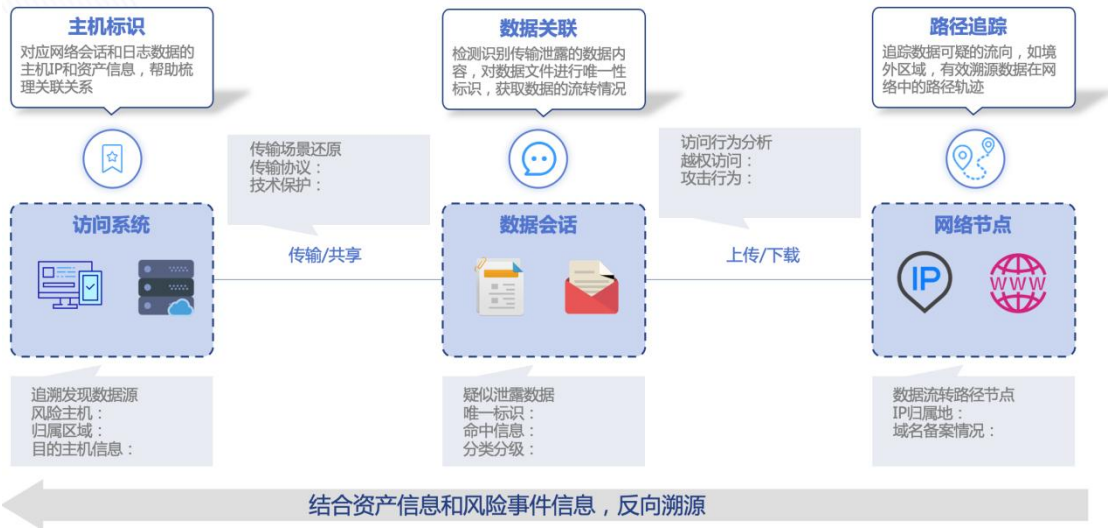


图 3-6　数据安全风险的还原和追溯

5）告警管理

平台基于接入的多源异构数据和告警规则产生安全告警，从攻击方向（由外向内，内部横向和由内向外等）以及主机状态等多个维度，向客户展示资产的安全风险和面临的威胁状态，并进行预警（见图 3-7）。安全告警类型包括：

- 外部攻击告警

攻击者绕过和突破企业网络边界防御，由外向内向企业内资产发起攻击和威胁，例如：扫描探测、暴力破解、恶意文件传播等。

- 风险外联告警

企业内资产，与外部主机或攻击者发生异常通信行为，可能导致敏感数据泄露，包括：https 隐蔽隧道、dga 域名请求、http 隐蔽隧道、暗网通信等。

- 横向扩展告警

发现攻击者在企业内网中横向渗透的攻击行为，例如，企业内资产之间的扫描探测、暴力破解、漏洞利用等行为。

- 主机异常告警

发现工控终端和系统状态异常，包括：CPU 使用率异常、网卡状态异常、通信状态异常等主机状态异常。

6）报表分析管理

告警报表：记录系统检测到的数据威胁事件、网络攻击预警等信息，提供事件时间、威胁等级、影响资产等内容。用户可以选择时间段和事件类型生成相应报表，可导出Excel格式。

资产报表：详细记录企业网络内部的各类网络资产，如服务器、路由器、工控设备等的型号、配置、系统版本、运行状态等信息。资产报表可按不同维度分类导出。

7）资产管理

平台支持下列 3 种资产数据接入方式：

- 与客户已有的资产管理平台对接，接入资产数据。
- 与第三方资产扫描系统对接，接入资产探测结果。
- 手动录入，提供资产录入模板，实现资产数据的一键导入。

同时也接入资产的漏洞数据，并针对漏洞，从漏洞类型、危害级别、区域分布等多个维度，将资产与漏洞进行关联分析，对高风险资产向客户进行预警，如图 3-8 所。

图 3-7 安全告警示意图

图 3-8 资产与漏洞的关联分析

覆盖范围包括工业企业 IT 域和 OT 域等节点流量、工业设备和系统、网络设备和安全设备等设备日志数据，基于平台大数据技术手段，实现资产的自动识别和分类分级管理：

数据资产自动识别：通过汇聚企业内 IT 和 OT 域安全数据，结合丰富的工业协议指纹、敏感数据指纹和资产测绘引擎，实现工业数据资产的自动化、智能识别，为数据的分类分级管理奠定基础。

数据分类分级管理：对企业全网数据资产进行发现、检测、“清单式”管理，对其中重保、涉敏的网络数据资源进行集中、统一监管，做到摸清家底、资产清查、理清思路、完善管理。

8）策略配置

策略配置包括区域配置、数据来源、范化策略和关联规则等功能模块，其功能是实现多源异构数据的统一接入，以及安全分析规则配置和运营，为安全告警，深度分析和攻击行为回溯等功能提供支持（见图 3-9）。

图 3-9 范化策略设置图

关联规则模块是安全分析知识库和规则库，通过规则的配置和运营，针对接入的多源异构数据进行多维度关联分析，产生安全告警和深度分析结果。在多源异构数据统一接入的基础之上，平台提供灵活、人性化的配置框架，帮忙用户进行规则配置和运营，如图 3-10 所示。

图 3-10 告警规则配置图

9）安全运营支撑

■ 威胁研判分析

通过构建威胁研判分析引擎对监测发现的风险数据进行深入分析，基于访问逻辑、攻击链分析、特定协议的深度业务逻辑分析和事件特征匹配，快速定位问题影响和源头；基于研判引擎识别出的高精准安全事件，按照主机 IP、事件类型等关键信息进行聚合展示，业务分析人员可以清晰的看到受害企业及相关事件信息；同时，支撑研判规则的新增、编辑和删除，网络威胁告警日志命中研判规则后，并满足安全事件规则特征的条件后，即会生产相应安全事件记录。

■ 安全分析报告

系统实现了多种类型报表的灵活生成与导出功能，用户可以按需提取所需的数据信息。通过提供丰富的报表类型，快速方便地下载提取各类数据威胁相关数据信息，更全面地满足企业数据威胁及安全管理的监管需求。

■ 安全可视化分析

数据安全风险态势是对数据安全事件、涉及敏感文件、跨境目的地国家和风险企业等方面的监测和分析，提供了全面的数据安全态势信息，及时掌握数据安全状况，发现问题并及时采取措施。

图 3-11 数据安全态势展示平台

■ 数据安全威胁态势

围绕企业资产风险和安全告警，向客户展示资产的漏洞分布、告警趋势和实现主机排名等信息，帮助企业实时掌握高风险资产和告警，并对其进行及时处置；

从外部、内部和横向三个方向和维度，展示威胁事件的类型排名、趋势变化，同时从攻击阶段的维度，展示不同攻击阶段的威胁事件（见图3-11）。

图3-12 综合态势展示平台

10）安全保障

■ 系统权限管理

➢ 系统设置。平台支持配置日志存储查询和系统运行监测策略和邮件服务配置。支持登录管理策略配置，可以设置用户连续登录失败最大次数、超时登录，支持数据备份和恢复等系统层面配置。

➢ 区域管理。为达到用户能对资产进行组织化管理的目的，平台支持创建分组和分支，以及对资产绑定分组和分支，帮助企业合理、高效、有序地管理资产。

➢ 用户管理。平台支持用户管理、角色管理和权限配置。用户包括用户名、密码、真实姓名、工号、联系电话、邮箱、角色选择、IP 认证等信息。

■ 系统操作日志

平台支持记录并存储用户登陆、登出的用户日志和系统操作日志，可满足网络安全法规要求的180天存储要求，可帮助安全运维者进行平台操作日志溯源，及时追溯、取证平台管理员的安全操作。

（3）项目主要功能

1） 数据还原

支持通用协议的识别和内容还原，可识别 HTTP、SMTP、POP3、FTP 等协议，并针对协议内容进行还原，对通过通用协议传输的工业互联网数据进行分析识别。设备支持对流量采集的协议识别和样本捕获还原，以及基于实时流量对文本、图像、邮件等文件的还原能力。设备对流信息进行识别，识别有效的负载包，对流量包进行重组，还原、解码，还原数据文本、图像、文档、邮件等文件。支持工业协议的驱动层适配和芯片级匹配，可精确识别工业互联网流量，设备支持工业协议会话级话单，可识别 Modbus 、Profinet、S7、MQTT 等 100 种主流工业互联网协议、物联网协议。可根据后端应用系统的需求，可对系统进行配置，实现对输出的字段信息扩充或减少，按需输出所需要的字段日志会话数据。

2） 数据安全威胁检测

对工业网络的网络攻击行为进行实时监测，通过对异常操作行为、工控异常指令的解析，及时定位分析数据威胁问题，发现网络攻击、违规操作等可能产生安全事故的风险，为安全事件的溯源取证提供依据。对工业生产网络进行监测审计，满足工业安全监测的合规要求，降低安全责任风险。

3） 数据安全检测

基于深度包检测技术、数据包还原的技术，支持工业数据识别、工业数据安全风险监测、工业数据跨境监测、导致数据安全风险的网络攻击检测等。根据工业数据的分类分级标准，结合传统的特征匹配等技术，并采用深度学习等 AI 技术，对工业数据（包括文本、图片、文档等）进行深入分析。

4） 数据异常跨境检测

对敏感数据传输、异常流转、异常跨境等安全风险和异常行为进行监测和审计，满足数据安全法、工业互联网分类分级等合规要求，降低安全责任风险。

5） 数据推送

基于规整和归一化的数据，进行封装和加密等自动化处理流程，系统支持通过向导式、可视化和人性化的设计，构建伸缩性强的字段映射规则和数据字典，支撑数据自动化封装。数据上报遵循相应接口规范，自动完成数据上报准备工作，包括数据核验、封装、加密和推送等。

2. 网络、平台或安全互联架构

（1）系统部署全图示意

综合考虑山东电力设备网络拓扑、已建设安全能力、网络和数据资产，以及工业领域网络安全和数据安全合规要求。建议安全防护体系采取“安全分区、网络专用、网间隔离、操作授权、持续监测”的总体策略，具体如下：

采用工业数据安全威胁和风险监测系统，对安全分区的流量进行安全分析，常态化监测数据安全风险、网络威胁、工控威胁；

通过工业数据安全认证网关，加强访问控制以及各安全分区内的授权管理；

通过工业主机防勒索系统，防护 OT 域工业主机环境安全；

通过工业数据安全智能分析预警平台，接入网络设备、安全设备等多源异构安全数据，实现工业数据分类分级管理、安全风险统一分析、威胁溯源、安全风险预警、安全态势感知。

最终建成数据安全风险、网络威胁的事前预警，事中监测，事后溯源处置的整体安全防护体系，如图 3-13 示意。

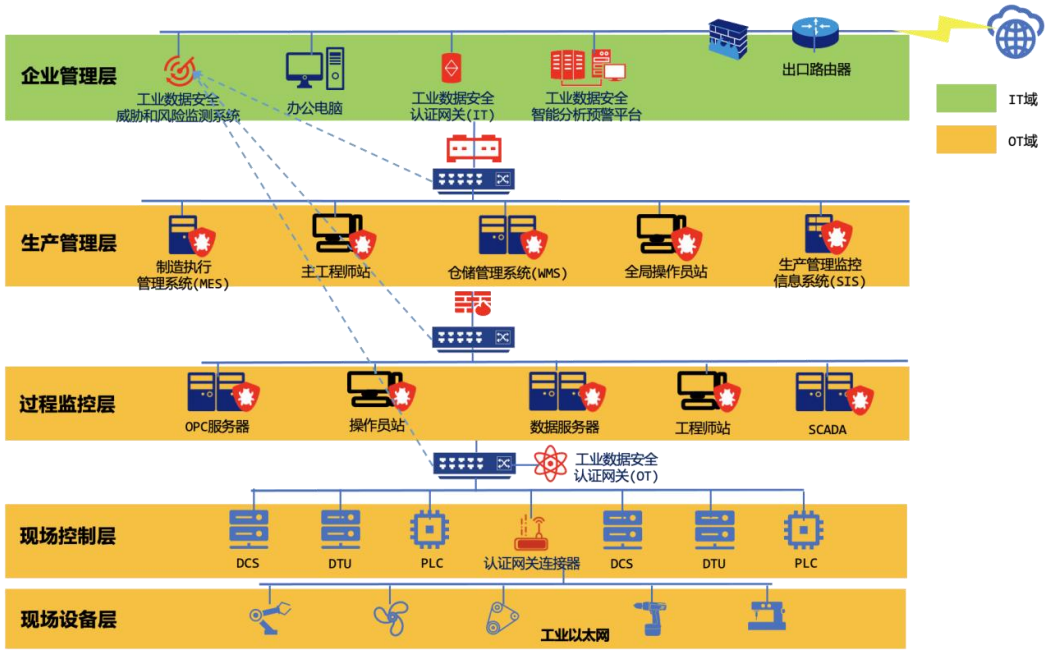


图 3-13 系统部署全图示意

（2）项目网络部署

本次在山东电力设备有限公司部署工业数据安全融合分析系统 1 套、工业数据安全智慧运营平台 1 套。

1） 部署说明

本次系统部署包含 4 台物理设备，单台设备高度 2U，额定功率 550W、采用双路供电，支持 19 英寸标准机柜安装，机柜深度不小于 1000mm（见表 3-1）。

表 3-1 设备部署清单

产品名称	单位	数量	备注
工业数据安全融合分析系统	套	1	共 3 台，单台 2U 机架式
工业数据安全智慧运营平台	套	1	共 1 台，2U 机架式

资源分配：本项目中涉及 4 台硬件设备，需要 IP 地址数量需求如表 3-2 所示：

表 3-2 IP 地址需求数量

序号	设备名称	IP 地址数量
1	工业数据安全融合分析系统	3
2	工业数据安全智慧运营平台	1

2） 网络部署拓扑

根据调研企业 IT 域网络流量，测算各工业数据安全融合分析系统通过 10GE 光口的数量，与交换机互联进行镜像多源异构数据的采集；各通过 1 个 GE 电口与交换机互联，用于向工业数据安全智慧运营平台上报数据，进行智慧分析研判，呈现各维度数据安全监测情况。部署拓扑如图 3-14 所示。

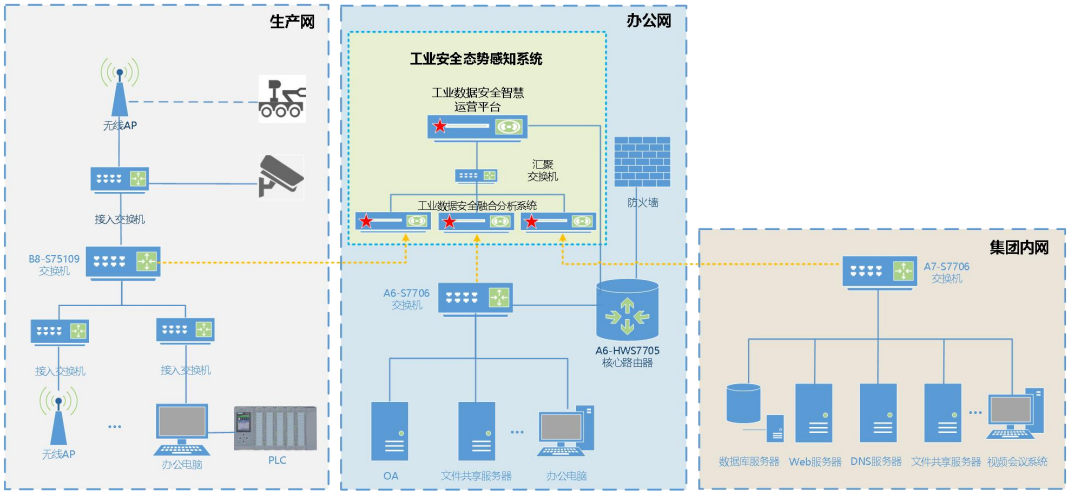


图 3-14 部署拓扑图

3） 部署位置

根据现场机房工勘情况，本次将工业数据安全融合分析系统、工业数据安全智慧运营平台分别部署于山东电力设备有限公司指定机柜内，采用 220V 交流供电方式。

3. 具体应用场景和安全应用模式

1）安全应用场景

项目方案后续对工业互联网企业各行各业均适用。

本次项目实用于工业企业的资产整体测绘、数据安全监测、网络数据安全威胁识别及溯源、态势感知呈现及省企对接服务。

2）安全应用模式

项目的建成，极具推广价值，这个项目的安全应用模式，主要体现在以下几个方面发挥效果:

a.能够快速实施部署并达到既定效果，发挥试点区域先行示范的良好作用，为后续向全国工业互联网企业建设积累足够的建设经验，发挥试点区域现行示范的良好作用。

b.解决工业互联网企业网络数据安全痛点需求，如对监管部门要求理解不透彻，对省企接口规范了解不深入，难以满足监管部门的合规要求。

c.针对不同企业提供分类、分级差异化安全解决方案，开拓工业互联网服务客户市场，对分级分类工作提供全面保障，从企业安全全方位支撑工业互联网企业分级分类保障工作，建立实战化常态化安全技术手段，形成支持工业互联网安全发展合力。

4. 安全及可靠性

本项目将通过构建工业领域数据安全诊断能力，实现工业互联网企业全周期生命安全体系保障，从工业互联网企业互联网网络底层设计出发，采用多种先进的安全技术手段，为我国工业互联网的数据安全提供了有效的监测、预警、通报、协助处置能力。

该项目的实施，将会为工业互联网领域的发展提供有效的安全保障。具体包括:

（1）为工业互联网行业健康发展提供有效保护

我国是制造业大国，加快建设和发展工业互联网，推动互联网、大数据、人工智能和实体经济深度融合，发展先进制造业，支持传统产业优化升级，具有重要意义。通过本项目的研发，建设工业互联网安全态势监测与感知技术手段，有效应对网络安全攻击，形成与工业互联网发展相匹配的安全保障能力，为我国深化“互联网+先进制造业”战略的顺利推进和推广保驾护航。

（2）构建工业互联网安全监管技术体系

工业互联网作为产业互联网新业态，建设企业级工业互联网平台，有利于增强企业安全防护能力，为行业主管部门的安全技术保障提供支撑，为行业主管部门政策制定、安全监管、事中处置、事后溯源提供强有力协同共治。

（3）提升企业效益

a.加强全员安全意识普及：通过本项目的开展，经过一段时间后，我们有理由相信，员工的安全意识将得到极大的提高。在日常生活中和工作中发生安全事故的可能性将大大降低，由此造成的经济损失也会大大减少。

b.通过平台的建设，能够帮助企业全面掌握工业控制的网络资产及资产运行情况，可获取加入资产分析中的所有设备运行状态、安全事件等信息，有助于帮助公司在今后信息安全建设决策及系统升级、优化等方面提供科学决策的数据依据，避免后期信息化建设的投资失误和资金浪费。

c.平台开启关联分析功能，能够帮助管理员准确并快速定位安全事件发生源头，同时还能够帮助运维技术人员快速分析故障、准确定位故障点、高效排除故障，有效减少生产网故障中断数量和中断时间，保障生产网高效、稳定运行。

d.通过实时运行监控和 AI 分析能够尽早检测、提前预测到发生在工控网络中的攻击行为，在攻击发生前及发生过程中迅速定位事件，并在其造成危害前将其制止，有效避免安全事故发生带来的损失。

e.工业控制网络中数据绝大部分属于涉密信息，一旦被泄露出去，被非法人员利用，可能造成设计企业和国家的重大损失。通过平台能够及时发现和避免由于管理疏忽造成的数据泄露现象，减少因人员操作管理失误造成的损失。

5. 其他亮点

本项目在工业电力企业的成功实施，对电力行业数据安全治理提供有效的示范。

（1）促进安全数据和情报共享

本项目将监测分析企业关键节点的海量数据，并在此基础上建成分析计算能力，对数据安全事件和威胁情报具备全网的规模化采集，可为集团内部相关企业提供数据支持。

（2）促进网络流量采集监测技术发展

关键节点的数据采集涉及到企业内部多个网域，是对工业数据安全进行管道侧监测处置的关键环节。本项目利用现有企业关键节点的流量采集监测分析能力，实现对工业互联网协议、应用、安全威胁的分析能力支持。根据我国基础通信设施发展规划，涉及工业相关的关键网络节点链路和网络流量仍在将未来 10 年保持高速增长，预计针对关键网络节点的监测采集设备和技术应用前景十分广泛，市场容量每年约 50～100 亿左右，本项目成果将具备良好的市场化前景。

（3）推动数据挖掘及人工智能技术在工业互联网范围的应用推广

本项目在企业安全的基础上对安全形势进行分析、预警和处置，可用于支持各相关行业部门对数据安全的治理防控指挥等一系列工作。本项目预期的研发成果包括新型工业安全人工智能分析预测研判算法，是对 AI 人工智能前沿技术在工业互联网安全领域的探索和应用，未来既可以对算法进行推广和共享，也可以将算法的研发、训练、优化设施和软件框架进行开放共享，提升和促进行业研发能力。

（4）为数据安全监管提供决策依据

推动集团工业数据安全体系建设，提升行业总体安全能力，保障国家工业互联网数据安全战略实施。从全球范围来看，工业数据安全尚处于初步发展阶段，工业互联网信息安全防护、认证、标准等体系都还处于不断完善的过程中。因此，对于我国工业数据安全发展而言，想要通过借鉴发达国家的工业数据安全发展模式，快速提高工业数据安全水平难度很大。本项目对工业数据安全标准的完善，将有力推动集团工业数据安全体系建设。

（5）灵活的接入安全设备

方案产品支持丰富的探针类型，包括工控漏扫、工控防火墙、工控网闸、工控入侵检测、工控监测审计、工控主机卫士等，同时支持第三方设备接入，客户可根据实际网络、预算情况选择安全探针进行部署，灵活组合不同类型的探针。

（6）领先的安全检测能力

支持安全合规检测、异常攻击检测、非法外联检测、设备运行状态检测、内网异常访问检测、非法程序启动检测、APT 攻击检测、恶意加密流量检测等。

（7）全面的安全分析技术

方案支持汇总各类安全数据，运用关联分析、用户画像、模型分析、威胁情报等安全技术，有效发现各类安全事件与风险隐患，识别漏报及误报行为，提升安全运维工作效率，形成实时监测、动态感知的整体安全分析能力。

（8）智能的识别工业资产

通过工业资产指纹识别技术，全面发现工业互联网资产，从工业设备、主机、应用、业务等多个维度建立资产库，对网内资产进行实时安全监控，呈现网络安全风险、脆弱性等安全信息，为客户提供强大的资产管理与安全监控手段。

（9）多维度安全态势感知

从资产的脆弱性、威胁和攻击等多个视角全面分析工业网络系统安全态势。通过人工智能和大屏可视化技术，直观呈现全网拓扑视图、告警趋势、实时告警等工业安全态势。

2.3.3 下一步实施计划

1. 平台分析能力进一步提升

工业数据分类分级精准度需进一步提高: 工业数据涉及数据量大、范围广、种类多，需要结合人工根据数据遭受窃取、篡改导致的后果对分类分级模型进行训练，以提升分类分级精准度。

工业网络与数据面临的复合型风险识别提升:将工业网络与数据综合分析进而识别出安全风险，需要依据网络流量与数据内容、安全设备日志建立风险识别模型，识别模型对风险识别的准确度有待进一步提高。

2. 协议私有化问题导致数据包难以分析，需要进行进一步研究提升

加密流量分析难度高: 加密流量分析面临数据无法直接读取、算法难破解等多重困难挑战，需要依靠统计分析、机器学习、协议逆向等技术进行流量特征提取和协议格式推断，在信息受限的条件下实现流量的有效分析。

3. 加大加宽研究方向

进一步扩展工业数据分类分级管理和安全防护体系研究，提升企业防护水平，在产业中推广应用。扩展采集和识别的工业协议种类，适配 90%以上的主流工业协议。扩展移动互联网、物联网技术范围的安全分析能力，尝试将平台的数据监测能力扩展到移动 APP 等新技术领域。

2.3.4 方案创新点和实施效果

1. 方案先进性及创新点

（1）方案先进性

a.国内同类型测试验证对比优势

平台已通过第三方机构科技查新，查新结论为“目前国内未见与本查新项目研究内容相同的文献报道”。经与同类型工业互联网安全测试验证产品对比，山东省工业互联网安全测试验证平台在仿真实验环境个数、样本库一体化协同监控、数据全流量采集和分析技术、评估指标自定义管理及全面性方面的优势如表 3-3 所示。

表 3-3 关键技术指标与国内外主流或前沿指标比较

关键技术指标	山东省工业互联网安全测试验证平台	国内同类型测试验证产品
工业互联网仿真实验环境	模拟 10 个重要行业典型工艺流程。	模拟 5 个典型工艺。
样本库监控组态	一体化协同。	独立监控。
数据全流量采集和分析技术	对 Mysql、SSH、Telnet、OPC UA、Https、RDP、Ethernet/IP、DNP3 和 FTP 流量进行识别，还支持 Siemens S7、Modbus 等工业协议流量的采集，并分析其特征码和功能码。	多针对 TCP/IP 相关协议及部分工业协议开展流量分析，未能分析特征码和功能码。
评估指标管理	实现自定义检查指标库设计，支持工业互联网安全相关测试评估指标的自定义管理。	指标项均为固定型，无法根据用户需求调整测试指标。
全面性	可对 IT 和 OT 侧的设备、主机、安全设备进行功能性、适用性和安全性测试验证。	主要针对 IT 侧的主机、安全设备进行测试验证。

b.集中管理，满足合法合规要求

通过对工业数据资产、安全设备的集中管理、网络流量的全面分析、数据安全风险、安全事件集中告警，帮助企业以全局视角进行风险评估，从而提升企业数据安全和网络安全管理水平，满足工业数据分类分级、网络安全分类分级、等保 2.0 合规要求。

c.持续监测，实时掌握风险

通过对全网流量的持续监测，包括工业资产识别、漏洞发现、威胁监测、异常行为分析等，实时将数据安全风险、网络威胁可视化。支持单个、分组、全局等资产的风险分析，并能基于风险等级及告警，进行进一步的溯源分析。

d.动态防御，提升安全决策能力

联动企业各类安全设备及数据，实现安全数据全面整合，消除信息孤岛、提升安全分析的准确性，降低误报漏报，帮助企业识别和关注重点安全风险，快速修复安全漏洞、及时处置安全事件，最大程度降低事件影响范围，形成动态安全策略，构建整体安全防御体系。

e.关联分析，可视化呈现数据安全态势

通过对工业数据的采集、传输、使用、共享、销毁等数据处理阶段和全生命周期数据安全风险监测，以及综合态势、资产态势、数据风险态势等大屏，可以帮助客户全面可视化了解全网安全态势。

（2）方案创新性

a.企业安全能力建设

- 建设工业互联网完整基础资产库：工业互联网资产是其安全监测和预警的基础。本项目通过备案数据、主动探测、流量分析、特征识别等多种机制，形成覆盖全国各省的工业互联网资产库。
- 构建工业互联网特色安全知识库：构建最全面最权威的工业特征和安全知识库，提升安全管理能力。基于工控专用协议的盲识别与逆向解析技术。
- 工控设备深度信息扫描技术：通过工控漏洞互联网深度扫描技术，结合CNVD工控漏洞库，对目标区域的工控接入互联网设备进行深度扫描，从而实现攻击威胁和风险隐患识别预警，有效提升工业互联网资产发现能力。
- 大数据、云计算、人工智能关联分析技术：关联分析是对暗含攻击行为的安全事件序列建立关联规则。工业互联网网络安全公共服务平台可对网络攻击事件等建立关联。

b.建立多方联动安全管理和预警机制

通过建立工信部、省、企业等多方联动监测和预警机制，实现网络数据安全威胁数据共享、知识库共享、应急能力共享的全方位联动响应。

c.先进的技术路线

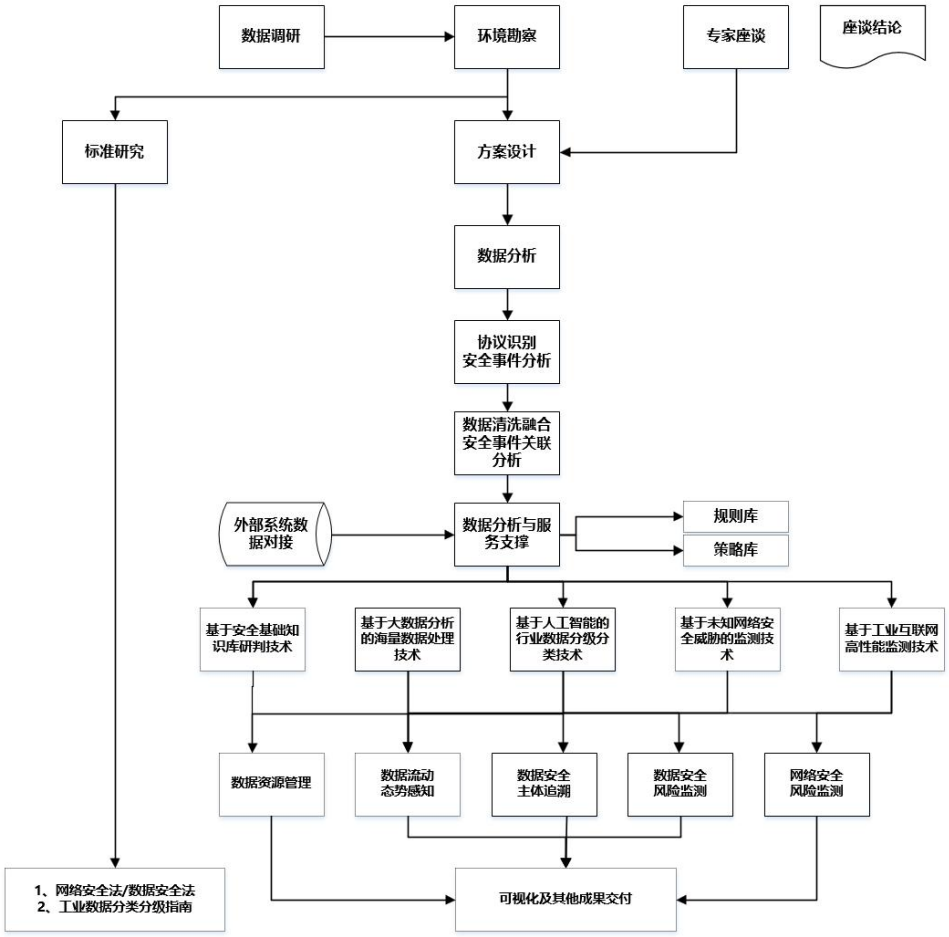


图 3-15 项目方案的技术路线

面向工业行业数据安全智慧运营平台的技术路线包括详细的数据调研、标准、专家详细论证、关键技术方案设计等，确保项目技术路线先进、合理。

- **数据调研：**针对企业内部网络环境及已有系统等进行调研，了解后续规划，重点利用工业数据安全融合分析系统的监测覆盖能力，通过部署实现大范围网络安全和数据安全风险监测。
- **专家座谈：**邀请安全企业、工业等重点领域、行业的数据安全专家，针对网络数据资产进行全方位梳理和分级分类，开展重要数据检测识别、数据异常流动监测、安全事件追踪溯源、数据安全事件阻断等技术方案进行座谈、可行性分析。
- **标准研究：**根据《网络安全法》《数据安全法》等相关政策文件的制定进展和精神要求，结合行业数据安全标准体系成果以及企业标准规范实

践情况，贯彻制定数据分类分级、数据安全风险类型等功能指标，保障数据安全风险监测和态势感知工作的体系性、标准性及有效性。

- **关键技术方案设计：**根据数据调研的结论、标准研究成果以及专家座谈结果等，对项目中使用的关键技术进行设计。

2. 实施效果

通过对山东电力设备有限公司 3 个网络区域的持续监测，监测总体发现如下资产、网络威胁和数据安全风险:

■ **资产发现**

现网识别到生产、研发、运维、管理等共 22 类，共 7159 条工业数据资产，其中重要数据 7048 条，核心数据 9 条。

共发现办公网、生产网和集团内网共 819 台工业资产，包括工控上位机、下位机、触摸一体机，智能终端、文件共享服务器、数据库服务器等。

■ **数据安全风险**

现网监测发现：未授权访问、 接口敏感数据明文传输、异常跨境访问、弱口令、匿名访问等 5 类数据安全风险，共 62494 条，占总体审计数据的 0.51%。

■ **网络威胁**

现网监测发现：特洛伊木马通信、挖矿木马、僵尸网络、暴力破解、远控工具使用、WEB 攻击等 6 类网络威胁，共 440935 条，占总体审计数据的 3.6%。

■ **工控异常行为**

现网监测发现：重启接入服务器、非授权操作、发送空消息、跨安全区域通信 等 4 类工控威胁和工控异常行为，共 23254 条，占总体审计数据的 0.19%。

■ **高风险主机**

监测发现 32 台主机存在网络威胁、数据安全风险和工控异常行为，包括：感染挖矿木马、特洛伊木马、僵尸网络等恶意程序，成为受控主机，并存在与境外 IP 通信、对内外网 IP 发起暴力破解攻击、高危指令执行等攻击行为。

1）工业资产识别和分类分级详情

工业资产的识别和分类分级情况见表 3-4。

表 3-4 工业资产的识别和分类分

工业资产识别详情

序号	工业资产类型	归属网络	主机数量（台）	协议数量（种）	主机IP网段
1	办公电脑，DNS服务器，工控上位机，工控下位机	办公网	255	57	128.126.130.0/24，192.168.0.0/16
2	触摸一体机，智能终端，工控上位机，工控下位机	生产网	204	15	172.16.0.0/12
3	办公电脑，DNS服务器，文件共享服务器，数据库服务器	集团内网	360	32	10.94.0.0/16

工业数据资产识别分类分级详情

序号	工业数据类型	归属网络	数据级别	数据量（条）	归属主机（IP）
1	协同研发数据	办公网	核心	5	128.126.130.129
2	共 10 类： 安全运维记录，售后咨询数据，安全管理日志，人员薪酬，物流公司数据，资产库信息，人员招聘考勤信息，设备运行监测数据，供货商数据，合同	办公网	重要	261	128.126.130.126，128.126.130.142等 9 台主机
3	共 4 类： 制造商数据，人员招聘考勤信息，产能统计数据，企业基础信息	生产网	重要	902	172.16.16.21
4	共 2 类： 协同研发数据，贸易信息	集团内网	核心	4	10.94.16.114，10.94.17.21
5	共 12 类： 制造商数据，人员招聘考勤信息，售后咨询数据，产能统计数据，合同，人员薪酬，设备故障数据，供货商数据，功能性能测试数据设备运行监测数据，运维操作日志，维修服务数据	集团内网	重要	5896	10.94.17.21，10.94.16.32等 21 台主机

2）数据安全风险详情

厂区异构数据复杂多样，缺乏工业数据安全风险审计手段、缺乏有针对性的工业数据资产识别和分类分级管理策略（见表 3-5）。

表 3-5 数据安全风险

序号	数据风险类型	数据风险描述	数据风险危害	数据风险处置方式	防护建议
1	数据泄露风险	**重要和核心数据明文传输到外网：** **风险描述：**128.126.130.129（办公网）使用明文的方式，向部署在外网阿里云上的云巡检平台(xjrfid.com)，传输重要和核心数据。此外，云巡检平台存在Web明文口令泄露风险，极易导致重要和核心数据泄露事件发生。 **涉及数据：**重要数据（安全运维记录-安全巡检日志）、核心数据（协同研发数据-巡检系统数据字典开发代码）	1. **数据泄露**：通过监听和劫持网络通信，攻击者可以获取明文传输的数据，包括数据库用户名密码、服务器账号密码以及数据库内容等敏感信息； 2. **数据篡改**：攻击者可对明文传输的数据进行篡改，从而导致数据的完整性受到破坏； 3. **安全性低**：明文传输的数据容易被窃取、篡改和伪造，安全性非常低。	1. **使用加密协议传输数据**：通过使用加密协议如HTTPS等，对传输的数据进行加密，保障数据的机密性和完整性。 2. **安全审计**：对于系统的网络通信和数据传输进行监控和审计，及时发现和报告异常事件和行为，确保系统的安全性和稳定性。	1. **部署工业数据安全威胁和风险监测系统**，对传输的文件、图纸等信息进行分类分级管理，针对核心数据、重要数据进行重点监测，对重要、核心数据流转异常行为（包括IP地址异常、时间异常等）情况进行预警； 2. **部署工业实时数据库审计、数据防泄漏系统**，监测和记录工业系统中的数据处理活动，保护关键数据和系统的完整性。 3. **部署工业数据安全智能分析预警平台**，实现数据安全风险集中分析、管理和预警。
2	未授权访问风险	**风险监测预警系统和邮件系统存在未授权访问和弱密码** **风险描述：**山东电力风险监测预警系统（部署在外网，http://123.232.107.115:28080），可通过未授权访问（不需要密码），直接进入监控页面，查看系统数据源、WEB URI、SQL语句等信息，查看厂区监控画面和数据库查询详情。 **风险描述：**内网邮箱系统（10.94.212.15:mail.cee.com.cn）存在弱口令，极易遭受暴力破解攻击，造成数据泄露。 **涉及数据：**重要数据（安全运维记录-安全隐患信息），一般数据（厂区监控画面）。	1. **数据泄露**：未经授权的用户或攻击者可能访问重要核心数据被窃取、滥用或传播，导致数据泄露和声誉损害。 2. **数据篡改**：攻击者可修改、破坏或操纵数据，导致数据的完整性丧失，对企业流程、决策和合规性产生严重影响。 3. **服务中断**：攻击者可使用未授权访问或弱口令来破坏系统、网络或应用程序的正常运行，导致服务中断、停机时间增加和业务中断。	1. **加强访问控制**：对于非法或未授权的访问请求进行拒绝或限制，只允许授权的用户或系统调用接口。 2. **安全审计**：对于系统的网络通信和数据传输进行监控和审计，及时发现和报告异常事件和行为，确保系统的安全性和稳定性。	1. 针对账号密码，建议**加强密码强度**； 2. 工业主机侧**启用加密传输机制**，防止数据被篡改和窃取； 3. **部署工业数据安全威胁和风险监测系统**，对网络中传输的数据进行数据识别和流转异常等风险监测 4. **部署工业数据安全认证网关**，加强访问控制以及各安全分区内的授权管理。

3）网络威胁详情

缺乏纵深网络监测防御手段，主机感染恶意程序较多，缺乏工控主机防病毒功能和工控网络威胁、异常行为常态化监测能力（见表 3-6）。

表 3-6 网络威胁

序号	网络威胁类型	网络风险特征	涉及工业主机IP地址	网络风险处置方式	防护建议
1	挖矿木马、特洛伊木马	1. 常见的攻击方式为弱口令攻击、漏洞利用、软件供应链攻击等； 2. 工业主机被植入挖矿木马后，最明显的特征为内存和CPU利用率升高，企业用电量以及用电费用呈增长趋势； 3. 挖矿木马并不一定以挖矿为目的，而是以通过增加管理员权限、关闭系统防火墙和安全防护软件等，盗取企业数据为目的。	内网IP 128.126.130.129存在与矿池IP 95.168.216.7及矿池域名webmine.cz通信十余次，系统告警描述为挖矿木马加密流量通信。该域名和IP均已被情报系统标记为恶意，判定该内网主机已感染挖矿木马。 内网IP 128.126.130.138 访问麻辣香锅恶意软件远控域名 db.testyk.com 、du.testjj.com 共 12 次，通常为感染木马病毒造成的访问行为。 内网IP 128.126.130.142 存在访问恶意软件 Flystudio 相关 IP 及域名 faf6.com 行为30 次，该恶意软件为窃密软件。	1. 隔离被感染的服务器或主机 2. 确认挖矿进程 3. 清除木马	1. **加强密码策略**，增加密码复杂度并进行定期修改，开启相关登录失败处理功能； 2. **安装工业主机防勒索系统**，有效阻止通过网络和U盘等引入系统的病毒、木马以及0-Day漏洞，创建主机进程白名单； 3. **部署工业网络安全监测与审计设备**，从网络流量行为发现挖矿木马、远程控制等网络攻击行为； 4. **部署工控防火墙**，清晰划分网络安全边界，层层阻击非法网络行为，创造工控白环境；
2	僵尸网络	1. 远程控制：僵尸网络最主要特征是攻击者能够远程控制受感染的计算机，执行各种恶意操作，如发起分布式拒绝服务（DDoS）攻击、传播垃圾邮件等。 2. 大规模攻击：僵尸网络通常由大量受感染的计算机组成，攻击者可以集中这些资源来发动大规模网络攻击，对目标造成严重影响。	内网 IP 128.126.130.142 存在访问DGA 域名行为，所访问的五个域名均存在可读性差、解析 IP 在境外等特点，符合 DGA 僵尸网络域名利用算法随机生成特征，判定该主机感染了僵尸网络病毒。	1. 隔离受感染的计算机：立即隔离感染主机，阻止其访问网络，防止感染的计算机继续参与攻击或传播恶意软件。 2. 移除恶意软件：对于受感染的主机，使用安全软件和工具来检测和清除恶意软件。	1. **部署工业数据安全威胁和风险监测系统**，从网络流量行为发现僵尸网络病毒受控主机与C&C域名访问行为； 2. **安装工业主机防勒索系统**，自动扫描系统生成文件级别白名单，防止病毒入侵；
3	工控异常行为	1. 高危指令执行：工业控制系统中，攻击者或恶意软件通过执行危险指令，操纵或破坏关键工业过程的行为，可造成工业过程中断，设备破坏，生产数据损坏等危害。 2. 异常通信行为：非授权工控主机和终端接入工控网络，并执行非授权操作。工控通信异常，工控指令和操作执行报错等异常行为。	内网IP 128.126.130.100 给 36.148.158.218（IP归属地：湖南长沙），111.14.92.70（IP归属地：济南市天桥区），内网IP 128.126.130.139 给 39.154.170.76（IP归属地：内蒙古鄂尔多斯准格尔旗）共下发 6 条网络接入服务器重启指令。 内网IP 128.126.130.80、128.126.130.173、128.126.130.139等 5台主机，监测发现发送工控空消息和异常指令导致服务器报错。 生产网IP 172.16.16.21与集团内网存在大量API接口调用和文件共享访问（超过700次）等跨域访问行为。	1. 排查和全盘查杀下发高危指令和通信异常的工控主机，是否感染恶意病毒，立即停止高危指令执行，以及异常工控通信行为，必要时可断网。 2. 明确工控系统和网络访问控制权限并进行有效配置和访问控制，阻止非授权跨安全域访问和操作。	1. **部署工业数据安全威胁和风险监测系统**，从网络流量行为发现僵尸网络病毒受控主机与C&C域名访问行为； 2. **安装工业主机防勒索系统**，自动扫描系统生成文件级别白名单，防止病毒入侵； 3. **工业数据安全认证网关**，加强访问控制以及各安全分区内的授权管理。

2.3.5 单位基本信息

北京亚鸿世纪科技发展有限公司（简称“亚鸿世纪”）成立于 2012 年，2017 年正式成为任子行网络技术股份有限公司的全资子公司，是一家专注于互联网空间数据治理、网络与信息安全及数据增值解决方案及服务的高科技公司。公司在北京和武汉设有分公司及研发基地中心，能够快速响应客户安全需求。目前研发中心技术人员达到 400 多人，其中 985、211 高校毕业人数达到 80%以上。

公司成立以来，协助工信部起草《IDC/ISP 信息安全管理系统技术要求》、《IDC/ISP 信息安全管理系统接口规范》、《域名信息安全管理系统技术要求及接口规范》、《数据核验技术要求及接口规范》等多项技术规范。公司目前已经承建了工信部全国统一资源协作管理系统、工信部全国域名信息安全管理系统、工信部互联网大数据管理子系统、设备运维子系统、全国 25 省通信管理局互联网网络与信息安全综合管理平台、19 省移动 IDC/ISP 信息安全管理系统、17 省联通 IDC/ISP 信息安全管理系统、14 省铁通 IDC/ISP 信息安全管理系统、5 省电信 IDC/ISP 信息安全管理系统。在 IDC/ISP 信息安全领域市场综合占有率达 80%以上，在互联网反欺诈安全市场占 50%以上。具备丰富的互联网信息安全和网络安全的实战经验以及相关安全能力。

2.4 案例四：面向电子信息行业的工业互联网安全态势感知平台——江西省工业互联网安全风险监测预警体系

随着工业数字化、网络化、智能化的加快发展，新形势下工业互联网安全工作的重要性和紧迫性更加凸显。为有效应对工业互联网企业面临的网络安全风险和威胁，中国联通研究院联合北京天融信网络安全技术有限公司（以下简称“天融信”）共同建设面向电子信息行业的工业互联网安全态势感知平台，有效提升江西省工业互联网企业网络安全监测与态势感知能力，实现网络安全风险的实时监测和及时预警，为工业互联网安全发展提供了新的思路和方向。

2.4.1 方案概述

1.方案背景

工业互联网通过系统构建网络、平台、安全三大功能体系，打造人、机、物全面互联的新型网络基础设施，形成智能化发展的新兴业态和应用模式。工业互联网由传统的 IT 网络和用于控制生产运行的工业 OT 网络组成，因此，工业互联网企业除面对传统 IT 网络安全风险外，还必须面对来自 OT 网络的全新安全风险。传统 IT 网络有着几十年的历史，仍旧存在很多的安全风险问题，一是人员对信息化的安全防护意识不高；二是为了便于网络中的信息传输和交换，开放非必要端口，由此给了植入病毒木马的机会；三是操作系统本身存在的漏洞和缺陷逐渐被黑客攻击。而在生产网络 OT 层面，是一个全新的安全领域，尤其近几年，勒索软件对工业企业频繁攻击，工业控制系统自身又出现一系列问题，引起工业企业高度重视，工业生产环境中较多的设备、系统逐渐与互联网相连，甚至非法外联，使得边界越来越模糊，又缺少必要的安全措施，并且安全措施难以实施。

在现阶段和未来工业互联网蓬勃的发展情况下，构建全方位的 IT 网络和 OT 网络的综合技术保障是工业互联网企业安全发展的前提。江西省工信厅为加强工业信息化安全管理，组织构建工业互联网安全态势感知平台，通过平台使监管单位全局洞悉本区域工业互联网的网络安全态势，并结合工业互联网威胁情报中心与响应中心的情报，及时发现可能面临的安全威胁和风险，实现安全风险预警响应。

2.方案简介

项目面向江西省电子信息行业建设一套行业级工业互联网安全态势感知平台，依据平台形成本地化的工业互联网安全技术支撑体系和专业技术力量，构建工业互联网安全风险预警体系，并实现平台侧、网络关键节点侧、企业侧安全能力联动，有效提升本地区工业互联网安全整体保障水平。

项目建设内容包括工业企业安全监测系统、网络关键节点监测系统、工业互联网安全风险预警系统等。平台具备工业互联网流量全面监测、全局态势展示、自动化风险预警处置等安全功能，通过在不少于20家工业企业互联网接入侧部署工控安全信息采集与防护感知探针设备，快速精准识别网络中各种已知和未知网络威胁，有效防范重大网络安全事件发生。

3.方案目标

为有效应对工业互联网企业面临的安全威胁，解决工业互联网安全风险无法快速发现、无法精准识别、缺乏风险预警手段等安全问题，本项目以提升区域工业互联网安全态势感知能力为目标，建成涵盖全市区域的重点工业企业网络安全态势感知平台，为工业企业提供监测、预警、应急响应等支撑能力，依托平台形成本地化的工业信息安全技术服务支撑体系和专业技术力量，构建覆盖全市的工业互联网安全监测和态势感知能力，并实现国家、省、市联动，有效提升本地区工业互联网安全整体保障水平。

项目基于成熟产品与自主可控技术，通过定制开发等工作，打造网络安全工作开展的支撑平台，全局洞悉工业互联网安全运行情况，结合工业互联网威胁情报中心与响应中心的情报，及时发现并预警网络中可能面临的安全威胁和风险，以便企业开展响应处置工作，有效降低网络安全事件发生概率。

2.4.2 方案实施概况

项目的实施建成，可以实现对辖区、电子信息行业内重点工业企业的安全监测，监测范围覆盖企业大多数工控网络，可以识别企业内的资产网络信息，分析企业内网存在的安全风险隐患，针对高危网络安全风险及异常操作发出告警。并可实现风险预警联动，联合主管部门、工业互联网企业、应急支撑单位等相关机构，建立线上或线下对接，向相关单位提供风险预警信息。同时通过汇集企业侧

安全数据及省级平台下发的各类安全监测数据，进行交叉关联和数据分析，从企业、行业、地域等多维度分析工业互联网安全风险特点、重点企业安全趋势，宏观把控辖区整体安全态势。

1.方案总体架构和主要内容

项目构建江西省电子信息行业工业互联网安全态势感知平台，依托集中化技术能力，起到省级平台与企业级平台的连接枢纽作用，围绕主管部门工业互联网安全监管需要和企业需求，通过流量分析、日志采集等技术手段，构建集数据汇聚、安全分析、风险预警等与一体的态势感知平台，实时感知电子信息行业工业互联网安全态势。

面向电子信息行业的工业互联网安全态势感知平台包括以下子系统:

- 工业企业安全监测系统
- 网络关键节点安全监测系统
- 大数据融合分析展示系统
- 安全风险预警系统

项目总体架构如下图所示:

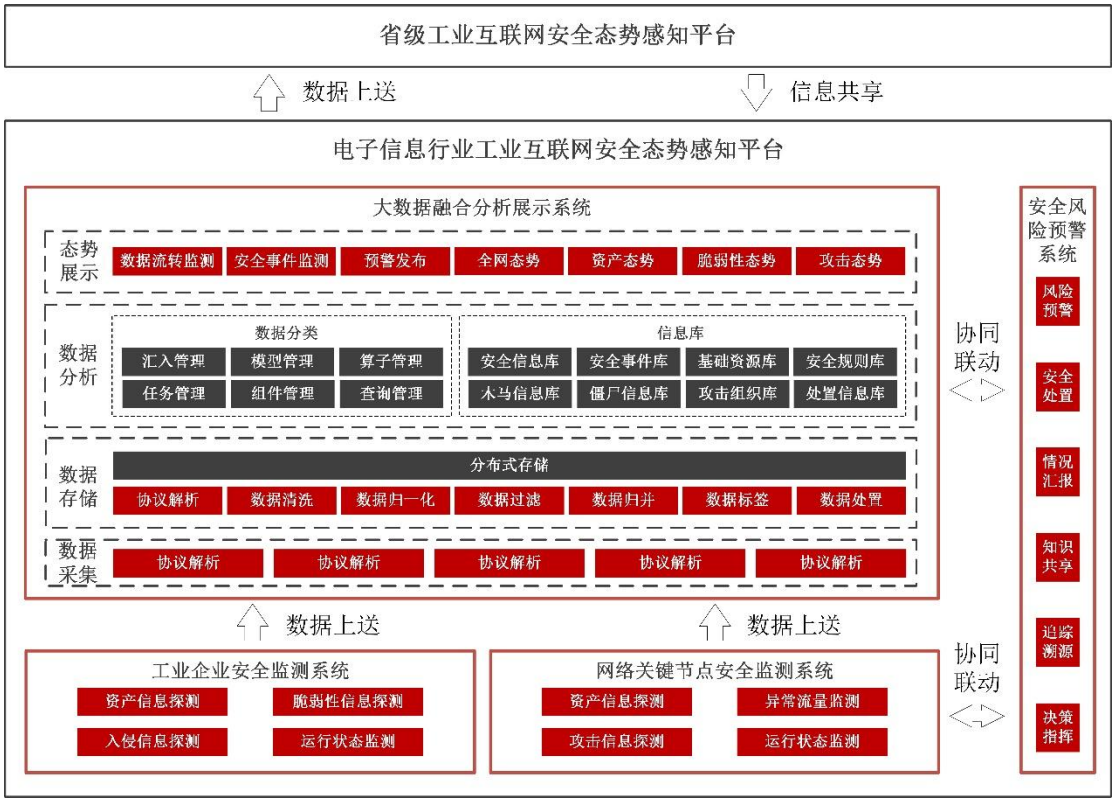


图 4-1　项目总体架构

项目组织实施方案主要从以下四个方面进行建设:

一是工业企业安全监测系统实施。在工业企业生产内网运维管理区中，旁路部署工控安全信息采集与防护感知探针设备，通过探针自身具备的扫描管理、漏洞验证、策略管理等功能对工业企业侧安全状态进行监测，将网络中存在的脆弱性信息、异常信息等通过 syslog 方式上传至大数据融合分析展示系统，同时存储在本地便于后期的检查。

二是网络关键节点安全监测系统实施。网络关键节点安全监测系统是整个平台的重要组成单元，这一系统包括流量监测探针，在辖区内重要工业企业、工业互联网平台企业、重要 IDC 机房等互联网网络出口部署流量监测探针设备，通过对上述关键节点的网络流量采集解析，实现工业互联网相关业务分析，包括资产监测、安全事件监测、漏洞分析验证等。探针的分析结果通过接口上报到大数据融合分析展示系统进行统一处理。

三是大数据融合分析展示系统实施。大数据融合分析展示系统硬件设施主要包括数据采集服务器和存储分析服务器。其中数据采集服务器实现对所有监管的工业企业和传输工业数据的运营商所有流量和数据的采集汇总，存储分析服务器用于不同业务区域独立的数据存储备份和分析使用。系统支持全网安全态势感知、事件通报预警、应急处置、威胁可视化和威胁情报等功能，同时该系统开放接口与省级态势感知平台进行数据交互和共享。

四是安全风险预警系统实施。构建统一指挥调度的工业互联网安全风险预警通报平台，对工业互联网网络中各种威胁因素和发现的安全事件等内容，进行通报预警，为下一步快速处置安全事件做好准备；根据安全事件的发生和传递的线索，对威胁源进行追溯，对安全事件进行侦查调查、取证，有效防范和打击网络攻击等违法犯罪活动；对网络中的监管对象进行实时的安全监测并结合最新的情报信息，及时发现网络环境中的漏洞、病毒木马等脆弱性及威胁信息，遵循相关等级保护机制要求，实现对全网络业务保护支撑。

项目实施完成后，能够实现工业互联网安全态势感知平台与联网工业企业/工业互联网平台企业之间数据对接及交互共享，同时接受省级平台下发的联网资产、攻击诱捕、风险通报等数据，上报辖区内企业侧安全态势感知数据，便于监管单位全面感知辖区内工业互联网安全态势，向区域内主管部门、工业企业等提

供威胁信息情报支撑服务。

2. 网络、平台或安全互联架构

（1）网络互联架构

本项目网络互联架构如图 4-2 所示，项目通过在联通机房部署工业互联网安全态势感知平台软硬件设施，辅以工业互联网企业内部署的安全探针，实现面向电子信息行业工业互联网企业以及运营商等网络关键节点的安全监测能力和安全风险预警能力。

工业互联网安全态势感知平台部署在联通数据中心机房，其中硬件设施包括数据存储服务器、FTP 服务器、数据分析子系统服务器等设备，软件包括大数据分析系统、融合分析展示系统、风险预警系统等系统。面向电子信息行业的工业互联网安全态势感知平台与省级工业互联网安全态势感知平台进行对接，数据通过互联网加密传输至省级平台。同时平台可通过设置的互联网接口接收来自第三方支撑单位的威胁情报、安全事件上报等信息，并且将监测到的安全风险信息下发给支撑单位，以便支撑单位提供风险研判、安全运维、应急响应等安全服务。

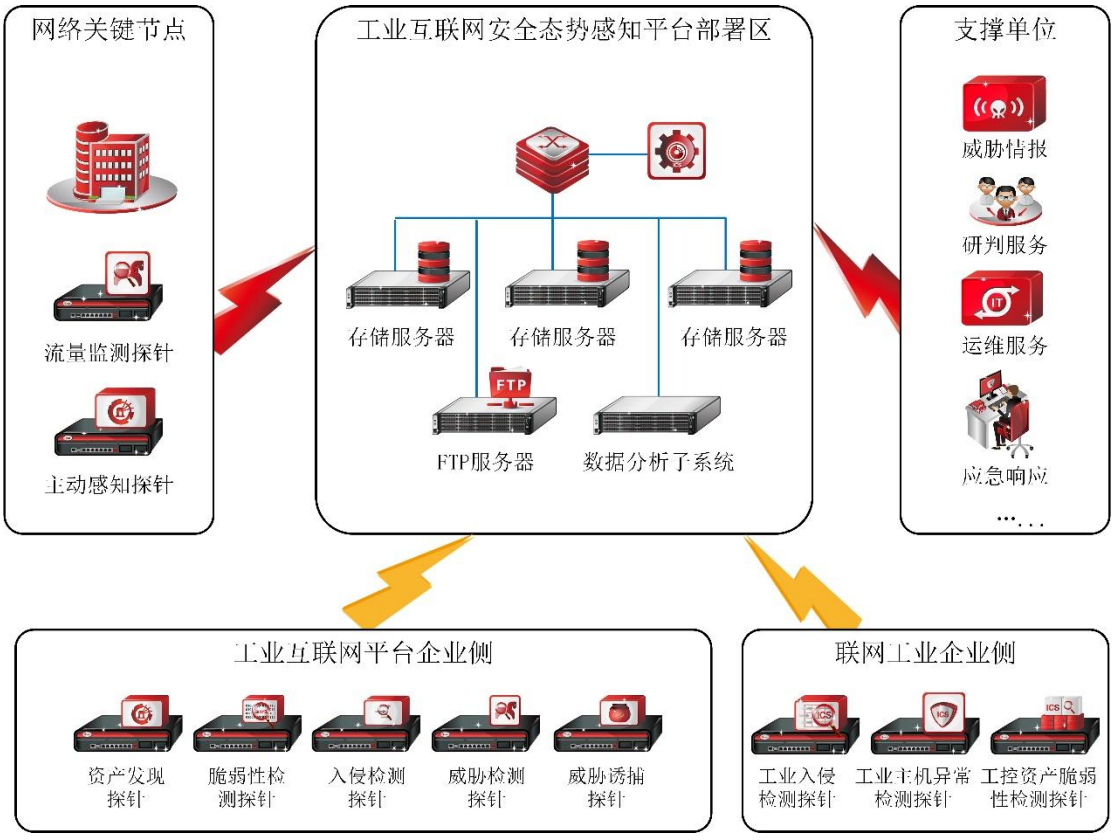


图 4-2　部署架构示意图

联网工业企业侧内工业入侵检测、工控资产脆弱性检测探针旁路部署在工业企业生产内网核心交换机处，工业主机异常检测探针部署在生产内网运维管理区中，各类探针连接汇聚交换机后通过光纤连接工业互联网安全态势感知平台，将采集的数据经过加密后以 syslog 方式上传至工业互联网安全监测与态势感知平台，同时存储在本地便于后期检查。

工业互联网平台企业侧各类检测探针旁路部署于互联网出口路由器处，探针采集数据经过互联网加密传输后以 syslog 方式上传至工业互联网安全监测与态势感知平台，同时存储在本地便于后期检查。

网络关键节点侧流量采集探针部署于地市级运营商网络出口路由器旁路，筛选符合工业通讯协议的相关流量，以及符合工业企业侧、平台企业侧发送或接受流量，各流量采集探针本地生成日志记录，经过互联网加密传输后以 syslog 方式上送至探针集中管理平台，然后由探针集中管理平台统一上送至工业互联网安全态势感知进行深度分析。

（2）探针说明

本项目应用流量监测探针、资产发现探针、脆弱性检测探针、工业入侵检测探针等多种安全监测探针，实现在网络关键节点、重点工业企业的安全数据采集、日志存储和数据上送。

1）流量监测探针

流量监测探针设计的系统架构如图 4-3:

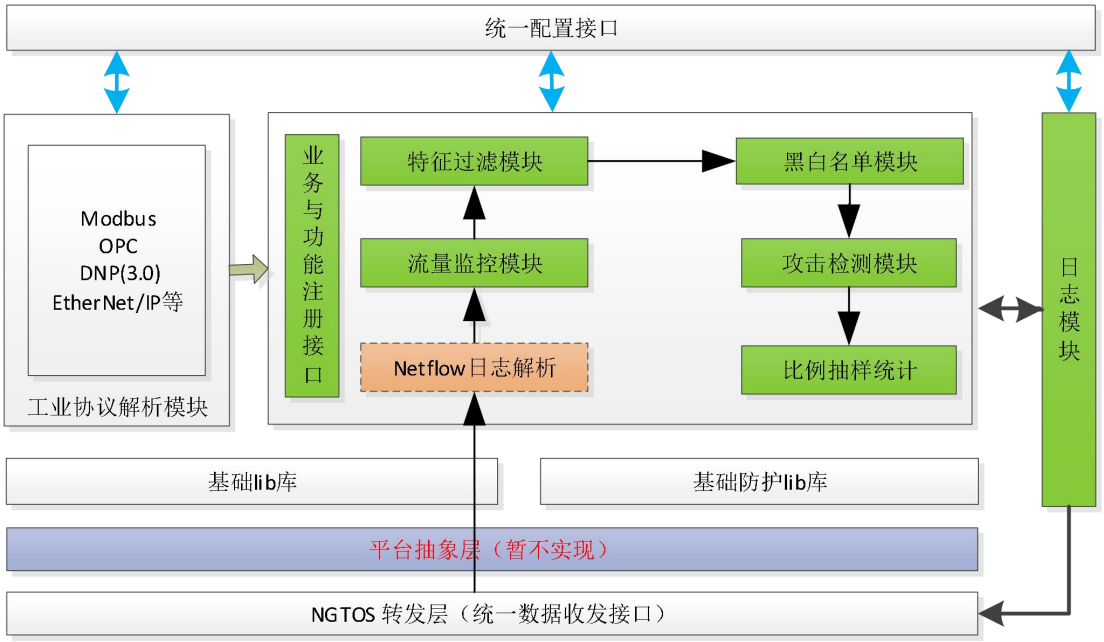


图 4-3　流量监测探针系统架构

流量监测探针部署后能够实现如下安全功能:

a.首先对已经识别的异常流量进一步深度分析，提取 IP 等要素，然后根据黑名单和特征，二次验证匹配，对命中条件的异常 IP 流量直接报警，日志模块记录相关报警信息。

b.对异常流量的 IP 的地址进行追踪溯源（基于 IP 地址库或者其它 IP 库资源），从而定位到该 IP 对应的相关企业用户。

c.对该企业 IP 的异常流量进行多种监控连接行为分析，对源发起的异常连接进行分析检测。

d.对异常流量上报，以供平台进一步深度人工分析。

2）主动感知探针

主动感知探针系统架构如图 4-4:

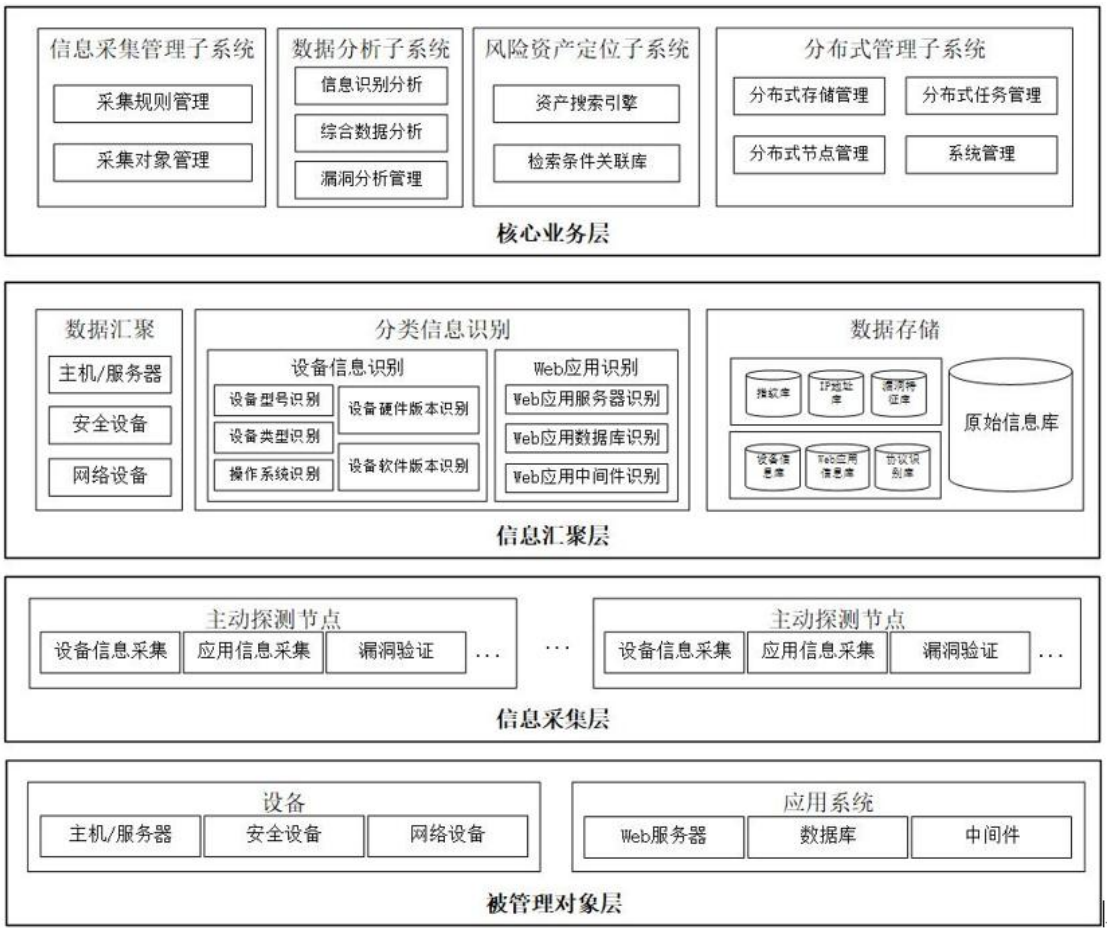


图 4-4　主动感知探针系统架构

主动感知探针由 4 个层次组成，包括被管理对象层、信息采集层、信息汇聚层、核心业务层。主动感知探针支持主动发现互联网中的设备、应用系统等对象，

经过对探测到的信息汇聚分析后，感知被管理对象的安全风险。

a.被管理对象层：包括各网络设备资产主要组成部分，包括各类主机/服务器、安全设备、网络设备、工控设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等，系统将通过网络对这些对象信息进行主动探测与收集。

b.信息采集层：包括分布式部署的各个主动探测节点，这些节点通过主动探测对资产基础信息进行采集，如设备 IP、设备类型、厂商、地理信息、开放端口、中间件类型与版本等。

c.信息汇聚层：将信息采集层获取的信息进行数据的抽取、转换和加载后，以基础资源知识库中的指纹数据为识别依据进行分类信息的识别，并将分类识别后的数据信息进行存储。

d.核心业务层：包括分布式管理子系统、信息采集管理子系统、数据分析子系统以及风险资产定位子系统，其中分布式管理子系统负责分布式节点管理、分布式存储管理和分布式任务调度以及其他系统管理功能，信息采集管理子系统负责对采集规则和采集对象的配置管理，数据分析子系统负责对采集数据进行综合统计分析，风险资产定位子系统通过多维搜索分析和关联搜索分析，实现快速检索。

3）资产发现探针

资产发现探针可自动对网络环境中存在的资产进行探测发现。发现资产后，探针可根据探测结果对资产基本属性进行自动填充，如：资产的 IP、名称、操作系统类型等。

4）脆弱性检测探针

脆弱性检测探针可以通过智能遍历规则库和多种扫描选项的组合手段，深入检测出系统中存在的漏洞和弱点，最后根据扫描结果，提供测试用例来辅助验证漏洞的准确性，同时提供整改方法和建议，帮助管理员修补漏洞，全面提升整体安全性。

5）入侵检测探针

入侵检测探针以专业的检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段，深入分析 L2~L7 层网络判断入侵行为，深度、精准、

快速发现网络中攻击威胁，实时保护工业互联网平台企业网络资源。

6）威胁检测探针

威胁检测探针通过深度解析网络流量，结合特征匹配、机器学习、虚拟沙盒等技术，实现迅速、精准识别网络中各种已知和未知网络威胁。综合威胁检测探针全面的威胁监测能力，有效的帮助运维人员管理维护网络安全，降低安全风险。

7）威胁诱捕探针

威胁诱捕探针通过在网络中部署仿真主机，主动诱导攻击，记录攻击细节并产生告警，可定位攻击源，弥补网络防护体系短板，提升主动防御能力。

8）工业入侵探针

工业入侵探针内置专业的工控入侵规则库，同时可根据业务功能需求制定白名单策略，采用攻击规则检测+业务白名单两种方式，对工业控制网络上捕获的数据包进行相应的行为匹配，及时发现来自生产网内外部攻击威胁，为客户提供直观、落地的安全防护建议，保障生产网络安全运行。

9）工业主机异常检测探针

工业主机异常检测探针采用白名单技术为工作站、服务器提供全生命周期的管理，为工作站、服务器的可用性、可靠性、可信性提供保障。只需一个客户端即可实时监控分析应用程序和人工操作的行为特征，及时发现风险并阻断。

10）工控资产脆弱性检测探针

工控资产脆弱性检测探针首先通过漏洞库、攻击特征规则库和多种扫描选项的组合手段，深入检测出工业企业系统中存在的漏洞、弱点以及可能存在的攻击行为；然后根据漏洞扫描结果，提供测试用例来辅助验证漏洞的准确性；最后将系统中存在的工业漏洞和攻击行为进行数据上传，以便工业互联网安全态势感知平台对工业漏洞和攻击行为进行关联分析，对工业漏洞引起的安全威胁进行态势展示和预警。

3. 具体应用场景和安全应用模式

工业互联网安全态势感知平台基于数据采集、数据监测、威胁分析、风险预警等多种技术手段，实现对辖区网络关键节点、重要企业的安全监测，监测范围

覆盖重点企业大部分的工业网络，运用技术手段识别网络运行情况，构建网络资产拓扑，将企业安全运行情况通过平台全方位展示出来。

工业互联网安全态势感知平台可应用于以下场景:

（1）基于企业侧的安全监测应用

针对联网工业企业，对工业企业底层设备、资产、工艺参数等进行多维度的参数解析和审计，及时发现联网工业企业异常流量，若出现某些内容超出合法范围等情况则判断为通信异常，然后进行报警。通过漏洞库、攻击特征规则库和多种扫描选项的组合手段，深入检测出工业企业系统中存在的漏洞、弱点以及可能存在的攻击行为，然后根据漏洞扫描结果，提供测试用例来辅助验证漏洞的准确性。

（2）基于平台侧的安全监测应用

在江西省联通机房部署工业互联网安全态势感知平台，对运营商、工业互联网平台等关键网络节点开放数据接口，实现工业互联网平台企业内部工业网络数据的全面采集，构建包括态势感知数据交互式检索、工控数据实时监测、态势分析展示、安全风险快速处置、工业安全问题追踪溯源等安全监测能力。

3）建立“互联网+安全生产”应用模式

通过部署在工业企业、平台企业侧以及关键网络节点的探针设备，将安全信息上传至工业互联网安全态势感知平台进行综合分析后可视化展示安全态势，联合工信主管部门、工业企业、运营企业等相关机构，建立线上或线下对接，向相关单位提供风险预警信息，与工业互联网企业实现很好的联动，助力企业安全生产，发现异常及时预警响应。

4. 安全及可靠性

（1）安全性

从安全维度考虑，本项目基于工业互联网安全态势监测与感知平台对重点企业工业互联网网络进行安全监测，有助于建立工业互联网网络安全预警和应急响应流程体系，有助于发现长期潜伏在企业工业互联网中的安全威胁，改变在攻击来临时无法察觉、在遭受攻击后无法追踪的现状，促进工业互联网企业积极进行网络安全整改。同时有助于推动和实现工业互联网网络安全防护的跨行业协作和信息共享，为工业互联网整体安全监测与态势感知提供网络安全风险数据和决策支撑。

通过建设工业互联网安全态势监测与感知平台可掌握工业互联网基础设施脆弱性和互联网资产暴露情况，防范和阻止敌对组织、商业间谍、内部不法人员、外部非法入侵者利用系统漏洞或管理上的疏漏入侵企业工业控制系统，从而造成系统瘫痪、信息泄露甚至系统的运行被恶意控制等安全问题。

（2）可靠性

本项目建设的工业互联网安全态势监测与感知平台具有较高的可靠性，平台依赖于强大的大数据平台架构支撑，以及全面的日志采集能力，可以从监管层面对工业互联网企业进行更广泛的安全监控。平台利用多种新型威胁监测手段，再结合威胁情报的使用，能够比传统安全运营中心（SOC）或安全信息和事件管理工具（SIEM）更快的发现隐藏在各类日志中的安全问题。

平台中的大数据融合分析展示系统可帮助用户直观的查看企业内部不同资产组的风险分布，相关风险值会在逻辑拓扑上直接映射，可以将风险以可视化的形式呈现的大屏幕上。外部威胁的攻击态势则能直接以地图展示的方式帮助管理者理解外部攻击的主要来源地，主要的外部攻击分类、本地最容易被攻击的资产等信息。所有态势感知的展示都可实时刷新，及时的将最新的安全态势呈现在平台监管者面前，从而为风险预警系统提供有力的技术支撑。

5. 其他亮点

（1）采用可扩展数据建模技术

平台的多维数据分析功能都是基于多维分析技术来实现，提供可扩展的数据建模框架，利用丰富的过程组件，实现可视化的数据建模定义。

（2）采用主动资产分析识别技术

对分布在各个探测节点处的信息，通过主动探测方式对资产基础信息进行采集，将获取的信息进行数据的抽取、转换和加载后，进行分类信息的识别。

（3）采用数据主动分析技术

通过数据分析子系统对采集数据进行综合统计分析，系统通过多维度搜索分析和关联搜索分析，实现数据的快速检索比对。

（4）采用威胁诱捕攻击技术

通过在网络中部署仿真主机，诱导攻击，记录攻击细节并产生告警，可精准定位攻击源，弥补网络防护体系短板，提升主动防御能力。

2.4.3 下一步实施计划

1. 实施计划一

目前国内地市级/行业级的工业互联网安全态势感知平台建设数量较少，该项目的顺利实施，可以作为标杆项目向江西省其他市区推广，如上饶市。当地有较多的制造业企业，可实现在上饶市建立一套制造业工业互联网安全态势感知平台，连接更多的制造工业企业、工业联网企业平台安全信息录入到上饶市制造业工业互联网安全态势感知平台，优化企业生产结构，建设企业安全生产新生态。

2. 实施计划二

在现有工业互联网安全态势感知平台基础上，进一步深化联网工业企业、工业互联网平台企业与平台之间的联动，增加接入工业企业的数量，由最初接入的20家扩展到50家，鼓励中小企业接入。实现联动防控、纵深监管，有效提升平台的综合管理和安全保障能力，推动工业互联网安全工作落实，构建工业互联网安全管理体系，提升工业互联网安全防护水平，强化工业互联网安全风险监测预警能力，推动工业互联网安全科技创新与企业发展。

3. 实施计划三

通过部署在晋南钢铁企业侧以及关键网络节点的探针设备，实时监测安全风险和脆弱性，对发现的重大威胁提前1小时进行安全风险预警，减少因为网络安全问题导致停工停产带来的经济损失，提升企业经济效益。

2.4.4 方案创新点和实施效果

1. 方案先进性及创新点

（1）项目先进性

a. 项目采用大数据关联融合分析技术，感知辖区内工业互联网安全整体态势。通过大数据关联融合分析系统采集数据信息，结合风险预警功能模块，将数据信息分类统计，进行安全事件汇总统计、安全风险预警发送。实现对接入工业企业的工业网络集中化监测、风险评估、合规性检测和异常行为监测，可以实现大规模企业接入。

b.建立大数据存储的标准化技术体系，有利于促进大数据存储的基础性标准。面对不同种类工业设备的各种各样数据格式，规范、制定统一的采集、存储、共享格式，以便于数据的处理，并为未来制定相应的行业数据标准打好基础。

c.基于大数据分析技术，全天候感知工业企业控制系统安全状况，有效预知威胁信息，并进行预警处理。面对传统安全防御体系失效的风险，态势感知平台能够全面感知网络安全威胁态势、洞悉网络及应用运行健康状态、通过全流量分析技术实现完整的网络攻击溯源取证，帮助信息安全人员采取针对性的响应处置措施。

（2）项目创新点

a.创新应用工业互联网资产规则识别技术。通过机器学习方式结合 IP 资产库、访问行为、业务特征建立资产识别模型；全面支持业内主流工业通讯协议，并支持各类行业的业务安全。

b.创新应用基于深度学习的指纹特征空间拓展技术。本项目创新提出了基于深度神经网络学习的指纹提取思路，这种方法对未知协议设备的指纹提取具有一定的适用性。

c.创新应用深度学习与挖掘分析技术。本项目引入一些深度学习技术，打破传统固定阈值、固定维度，将网络行为特征标签化，使用具有自学习能力的模型和算法。

d.创新应用可扩展的安全分析插件技术。采用 Storm 集群进行实时流数据分析计算，提供方便的可扩展处理能力；采用 Spark 进行高性能的离线处理。基于模块动态扩展技术，实现模块级别的扩展。

2. 实施效果

本项目实施完成后，具有显著的实施效果，主要体现在以下几个方面:

（1）本项目面向电子信息行业建设完成 1 套地市级工业互联网安全态势感知平台，在 20 家工业企业互联网接入侧部署工控安全信息采集与防护感知探针设备，能够解决工业互联网安全风险无法快速发现、无法精准识别、缺乏风险预警手段等安全问题，快速精准识别网络中各种已知和未知网络威胁，及时上报工业互联网安全监测与态势感知平台。

（2）工业互联网安全态势感知平台基于特征匹配、异常行为分析、机器学习、虚拟沙箱等安全技术，实现自动资产发现、脆弱性扫描、工业互联网流量全面监测、全局态势展示、自动化风险预警处置等安全功能，为监管单位和重点工业企业提供大量安全运行数据和安全情报。

（3）本项目从监管层面可视化监控全网主机和关键节点的综合安全情况，实时监控节点信息的状态，便于监管单位和重点工业互联网企业全局洞悉工业互联网的网络安全态势，有利于国家对于工业互联网安全的管控。

（4）工业互联网安全态势感知平台支持多维可视化并行分析，充分发挥中国联通和支撑单位的资源集中、技术领先优势，全面评估工业互联网行业安全风险，依托工业和信息化部网络安全威胁监测与处置机制，及时向存在风险的单位提供预警信息，为企业进行威胁防范和应急响应提供有力支撑。

（5）本项目通过建立工业互联网安全态势感知平台，可实时监测重点企业和网络关键节点的安全风险和脆弱性，对发现的重大威胁提前 1 小时进行安全风险预警，有效提升工业互联网企业应对网络攻击风险的能力，减少因为网络安全问题导致企业停工停产带来的经济损失，保证生产业务的连续性、安全性，提升工业互联网安全产业的应用和推广价值，最终实现产业创新发展。

2.4.5 单位基本信息

本次项目申报的牵头单位是中国联合网络通信有限公司研究院（简称中国联通研究院）。中国联通研究院作为联通集团科技创新的主体，立足国家战略、公司战略和产业服务，成为公司战略决策的参谋者、公司技术发展的引领者、产业发展的助推者。内设一个综合支撑板块和智库研究、网络研究、应用技术研究三个技术研究板块，具备智库的专业咨询能力、网络技术的自主核心能力、前瞻技术的研究能力、技术与业务融合的应用能力。公司面向未来积极抢占技术制高点，构建起有算力、有能力、有生态的“两云、两院、两联盟、三基地、N 实验室”创新生态体系，全面加速 5G、工业互联网等“新基建”能力建设及融合应用推广，孵化 5G 示范应用超百个，加快释放“数字经济”新动能，为我国经济社会发展建功立业。

北京天融信网络安全技术有限公司（简称天融信）创始于1995年，截止目前员工人数超过6500人，是中国领先的网络安全、大数据与云服务提供商。天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。公司自成立至今为工业企业提供了大量优质的解决方案，覆盖电力、轨道交通、航空航天、能源、石油化工、机械制造、国防工业、汽车、电子等行业领域，多次获得CCID、工业互联网产业联盟等机构颁发的优秀解决方案、优秀应用案例奖项。

2.5 案例五：5G 安全守护智能制造，再造传统汽车工业——数字化转型，智能制造引领未来

广州明珞联合广州移动将打造智能化水平领先的“5G+云+WiFi+工业互联网安全”的数字制造与工业互联网全球数字智造 5G 总部标杆，开展 5G 专网融合工业场景安全管理研究，打造明珞装备新一代通信与网络安全应用示范，开展“5G+智能制造+安全”的一体化解决方案合作研究，打造制造业大型企业、中小企业、产业集群参观展示基地，赋能汽车制造产业集群数字化转型升级与高质量发展。

2.5.1 方案概述

1. 方案背景

广州明珞是汽车领域全球首个实现数字化工厂虚拟制造与工业物联网大数据智能分析无缝对接的服务商，承接产业链上游核心装备/共性底座企业和下游汽车整机厂/零部件企业，具备较强的技术资源整合能力和汽车产线迭代创新转型方案交付服务能力，打造了多个数字化与工业互联网应用示范项目，包括：国家工信部制造业与互联网融合发展试点示范；国家工信部工业互联网试点示范；国家工信部 大数据产业发展试点示范 ；国家工信部智能制造系统解决方案供应商 ； 广东省工信厅 CPS 离散制造数字化创新中心等项目。

图 5-1 明珞全球数字智造 5G 算智总部基地

工信部在《“十四五”智能制造发展规划》中强调，智能制造发展水平关乎我国未来制造业的全球地位。习近平总书记多次对中国制造转型升级作出重要论述，明确指出“突围破局”之路，要把握数字化、网络化、智能化融合发展的契

机，以信息化、智能化为杠杆培育新动能。要以智能制造为主攻方向推动产业技术变革和优化升级，推动制造业产业模式和企业形态根本性转变，促进我国产业迈向全球价值链中高端。同时，工业互联网是制造业数字化转型升级的基础，也是支撑未来制造业转型的“基座”。此外，从2008年至2020年广东省人民政府多次印发相关文件提到加快推进以“工业互联园区+行业平台+专精特新企业群+产业数字金融”为核心架构的新制造生态系统建设。

为响应以上指示，提升企业生产效率。2021年，中国移动与明珞共建“5G工业互联网联合创新实验室”，在产线“智造”数字化的5G+数字孪生、云化IMS/PLC/MISP、5G远程运维、5G柔性生产和工厂数字化的5G+上下游协同5大应用场景取得了突破性成果。2022年5月，中国移动与明珞联合申报广东省产业集群数字化转型试点项目。

2. 方案简介

广州明珞联合广州移动将打造智能化水平领先的“5G+云+WiFi+工业互联网安全”的数字制造与工业互联网全球数字智造5G总部标杆，开展5G专网融合工业场景安全管理研究，打造明珞装备新一代通信与网络安全应用示范，开展“5G+智能制造+安全”的一体化解决方案合作研究，打造制造业大型企业、中小企业、产业集群参观展示基地，赋能汽车制造产业集群数字化转型升级与高质量发展。

3. 方案目标

本项目的主要目标是实现传统汽车制造过程的数字化转型和智能化升级，提高生产效率和质量，降低成本和安全隐患。具体目标包括:

- 引入5G网络和智能制造技术: 项目引入了5G网络和智能制造技术，实现了设备之间的互联互通和数据共享，提高了生产效率和质量。
- 数字化转型和智能化升级: 项目涉及数字化生产线、远程监控和维护系统、生产数据分析优化系统等，助力明珞实现数字化转型和智能化升级，为企业提供了更高效、更智能的生产方式。
- 安全防护措施: 项目采用了多种安全防护措施，如数据加密、访问控制、防火墙、入侵检测等，保障了数据的安全性和完整性。
- 技术研发创新: 项目在安全防护方面提升了明珞的产品力，并在后续的技术研发方面不断协同投入，优化和升级产品技术，提高产品性能和竞

争力

- 带动产业发展：助力产业的安全能力升级，合作提升新型工业化产业链、供应链的韧性和安全水平，协同实现在离散制造行业和非标制造行业的复制推广。

基于以上工业互联网安全解决方案方案，助力广州明珞全球总部基地智造工厂实现智能化升级，实现典型应用落地。

2.5.2 方案实施概况

针对生产、办公网隔离数据采集传输安全需求，打造 2B、2C 两张 5G 专网，采用切片等安全技术保证网络和业务隔离；

针对终端种类多、安全管理要求高的问题，对 5G 终端集中管理和安全认证，增强智能终端自身安全、访问控制能力；

针对工控生产网络高可靠、高安全的需求，加强工控网络隔离和安全审计，采取链路冗余保证网络高可用。

针对企业内部、供应链数据共享使用安全的需求，数据流转全生命周期安全设计，多地协同图纸设计安全、数据存储/共享安全。

针对统一安全运维安全监测的需求，建立 5G 全连接工厂安全管理体系，安全风险监测预警，威胁应急处置。

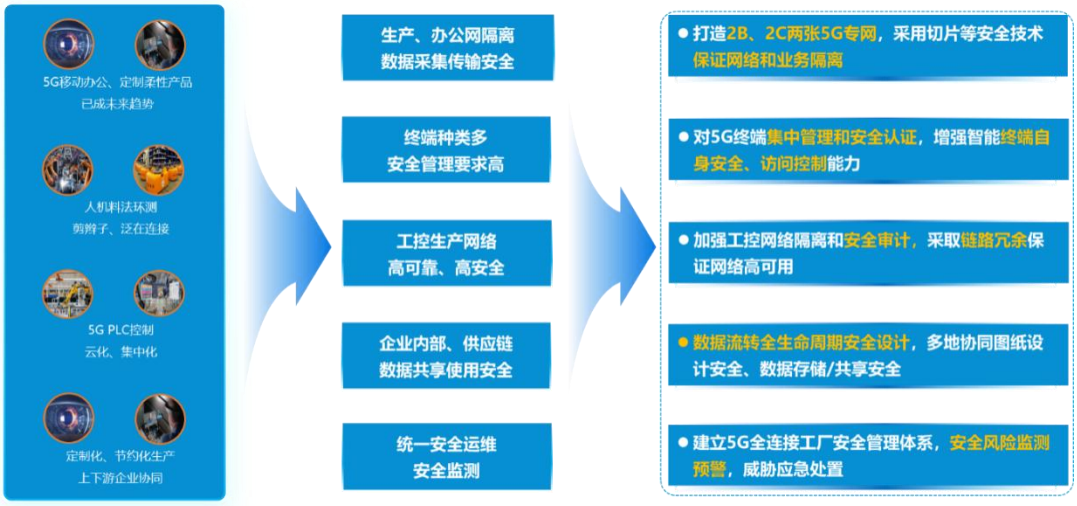


图 5-2 网络安全需求图示

1. 方案总体架构和主要内容

明珞 5G+智慧工厂采用产线级、工厂园区级两层设计，建立 2B 和 2C 两张 5G 专网，满足产线生产、智慧工厂、智慧园区、内外网办公等业务需求；总体安全设计按照等保三级标准执行，从终端安全、网络安全、生产网安全、数据安全、安全管理等五大方面进行安全建设，构建产线、工厂、园区多级安全防线。

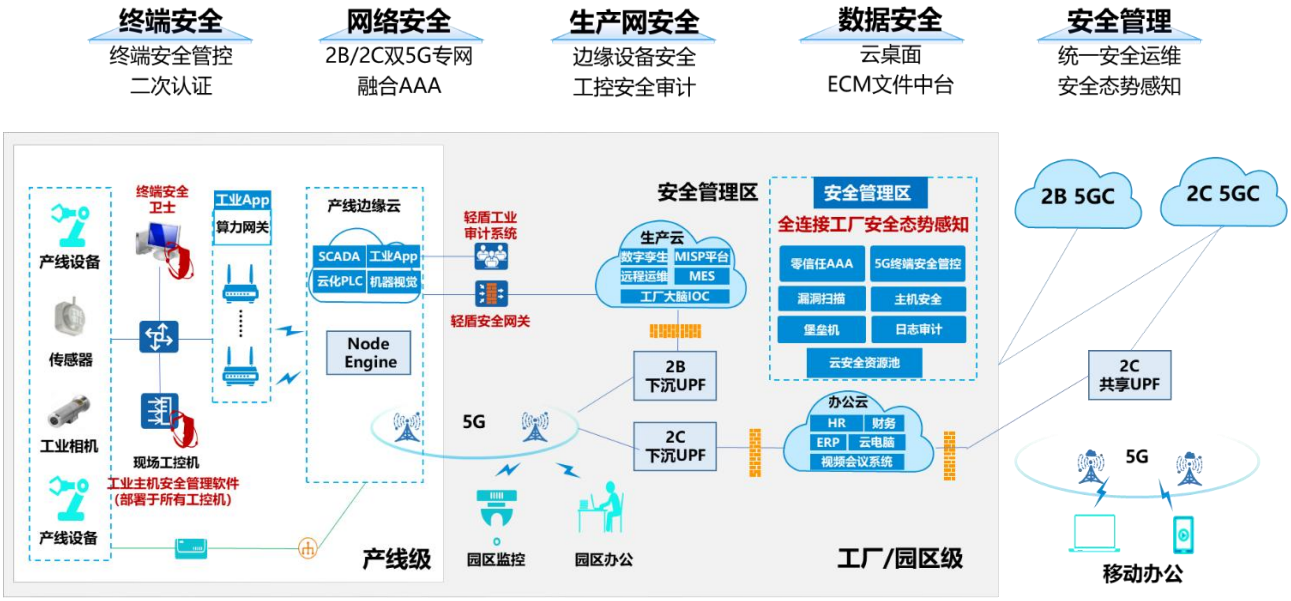


图 5-3 明珞工业互联网安全整体技术架构

2. 网络、平台或安全互联架构

2B2C 双专网网络强隔离组网设计

在组网安全方面，采用 2B2C 双下沉专网方式实现生产网络和办公网络的物理隔离，部署策略如下：

- 1 套融合零信任 AAA
- 2 台 UPF，生产和园区强隔离
- 2 朵云，生产云和办公云隔离
- 4 个 IP 地址段，不同安全策略。园区业务和生产业务不同 IP 池
- 6 个空口切片，建设高可靠和确定性时延的网络。控制、数采、园区、监控、办公别占用不同的空口切片
- 10 个不同的物理小区，多个物理小区，确定基站工作范围
- 11 个 VLAN，不同业务传输隔离，不同业务应用、不同网段不同 VLAN，实现业务细粒度的隔离和安全策略。

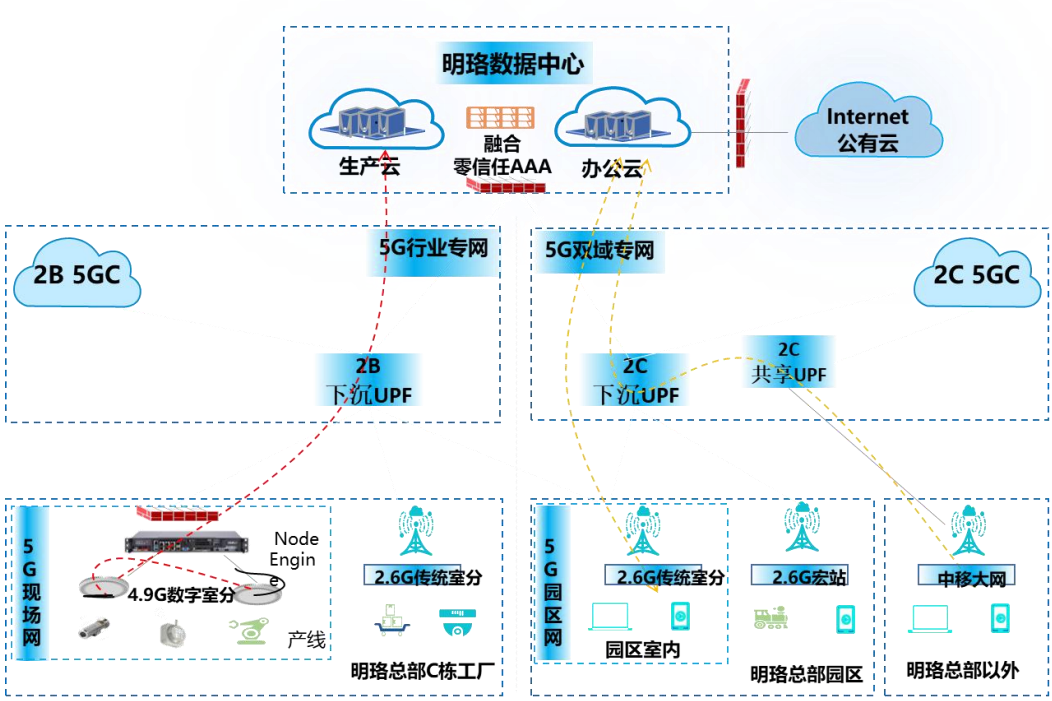


图 5-4 明珞网络架构

3.具体应用场景和安全应用模式

（1）应用场景

该项目是一个融合了 5G 技术、智能制造和数字化转型的先进性项目。以下是项目中的应用场景:

1）5G+数字孪生：通过数字孪生技术对汽车生产线进行模拟和优化，实现生产过程的可视化、可预测和可优化。数字孪生技术能够将实际生产线上的设备、生产线和工厂映射到虚拟环境中，实现实时监控、数据采集、分析和优化。通过 5G 技术，可以实现数字孪生应用的高效运行和实时数据传输。

2）5G+云化 PLC：将 PLC 的功能上云，通过 5G 网络实现远程控制和数据采集。云化 PLC 可以实现灵活的配置和扩展，支持多用户同时访问和操作，提高生产效率和降低成本。同时，5G 网络的高速率、低延迟和大连接数特性为云化 PLC 提供了强大的支持。

3）5G+柔性生产：通过 5G 技术实现生产线的快速调整和优化，满足多样化、个性化汽车产品的生产需求。通过 5G 网络的实时数据传输和高效控制，可以快速调整生产线的生产能力和产品类型，提高生产效率和产品质量。

4）5G+上下游协同：通过 5G 网络实现与上下游企业之间的实时沟通和协同合作。通过 5G 网络的实时数据传输和高效通信，可以实现供应链的透明化和协

同化，提高生产效率和降低成本。同时通过 5G 网络与银行等金融机构进行合作，实现供应链金融等创新模式。

5）5G+智慧办公：通过 5G 技术实现更加智能化的办公和管理，提高工作效率和降低成本。通过 5G 网络的实时数据传输和大连接数特性，可以实现办公设备的无线化和移动化，提高办公的灵活性和效率。同时，还通过 5G 网络与全球各地的分支机构和合作伙伴进行实时沟通和协作。

6）5G+智能质检：通过 5G 技术实现更加智能化和高效的质量检测和管理，提高产品质量和降低成本。通过 5G 网络的实时数据传输和高速度特性，可以实现自动化检测和数据分析等功能，提高检测效率和准确性。同时，通过 5G 网络与供应商和客户进行质量信息的实时共享和协同改进。

（2）安全应用模式

采用了多种措施和技术手段，以确保终端设备和数据的安全性这些措施包括防病毒软件、防火墙、入侵检测和防御等安全防护手段，加密技术、数据备份和恢复机制等数据安全措施，以及安全管理平台、安全培训和意识提升等综合措施。

1）终端安全：三重手段保障终端可信

经项目团队调研分析，5G 明珞工厂主要安全风险来自于终端，因此我们以终端安全建设为牵引，驱动安全体系的建设。通过 5G 主从认证、终端安全加固、终端安全检测和管理三重手段，提升终端安全保障水平。在不断加强终端自身安全防护的同时，建立终端安全防御体系：

a）在产线车间所有工控机部署工业主机安全管理软件，在所有 PC 电脑侧、云桌面侧，部署终端安全卫士，加强终端自身安全防护

- 内核级的安全加固
- 指令级的漏洞防护
- 进程白名单机制

b）建立终端安全防御体系

- 持续的安全监测
- 威胁分析，态势呈现
- 远程运维，响应处置

下图为终端安全防御体系逻辑示意图：

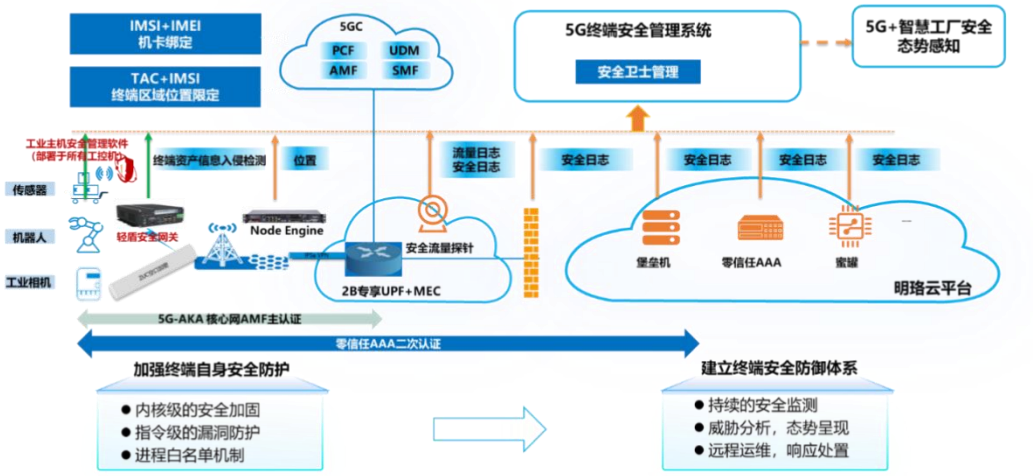


图 5-5 广州明珞终端安全防御体系架构图

2）工控+MEC 安全：保障 5G 生产网安全

明珞 5G 生产网，依托有线现场网，融入 5G 现场网和 5G 数采网，逐步构建明珞 5G 全连接工厂，部署专业的工业防火墙进行网络分区和安全隔离、部署轻盾工业审计系统进行流量监测；并结合原有的工控安全管理中心，实现对 5G 生产网的统一安全管理和运营。

a） 车间级工控组网安全

- 5G 工业网关内置双 5G 模组。
- TSN FRER 技术、双发选收。

b） 工控安全隔离与网络检测

- 30 种工业协议 DPI、1000 种功能码识。
- 工控白名单、指令级超精细访问控制粒度。

c） MEC 基础设施安全

- 防盗防拆防恶意断电、关闭协议无关端口。
- 服务器管理/存储/业务网络三面独立。

d） 系统及平台安全

- 补丁&漏洞管理、病毒防护。

e） 业务及数据安全

- APP 安全防护、数据访问控制。

f） 管理运维安全

- 威胁检测与分析、工控漏洞扫描、运维审计、日志审计。

3）数据安全：分区控制，业务数据安全流转

广州明珞提供汽车产线装备设计和集成服务，研发、产品图纸等重要数据跨企业、跨地域流动已成为常态，本项目采用数据分区控制机制，部署数据存储安全区、接收清洗区、外发中转审计区，保障业务数据安全流转，同时引入云桌面技术实现重要数据集中式管控。

a） 数据共享安全：设立外发中转区

- 跨区流通，可控、可溯、不落地
- 外发审批、加密，数据导出中转区
- 打开次数、时长限制

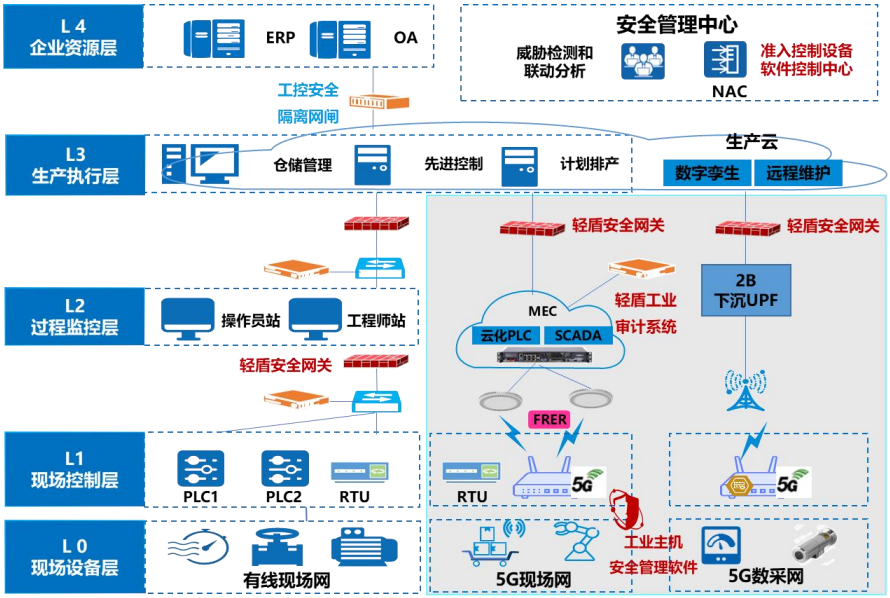


图 5-6 工控+MEC 安全五层架构

b） 数据使用安全：云桌面+ECM 平台

- 多地图纸协同设计安全管控

c） 数据存储安全：数据防泄漏

- 数据库加密
- 数据库访问控制
- 数据防勒索

d） 数据传输安全：IPSEC 加密隧道

e） 数据采集安全：终端访问控制

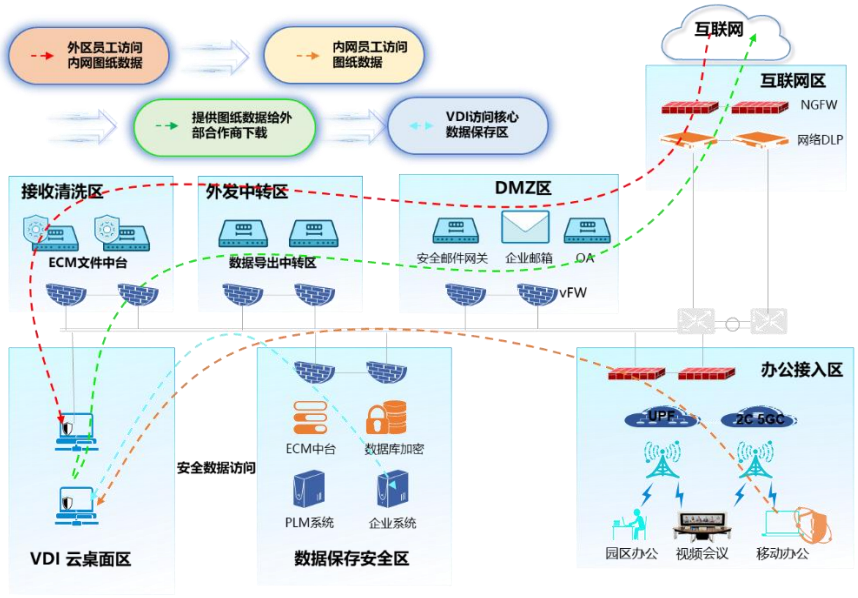


图 5-7 数据安全架构

4）运维安全：五大机制保障业务高可用

组建专业的安全运营团队，制定 5G 专网安全巡检制度和处置流程，开展安全监测、威胁响应工作，及时确认发现有效安全事件，处理问题终端，保障明珞智慧工厂业务安全运行。

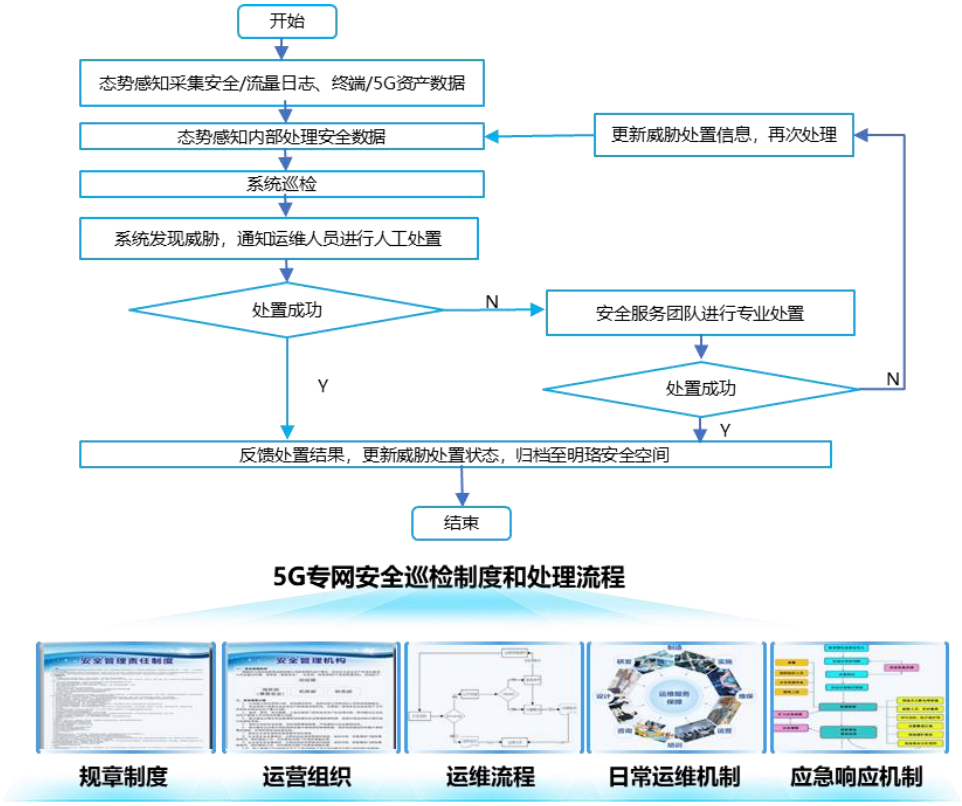


图 5-8 运维安全逻辑图

4.安全及可靠性

项目采用了先进的 5G 网络技术，实现了生产线的自动化和智能化，减少了人工干预，提高了生产的安全性。同时，项目还建立了完善的安全管理制度，包括网络安全、数据安全、设备安全等方面，确保项目的安全性和稳定性。

项目采用了高可靠性的设备和系统，如工业互联网平台、工业大数据平台、智能生产管理系统等，确保系统的稳定性和可靠性。此外，项目还采用了备份和恢复措施，对重要的数据进行备份和恢复，防止数据泄露、篡改和丢失等可靠性问题。

5.其他亮点

项目采用了大数据分析和人工智能技术，对采集到的生产线数据进行深入挖掘，发现数据中的规律和趋势，为决策提供更可靠的依据。这可以帮助企业更好地了解市场需求和消费者行为，提高产品的市场竞争力。

其次，项目还采用了创新的技术和商业模式。例如，通过工业互联网平台和按需生产、共享经济等模式，创新商业模式，拓展新的销售渠道和增长点。这可以帮助企业更好地满足消费者的个性化需求，提高企业的市场竞争力。

此外，项目还积极推动再制造产业的发展。通过再制造技术，将废旧汽车零部件进行再制造生产，实现废旧产品的循环利用和节能减排。这可以帮助企业降低生产成本，提高企业的环保意识和社会责任感。

2.5.3 下一步实施计划

1. 实施计划一

双方将围绕“5G+智能制造+工业互联”领域，依托中国移动提供云网融合以及属地化的渠道拓展和服务能力，明珞提供 SaaS+平台的行业应用服务，打磨一套“产线+平台+安全”的 5G 智能制造解决方案，优势互补，护航新型工业化。

2. 实施计划二

移动联合明珞，打造智能化水平领先的“5G+云+WiFi+工业互联网安全”的数字制造与工业互联网全球数字智造 5G 总部标杆;

双方联合共建“5G 工业互联网联合创新实验室”，打造工业互联网产研基地。

图 5-9 5G 工业互联网联合创新实验室

3. 实施计划三

双方联合开展“5G+智能制造”一体化解决方案合作研究，已成功联合申报广东省产业集群数字化转型试点项目，赋能汽车制造产业集群数字化转型升级与高质量发展，落实习总书记“中小企业能办大事”，赋能汽车制造产业集群数字化转型升级与高质量发展。

图 5-10 广东省 CPS 离散制造数字化创新中心

2.5.4 方案创新点和实施效果

1. 方案先进性及创新点

明珞在广州黄埔区新建总部基地，广州移动助力明珞打造智能化水平领先的“5G+云+WiFi+工业互联网安全”的数字制造与工业互联网全球数字智造 5G 算智总部标杆，是省内首个制造业园区+工厂+产业集群全场景覆盖的 5G+工业互联网项目。

1）5G 专网深入制造企业核心生产流程

打造 2B2C 两张 5G 专网（2B MEC 下沉+共享 5G 双域专网），一方面基于智慧园区平台、公有云等打造安全、便捷、节能、舒适的新型 5G 智慧园区总部标杆，另一方面基于 5G、边缘计算、精准定位、AI、AR 等技术，深入工厂核心生产流程，打造装备制造行业全自动加工线、工装和标准设备装配线等生产线的 5G 智慧工厂标杆。

2）项目经济效益显著，复制推广性强

一期总部园区建设项目金额 2350 万，二期智慧工厂建设项目金额超千万，明珞云桌面建设项目金额超千万。后续将以明珞为样本，复制制造企业总部及工厂建设，打造 5G+工业互联网应用示范，未来规模亿元级以上。

3）社会效益显著，标杆意义重大

广州移动与明珞强强联合，开展“5G+智能制造”一体化解决方案合作研究，赋能汽车制造产业集群数字化转型升级与高质量发展，并可打造成制造业大型企业、中小企业、产业集群参观展示基地，落实习总书记 “中小企业能办大事”。

2. 实施效果

2022 年 6 月，广州移动与明珞签订“广州明珞装备股份有限公司全球总部基地智能化服务”项目合同，项目首次在汽车装备制造领域打造 5G 工业云，将 5G 能力深入制造企业核心生产流程，将打造 5G 网络全覆盖，泛联感知、云网融合的网络架构，部署 2B2C 两张 5G 专网和 5G 工业云，实现业务数据不出园以及低时延、高可靠的数据传输，打通 5G+工业互联网的核心应用场景，打造智能化水平领先的“5G+云+WiFi+工业互联网安全”的数字制造与工业互联网全球数字智造 5G 总部标杆，助力明珞引领全球数字制造革命。

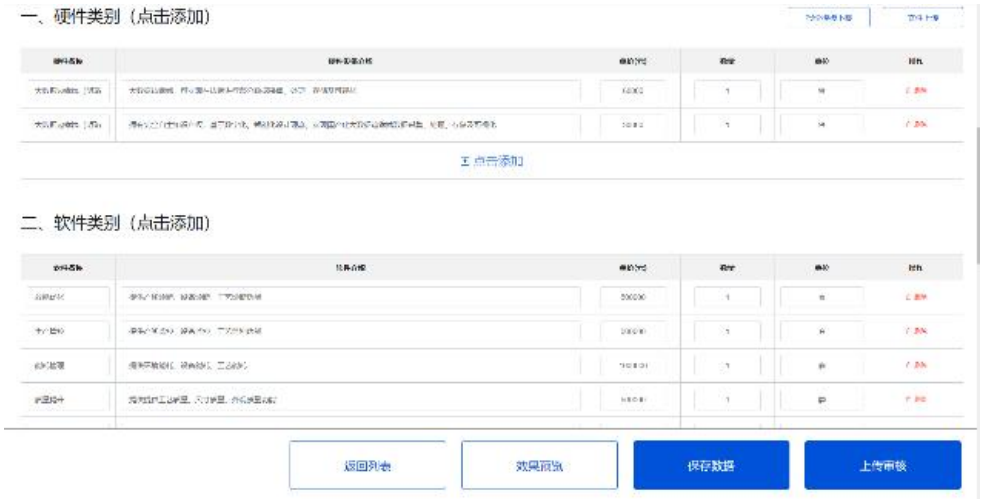
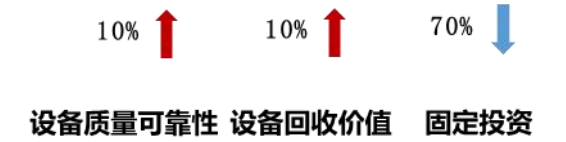


图 5-11 移动工业云承载明珞工业互联网平台

1）投入产出 / 综合制造成本显著降低

2）生产准备周期 / 数字化交付周期缩短

3）投资风险降低/ 柔性制造与设备通用化



2021 年，中国移动与明珞共建**“5G 工业互联网联合创新实验室”**，在产线“智造”数字化的 5G+数字孪生、云化 IMS/PLC/MISP、5G 远程运维、5G 柔性生产和工厂数字化的 5G+上下游协同 5 大应用场景取得了突破性成果。

2022 年 5 月，中国移动与明珞联合申报广东省产业集群数字化转型试点项目。由广州黄埔区政府推荐，明珞装备为牵头单位，广州移动、工信部电子五所等为成员单位，赋能汽车制造产业集群数字化转型升级与高质量发展，并将“5G 工业互联网联合创新实验室”打造成制造业大型企业、中小企业、产业集群参观展示基地。

目前，明珞与中国移动协同的 5G 智能产线研发项目已经开启，将围绕智能产线与 5G 网络的深度融合开展一系列技术研发和产业化推广工作，推动装备行业和离散行业“5G+智能制造+工业互联”相关技术标准的制定。

2.5.5 单位基本信息

中国移动作为国家首批原创技术策源地和现代产业链链长，锚定“世界一流信息服务科技创新公司”发展定位，推动数字经济和实体经济深度融合。广州移动积极响应市委市政府发展要求，近三年收入保持稳健增长，通过持续推进“提速降费”让消费者与中小企业享受技术进步红利。

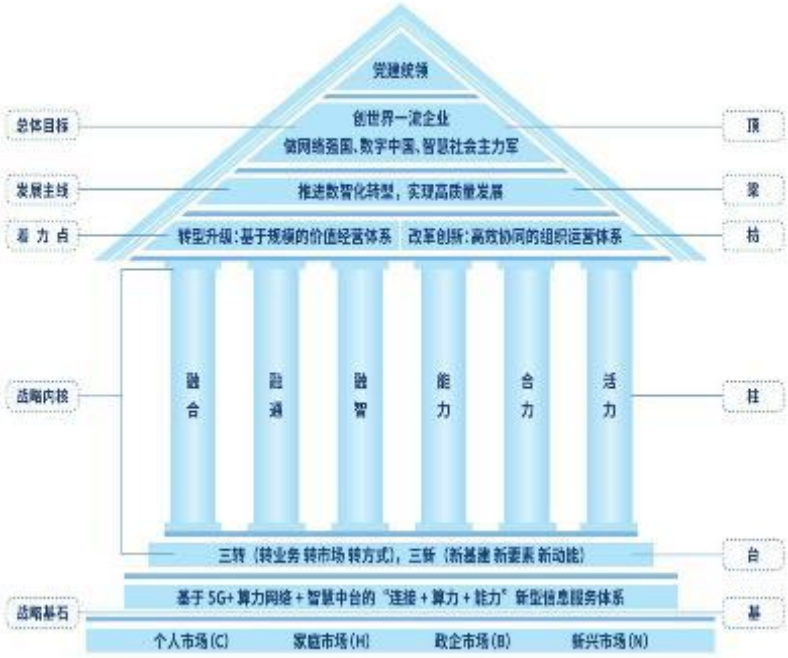


图 5-12 创世界一流“力量大厦”

秉承人民邮电为人民的服务宗旨，广州移动作为区域领先的通信运营商和信息化专家，服务千家万户、赋能千行百业，服务个人客户近 1800 万，家庭客户近 280 万。广州移动在网络资源、客户规模、信息化业务和项目实施能力各个方面，均处于行业领先地位。2022 年政企行业份额突破 40%，成为区域第一大政企信息化运营商，实现个人、家宽、政企三大领域行业份额领先。

图 5-13 三大领域行业份额

2.6

2.7 案例六：中核集团下属某燃料产业企业工控安全建设项目——军工行业“中国芯”自适应安全防御体系

近年来，随着两化融合的深入推进，工业控制系统（以下简称“工控系统”）日趋数字化、网络化和智能化。工控系统在极大提高生产效率、提升创新能力、促进产业转型升级的同时，也面临着漏洞层出不穷、威胁加速渗透、攻击手段复杂多样、防护措施相对滞后等前所未有的信息安全挑战。

本方案结合军工企业工业控制系统业务应用场景及工作实践，参考 Gartner 的自适应安全架构为模型，从预测、防御、检测、响应四个维度，强调安全防护是一个持续处理的、循环的过程 ，细粒度、多角度、持续化的对安全威胁进行实时动态分析，自动适应不断变化的网络和威胁环境，并不断优化自身的安全防御机制。方案规划设计工控系统网络安全技术防护框架，围绕物理环境、通信网络、终端主机、应用系统、终端设备等工控系统运行环境，从身份鉴别、访问控制、内容安全、安全审计及备份恢复角度设计安全防护技术框架，构建工控系统纵深防御体系，对同类型军工生产制造企业工控系统网络安全防护建设具有参考和借鉴意义。

2.7.1 方案概述

1. 方案背景

军工行业工控系统安全是关系国家安全的重大战略问题，随着安全问题逐渐暴露，军工行业工控系统的安全防护刻不容缓。军工企业应该以建设国防事业的标准和力度发展工控安全产业，建立完备的工控网络安全体系，切实提高军工行业工控系统的防护水平，筑牢网络安全屏障，推进网络强国建设。

2. 方案简介

项目以非密工业控制系统防护为主要防护对象，以等保三级为安全防护基本目标，结合军工企业工业控制系统业务应用场景及工作实践，在满足合规建设的基础上，参考自适应安全模型，规划设计工控系统网络安全技术防护框架，围绕物理环境、通信网络、终端主机、应用系统、终端设备等工控系统运行环境，从

身份鉴别、访问控制、内容安全、安全审计及备份恢复角度设计安全防护技术框架，构建工控系统自适应主动防御体系。

项目根据现场业务需求，部署工控安全产品满足基础防护功能的基础上，建立工控安全运营平台。平台提供工控资产自动化盘点、内网攻击面测绘、安全配置风险检查、合规风险评估、流量威胁感知、泄漏监测、日志审计与检索调查、应急处置及安全可视化等能力。

平台以安全运营中心为基础，建设检测中心、防御中心、回溯中心三大中心。检测中心专注于事前检测，防御中心专注于事中防御，回溯中心专注于事后回溯。四中心联动形成闭环流程，形成“预测、防御、检测、响应”的自适应安全闭环，护航军工企业安全生产。

3. 方案目标

1）按照等保三级防护的标准要求进行安全建设，满足合规需求，并预留网络接口，为后期智联融合建设提供基础条件。

2）提升系统“预测、防御、检测、响应”等方面的主动防御能力，在满足不同业务系统、不同安全级别网络间能够进行数据实时交互的同时，做好生产网络跨系统、跨区域边界的访问控制以及网络内部非法设备接入、异常通信监测及处置等工作，形成安全闭环，确保生产网络整体平稳运行。

3）配套形成契合企业实际业务情况的安全管理制度，通过“技管并用”，进一步提升工控系统安全防护能力。

2.7.2 方案实施概况

1.项目总体架构和主要内容

（1）方案架构

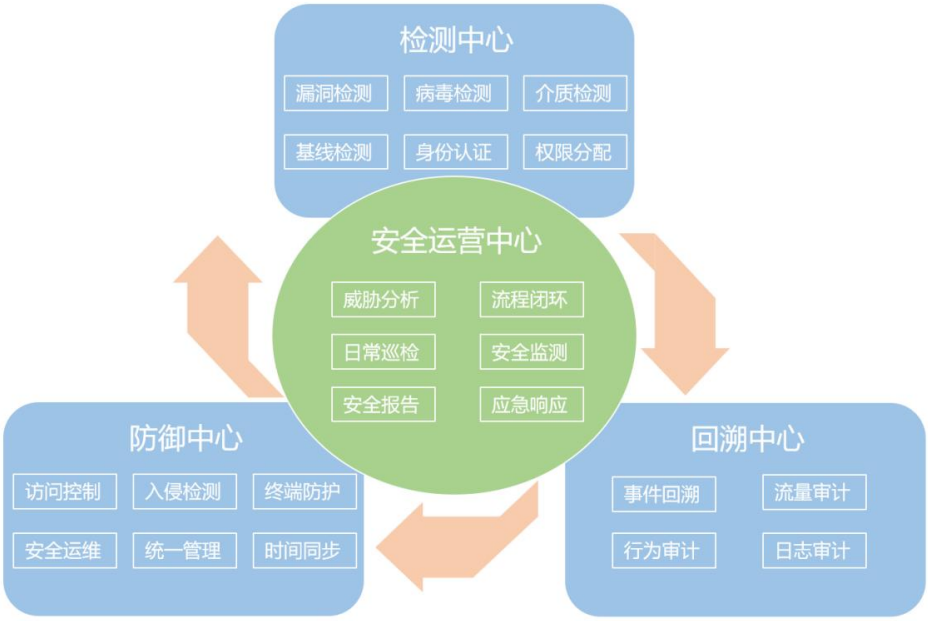


图 6-1 四中心架构

（2）业务流程

根据该企业的现网需求，本方案设计主要涉及两大业务流程，分别是终端、设备入网流程以及终端、设备更新流程，详细涉及如下：

- 终端、设备入网流程

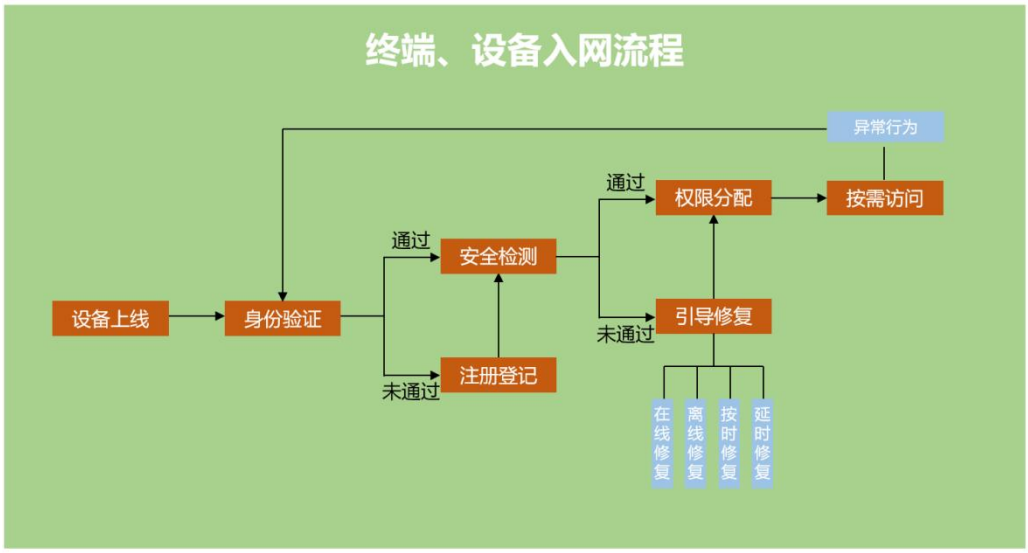


图 6-2 终端、设备入网流程

当新的终端、设备接入工控网络时，首先要进行身份验证，身份验证未通过则需进行注册等级的审批流程；

身份验证通过后，将对入网的终端、设备进行安全检测，安全检测包含病毒、

漏洞、基线等检测内容，未通过检测的终端、设备将通过在线、离线等方式进行修复，若终端、设备因业务需要，必须上线，则开启临时上线流程，限定整改周期并及时复查，若整改周期内未完成既定的修复，则进行下线处理；

安全检测通过后，设备将根据自有的属性以及身份验证时的信息，按需提供网络访问的权限；

终端、设备在运行的过程中若出现异常行为，则会根据预置的策略，重新进行身份验证、安全检测等工作。

➢ 终端、设备更新流程

当终端、设备需要进行更新时，首先在摆渡服务器上进行数据更新；

摆渡服务器通过安全检测，保障介质、终端、数据的安全，通过离线的方式，将更新内容导入到工控网络的窗口服务器；

窗口服务器根据更新机制，将更新数据推送至终端、设备，或由终端、设备主动连接窗口服务器进行更新。

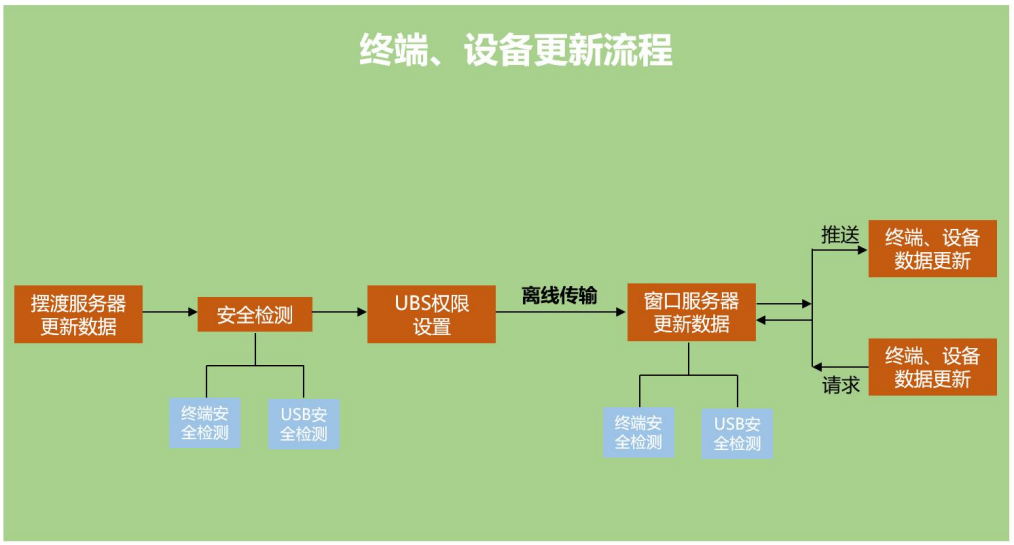


图 6-3 终端、设备更新流程

2. 方案详细设计

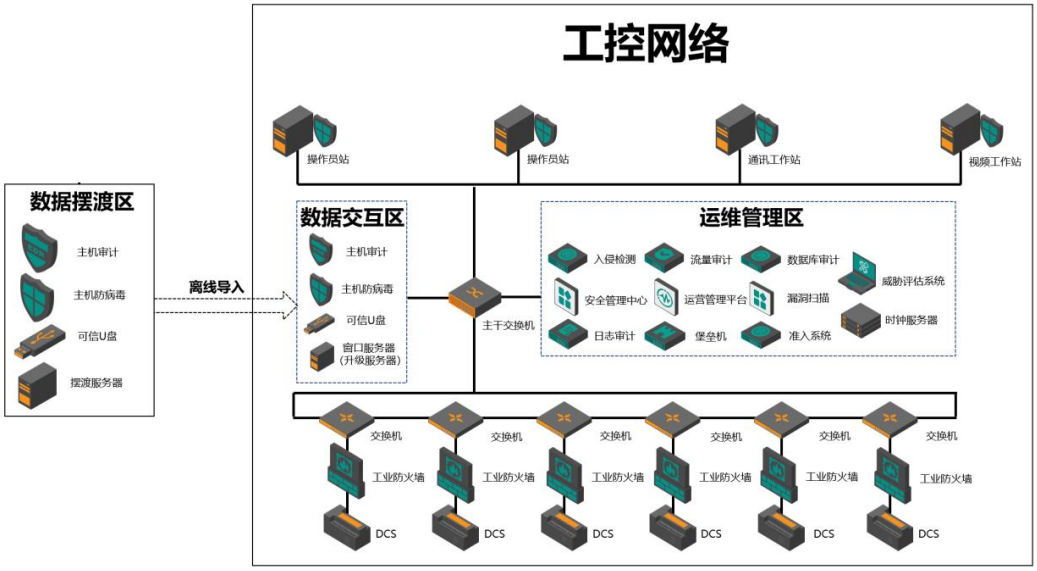


图 6-4 工控网络安全建设拓扑图

本次安全建设，将在工控网外建设数据摆渡区，数据摆渡区提供终端、设备更新时的源数据，同时对数据摆渡区的服务器、介质通过管控、审计的方式，保障安全;

工控网侧将搭建数据交互区，数据摆渡区的数据通过离线导入的方式，摆渡到数据交互区，同时对数据交互区的服务器、介质通过管控、审计的方式，保障安全;

工控网侧将搭建运维管理区域，部署入侵检测、安全管理中心、日志审计、流量审计、运营管理平台、堡垒机、数据库审计、漏洞扫描、准入系统、威胁评估系统、时钟服务器等旁路检测、审计类设备，建设工控网网络安全检测、审计能力;

工控网侧关键节点部署工控防火墙，建设访问控制、协议过滤等能力;

工控网上位机侧部署主机卫士，建设上位机终端安全防护能力。

（1）事前检测设计

事前检测旨在提升检测能力，用于设备、终端上线之前，通过对设备、终端严格的技术检测以及相应的流程，杜绝“带病上线”的情况。事前检测的设计主要包含漏洞检测、病毒检测、介质检测、基线检测、身份认证、权限分配六个方面。

➢ 漏洞检测设计

漏洞检测通过漏洞扫描工具实现，漏洞检测使用包含两种场景：新接入网内

的终端、设备进行安全检测以及周期性现网设备的安全检测。

漏洞检测能够全面、快速、准确的发现被扫描网络中的存活主机、网络设备、数据库，准确识别其属性，包括主机名称、IP 地址、端口、操作系统、软件版本、负责人、地区等，同时还能够自动生成网络拓扑，还可以进行后期人工修改，查看各资产的详细信息。

漏洞检测能够发现系统漏洞、工控设备漏洞、工控协议漏洞、Web 漏洞等，并提供解决方案。

- 病毒检测设计

病毒检测通过防病毒软件实现，用于数据摆渡服务器、数据窗口服务器，用以保护数据传输的端点安全。病毒检测能够对蠕虫病毒、恶意软件、广告软件、勒索软件、引导区病毒、BIOS 病毒的进行查杀，通过部署在数据摆渡服务器上的防病毒软件进行统一的病毒库升级。

病毒检测针对不同的场景，提供扫描以及实时防护两种运行方式。数据摆渡服务器、数据窗口服务器上的病毒防护软件采用主动防护模式，提供终端实时的病毒防护；对新接入网内的终端、设备采取扫描模式，发现其中的病毒并进行查杀。

- 介质检测设计

介质检测通过终端安全防护软件实现，用于数据摆渡、交互的场景。当终端、设备需要进行更新时，由数据摆渡服务器发起更新流程，并将更新内容通过移动存储介质进行离线传输，移动存储介质在接入数据摆渡服务器以及数据窗口服务器时，都会触发病毒检测策略，保障病毒不会通过移动存储介质由外部进入工控网络内部。

移动存储介质在接入数据摆渡服务器以及数据窗口服务器时还会触发认证机制，用以确保在数据摆渡服务器以及数据窗口服务器上不同的使用权限，如：在数据摆渡服务器上只能读取数据，并不能写入数据；在数据窗口服务器上只能写入数据，不能读取数据等；同时通过认证策略，确保移动存储介质的唯一性，即：只有专用的移动存储设备，才能被用于接入数据摆渡服务器以及数据窗口服务器，且专用移动存储设备只能接入数据摆渡服务器以及数据窗口服务器，不能接入其他终端（如上位机、办公终端、运维终端等）。

➢ 基线检测设计

基线检测通过准入系统实现，使用场景为：当有新的终端、设备接入网内，则会触发基线检测机制，通过预设策略，对终端、设备的基线进行检测，以保证接入设备的安全性。

基线检测的内容包含防火墙是否启用检查、系统空密码检查、U 盘是否开自动启动检查、远程桌面是否开启检查、文件共享是否开启检查、Guest 账号是否开启检查、IE 代理是否开启检查、IP 获取方式检查、是否登录域检查、服务黑白名单检查、进程黑白名单检查、软件黑白名单检查、外联访问能力检查、补丁检查，检查补丁完整性、注册表检查，检查注册表关键值是否存在、关键位置文件检查，检查指定路径文件存在性、操作系统检查等。

➢ 身份认证设计

身份认证通过准入系统实现，当有新的终端、设备接入网内，需要通过认证策略才可接入。

认证策略的方式包含短信认证、邮件认证、口令认证、域认证、客户端认证、动态令牌认证、软 token 认证，并且采取结合口令、指纹、人脸等多因子结合的方式进行认证，提高认证的安全性。

➢ 权限分配设计

权限分配通过准入系统实现，准入系统可以通过策略设置不同的终端、设备在接入网内后不同的访问权限，策略设置包含评分策略以及访问策略两种方式，根据不同的场景可以使用不同的权限分配方式。

对于严格管控的区域，可以采用访问策略，即：所有新接入终端、设备在接入网内后，只能访问公共资源区域，对于核心资源区域的访问，需要通过申请的方式实现。

对于非严格管控的区域，可以采用评分策略，即：将网内所有资源进行重要程度的划分，根据接入网内的终端、设备的安全基线检测评分设定可以访问的区域范围。

（2）事中防御设计

➢ 访问控制设计

访问控制通过工控防火墙之间，主要用于隔离区域之间的访问。根据 XX 现

网情况，将在 DCS 系统与上位交换机之间部署防火墙，由于通讯走的使 Moudbus 协议，所以需要能够识别相应的工控协议。

通过工控防火墙开启访问控制策略，确保区域之间不能互相访问，只能和上层的 MES 系统之间进行通讯，且通讯为单向通讯。

安全策略能够支持 Modbus/TCP、IEC104、DNP3、FINS、S7COMM、OpcUA、OpcDA、OpcAE 等工控协议的深度检测，包括报文完整性、格式检查、功能码控制、寄存器控制，连接状态控制等的检测，进行细粒度的控制，过滤不受信任的网络行为。

- 入侵检测设计

入侵检测通过入侵检测系统实现，安全域边界除了访问控制策略，还需做好入侵防御，本次方案设计入侵检测系统部署于过程监控层。

在工控网中，主要的网络攻击针对于管理层的服务器、过程监控层的上位机以及现场控制层、现场设备层的下位机，工控网种的入侵防御上对工业协议解析有更为严格的要求，本次部署的入侵检测系统要能够对 OPC、Modbus、S7、DNP3、IEC104 等常见工控协议进行解析，并能做到指令及的控制，以防止攻击利用合法的指令进行非法的操作；同时针对于管理层、过程监控层的攻击，提供针对应用层的防护。

- 终端防护设计

终端防护通过主机卫士实现，主要部署于上位机。

上位机通过安装主机卫士，实现最小化系统安装原则，杜绝安装与工控系统功能和安全防护无关的软件；同时主机卫士开启白名单以及端口管控功能，集中对终端安全软件离线安装、更新和管理。

白名单能够确保上位机只运行允许的进程、服务以及应用程序；端口管控能确保上位机不能使用移动存储介质。

- 安全运维设计

安全运维通过堡垒机实现，主要用于运维时防止运维人员的误操作、高危操作等行为引起的服务器系统破坏、数据丢失等问题。

堡垒机能够对服务器、网络设备、安全设备的操作监控，实现账号集中管理、高强度认证加固、细粒度访问授权控制、加密和图形操作协议的审计等功能，让内部人员、第三方人员的操作处于可管、可控、可见、可审的状态下；安全运维

的设计主要包含:

➢ 安全认证机制

在认证机制方面，堡垒机除了常规的静态口令认证外，还支持通过 LADP 认证、AD 域认证、USBKEY 认证、Radius 认证、证书认证、短信认证、指纹认证、动态口令认证等双因素认证来提高认证的安全性和可靠性。

➢ 访问授权控制

堡垒机能够通过集中统一的访问控制和细粒度的命令级授权策略，确保每个运维用户拥有的权限是完成任务所需的最合理权限。管理员可根据运维用户的实际权限，对其访问主机、使用的协议、目标系统账号设置细粒度的访问策略。

➢ 统一管理设计

统一管理通过综合管理平台实现，用于管理网内所有的安全设备。

综合管理平台能够统一管理防火墙、入侵检测、安全审计等安全设备，管理的维度包含设备管理、策略管理、报告管理。

■ 设备管理

能够接入所有的安全设备，并监测安全设备本身系统使用情况以及硬件使用情况，及时发现设备本身的问题；同时与准入系统联动，对安全设备进行注册登记，避免黑客冒充安全设备进行中间人攻击。

■ 策略管理

统一管理所有安全设备的策略，通过策略模板进行统一的策略下发；对冗余策略进行梳理、合并，提高设备性能以及网络通行效率。

■ 报告管理

汇总所有安全设备的告警日志、报告，根据自定义模板输出安全日报、周报、年报。

➢ 时间同步设计

时间同步通过时钟同步服务器实现，用于管理网内所有设备的时间，使其保持一致性。

本次时钟同步服务器采取本地化部署方式，不与互联网连接，也不采取 GPS、卫星等方式进行互联网时间校准，因此需要定期进行离线时间同步。拟采取上线

时进行时间校准，之后每半年离线同步一次的周期进行设计。

时钟同步服务器具有独立的恒温晶振，在本地化环境中依靠自身晶振指挥子钟运行。

（3）事后回溯设计

- 事件回溯设计

事件回溯通过运营管理平台实现，用于在攻击事件发生后，以失陷主机、时间链、攻击链等维度，进行安全事件的回溯。

运营管理平台将安全事件分为侦察、入侵、命令控制、横向渗透、系统破坏（数据窃取）、证据擦除六个阶段，当安全事件发生后，可结合各设备的告警，去重降噪分析后将安全事件以攻击链的方式进行回溯呈现;同时运营管理平台内置了 MITRE ATT&CK 战术技术知识库中的 12 种敌方战术和 200 余种敌方技术，能够精确展现每个攻击步骤所使用的技术、方法，并且给与修复建议。

- 流量审计设计

流量审计通过安全设计系统实现，用于攻击事件发生后进行路径回溯，安全审计系统会将流量相关信息发送至运营管理平台，进行统一的汇总分析。

安全审计要能够支持常见的工控协议，包含但不限于:ADS/AMS、BACnet-APDU、CIP、DNP3、EGD、ENIP、FINS、FOX、GE-SRTP、Hart/IP、IEC103、IEC104、IEC61850/GOOSE、IEC61850/MMS、IEC61850/SV、MODBUS、OPC-AE、OPC-DA、OPC-UA、PROFINET、S7COMM、UMAS 等；通过工业协议的审计，能够分析出工控网的运行状态，便于事后溯源。

- 行为审计设计

行为审计通过数据库审计系统实现，用于审计对数据库的操作行为。数据库审计系统会将行为相关信息发送至运营管理平台，进行统一的汇总分析。

数据库审计系统能够对访问数据库操作进行实时、详细的监控和审计，包括各种登录命令、数据操作指令、网络操作指令，并审计操作结果，支持过程回放，真实地展现用户的操作。

能够对数据库访问源头的分析，有效监控数据库访问工具，实现了对数据库绑定变量的审计，自动提取 SQL 语句中的关键字段实现精准审计。

能够通过对 IP 信息、用户登陆信息、账号使用情况、SQL 指令执行时长等

响应事件的关联分析，实现事件源的快速定位和事件发生过程的全面回溯。

➢ 日志审计设计

日志审计通过日志审计系统实现，用于搜集网内所有设备、终端、服务器的日志，并将日志相关信息发送至运营管理平台，进行统一的汇总分析。

日志审计系统能够通过 Syslog、SNMP Trap（被接收方式）及 WMI、JDBC、Log File、FTP、WebService（通过代理采集并转发）等方式实现数据采集功能。

能够支持主流主机设备、网络设备、安全设备、应用系统。具体包括：交换机、路由器、防火墙、Windows 服务器、AIX 服务器、Linux 服务器、HP-UX 服务器、Solaris 服务器、SQL Server、Oracle、DB2、Sybase、MySQL 数据库系统、webshpere/ weblogic 中间件、Mail/Web/FTP/DNS/DHCP/WINS 和 LDAP 服务等。

能够支持 NetFlow、sFlow、NetStream 等流数据的采集和归一化。

3.具体应用场景和应用模式

（1）威胁分析设计

威胁分析通过运营管理平台实现，用于对现网进行安全状态的分析，并根据现在进行态势统计、风险预测等，提供宏观层面的全网安全状态。

安全运营中心通过大数据架构设计的流式关联分析引擎，能够实时关联多维度数据，包括多数据来源的日志、威胁情报数据、资产管理数据、资产漏洞数据、关注的 IP 列表数据、可访问端口列表和可访问域名、URL 列表等，对告警进行有效降噪。

安全运营中心能够将现网安全状态，形成针对工控网络环境中人、物、地、事、关系的多维视图，将分析结果根据不同的场景进行展示，常见的场景分析应该包含 HTTP 代理分析、DNS Tunnel 分析、弱口令分析、暴力破解分析等。

（2）流程闭环设计

流程闭环通过人机互动的方式实现，以运营人员为基础，安全运营中心以及网内所有安全设备为工具，实现威胁处理的闭环。

安全运营中心提供多种响应处置方式，将不同危害等级、影响范围的告警通过三种主要场景实现闭环，场景如下：

➢ 场景 1

运营人员通过工单派发任务，实现人与人工作通过系统自动化流转场景。

➢ 场景 2

运营人员通过系统通知派发任务，支持短信通知、邮件通知、系统消息等。

➢ 场景 3

运营人员通过处置联动功能，发送指令给防火墙、主机卫士等安全设备，实现隔离失陷主机、全网隔离恶意文件、阻断内网主机与恶意 IP、域名的通信等处置方式。

（3）日常巡检设计

日常巡检是运营中心的日产工作之一，巡检的对象包含：重要网络设备、安全设备、主机，巡检的频率至少为每一天一次，巡检的应包含内容如下：

➢ 重要网络设备

序号	服务项	巡检内容
1	设备硬件状态巡检	● 设备硬件的运行情况：电源、风扇、机箱、各个板卡、flash 卡、状态灯的运行状态等 ● 各个物理端口的稳定性检查 ● 连线情况、标签和标识情况 ● 设备硬件报警信息
2	设备软件状态巡检	● 系统内核运行状况 ● 是否有新的内核升级程序可以使用
3	设备性能状态巡检	● CPU 利用率 ● 内存利用率 ● 网络接口使用率 ● Buffer 使用情况
4	安全策略检查与优化	● 安全策略正确性和有效性复核
5	日志检查	● 日志接收是否正常 ● 日志是否需要满日志处理 ● 日志收集和分析

➢ 安全设备

序号	巡检项	巡检内容
1	设备硬件状态巡检	● 设备硬件的运行情况：电源、风扇、机箱、各个板卡、flash 卡、状态灯的运行状态等 ● 各个物理端口的稳定性检查 ● 连线情况、标签和标识情况

		● 设备硬件报警信息
2	设备软件状态巡检	● 系统内核运行状况 ● 是否有新的内核升级程序可以使用 ● 软件系统版本升级
3	设备性能状态巡检	● CPU 利用率 ● 内存利用率 ● 网络接口使用率 ● Buffer 使用情况
4	安全策略优化	● 安全策略正确性和有效性复核
5	日志检查	● 日志接收是否正常 ● 日志是否需要满日志处理 ● 日志收集和分析
6	规则库检查	● 检查防毒墙等病毒定义升级情况 ● 检查 IDS/IPS 规则库升级情况

➢ 主机巡检

序号	巡检项	巡检内容
1	主机硬件状态巡检	● 主机设备硬件的运行情况：电源、风扇、机箱、各个板卡、状态灯的运行状态等 ● 网卡的状态、IP 地址、路由表等信息 ● 磁盘阵列运行状态 ● 系统故障灯显示情况 ● 系统硬件错误报告
2	主机操作系统安全检查	● 操作系统软件版本情况 ● Windows 系列补丁安装情况 ● Linux 系列补丁安装情况 ● Unix 系列补丁安装情况 ● 操作系统安全配置检查与优化：账户、安全策略、服务等 ● 系统日志分析 ● 补丁安装
3	主机性能检查	● CPU 利用率 ● 内存利用率 ● 交换区使用率 ● 磁盘占用空间

		● I/O 工作情况
4	可疑服务进程检查	● 开启服务名称 ● 服务开启必要性 ● 服务占用资源情况
5	病毒检查	● 客户端病毒软件安装情况 ● 病毒定义库升级情况 ● 策略分发情况 ● 病毒处理情况

（4）安全监测设计

安全监测是是安全运营中心主要工作之一，安全运营中心利用现有的安全设备，日常监测告警信息，对于结果做人工研判，进行误报/确认分类，日常监测的内容主要包含:

一级分类	二级分类
漏洞事件	● 配置错误、跨站脚本攻击、SQL 注入、路径遍历、未充分验证数据可靠性、安全特性问题等类型
访问异常事件	● 访问状态异常、DNS 解析异常、等其他异常
信息篡改事件	● 黑链、内容变更、违规内容、挂马等类型
信息假冒事件	● 钓鱼、中间人攻击等类型
攻击利用事件	● SQL 注入、URL 跳转、代码执行、非授权访问/权限绕过、XSS/CSRF 等类型
恶意软件事件	● 后门程序、间谍软件、恶意广告、键盘记录、病毒、勒索软件等类型
拒绝服务攻击事件	● SYN Flood、UDP Flood、ICMP Flood、ACK Flood、DNS Response Flood 等。

（5）安全报告设计

安全报告是运营中心的日常工作之一，安全报告的种类包含事件报告、安全月报、年度总结等模板，运营平台也可根据现网需求自定义报告格式及内容。

事件报告主要包含事件等级、事件影响、事件分析、修复建议、工单流程等内容;

安全月报主要包含告警数量、工单数量、安全态势、典型事件分析等内容;

年度总结主要包含告警数量、漏洞数量、病毒数量、工单数量、告警分类、告警分级、安全态势等内容。

（6）应急响应设计

应急响应是安全运营中心的重要工作之一，应急响应通常分为准备阶段、启动阶段、抑制阶段、根除阶段、总结阶段。准备阶段属于常态化阶段，建立在网络安全事件发生之前，需要事先建立应急组织以及应急预案；当发生网络安全事件后，进入启动阶段，根据应急预案调度相关资源；启动阶段后进入抑制阶段，第一时间将安全网络攻击阻断，损失控制在一定范围内；启动阶段后进入根除阶段，通过技术手段应对安全问题，并进行逐台数据、应用的恢复以测试应对方式的有效性，在有效性得到验证后，进行大面积的业务、数据恢复；根除阶段后进入总结阶段，对本次网络安全事件进行溯源分析，补足短板，避免后续再次发生同类的网络安全事件。

4. 方案亮点

（1）终端规范入网

终端，作为企业信息交互的最基本单位，其安全问题早已成为整个信息安全建设中最重要的组成部分。尤其随着数字化转型不断推进，终端种类繁多，数量巨大、部署分散、安全属性无法统一等现状，所带来的安全隐患不言而喻。

方案制定了完备终端的入网及更新流程，确保“违规不入网，入网必合规”，极大的收敛工控网络安全系统的受攻击面。

（2）定期风险评估

风险评估是风险管理的基础，风险管理要依靠风险评估的结果来确定随后的风险控制和审核批准活动，使得组织能够准确“定位”风险管理的策略、实践和工具。从而将安全活动的放在重点信息资产上，选择成本效益合理的、适用的安全对策。

网络安全风险评估是对信息资产进行评估分析，参照风险评估标准和管理规范，判断安全事件发生的概率以及可能造成的损失，提出风险管理措施的过程。本方案可依靠安全运营平台，实现定期风险评估。风险评估包括资产识别估价、威胁识别、脆弱性识别、风险分析、风险处置建议等内容。

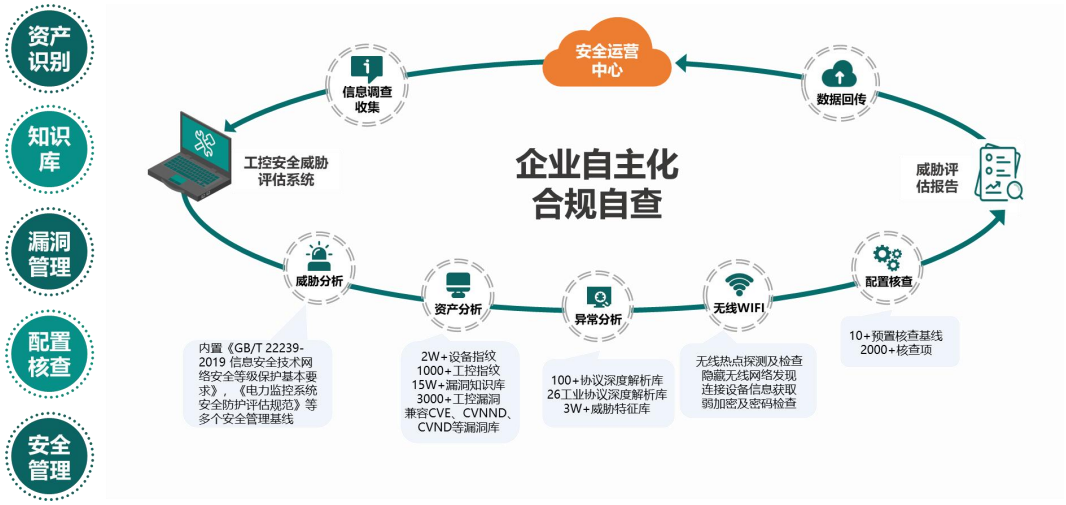


图 6-5 定期风险评估流程示意图

（3）应急响应闭环

成熟的网络应急响应机制能够帮助公司最大程度地降低信息安全突发事件的负面影响，通过检测，分析，研判等流程可以快速地对安全事件进行应急处置，例如：对已产生的攻击事件，根据研判组已经制定的处置方案结合处置，在明确攻击源IP的情况下及时对源IP资产进行确认，然后联系源IP所属资产管理人进行下线或断网处置，如为非法IP资产将及时通知网络封堵组对源IP进行封堵；分析攻击者尝试利用的漏洞信息，确认该漏洞的攻击条件与影响范围然后联系被攻击资产的管理人核查系统是否存在该安全漏洞，如存在安全漏洞将立即下线并制定漏洞的修复方案及时进行修复；使用自动化安全策略系统或者脚本化工具，自动封禁IP，并实现IDS、边界防火墙等安全设备的联动处理。通过安全运营平台完善的网络安全应急响应体系，能更加快捷高效地应对网络安全事件，保护自身的安全。

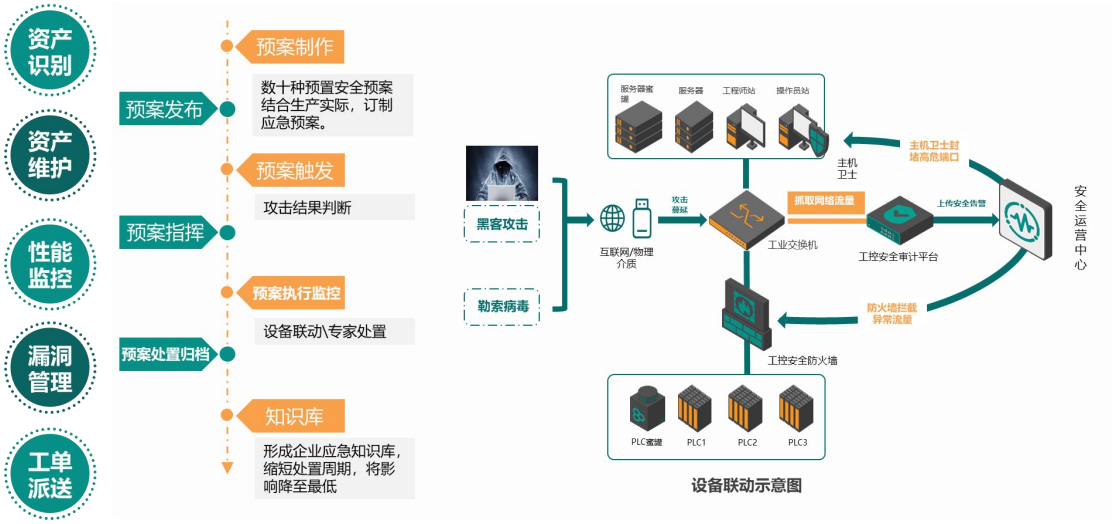


图6-6 应急响应流程示意图

2.7.3 下一步实施计划

1. 打造技术过硬的工控网络安全技术人才队伍

工控网络安全运维队伍是保障所有工控网络安全技术措施落实的基础，不折不扣的落实企业网络安全的合规性要求是其必须完成的任务；但如何更好的推行安全运维则是更具挑战性的工作。工业控制系统安全是信息安全和自动化控制技术的交叉学科，对网络安全人才的技术能力要求也更高，打造技术过硬的工控网络安全技术人才十分必要。

2. 建设核工业工控网络实训平台建设

为了整体提升网络安全防护水平，必须通过建设一套可供集团及企业内部开展网络安全仿真验证和能力培训的平台。而且网络安全队伍能利用平台进行持续的能力培训，提升对网络攻击的了解程度、对网络防护的能力水平，需要团队人员持续的开展系统知识学习、实战演练和能力评估。将人员培训、实践和选拔的活动形成良性循环，锻炼团队的网络安全协同作战能力。

同时，通过一套实训平台也能够满足企业开展网络安全技术实验和研究工作的需求。实现信息系统、工控系统等典型网络信息化环境的高度仿真，模拟真实环境下的漏洞挖掘、安全事件分析、攻防技战法验证、工控协议安全分析、安全研发测试等，也是实训平台的重要工作支撑方向。

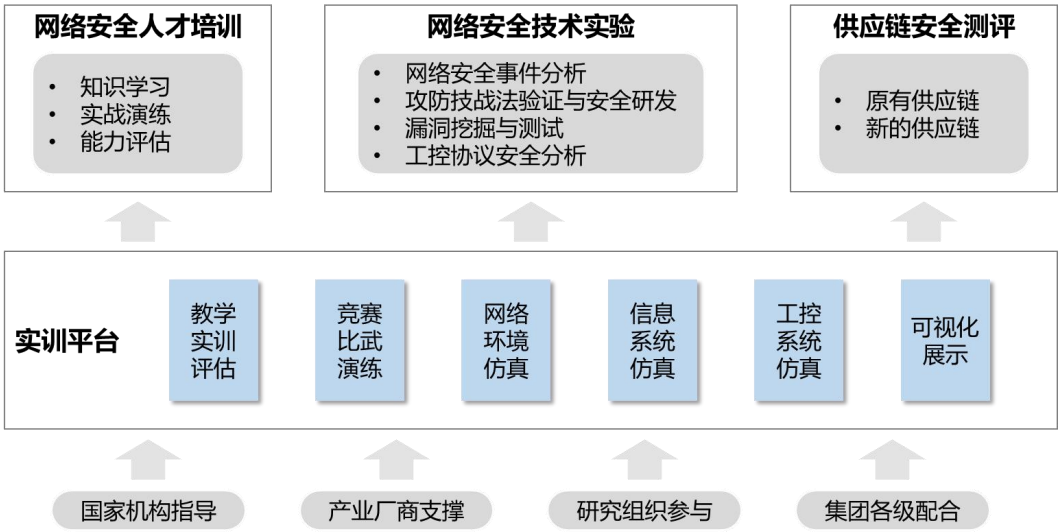


图 6-7 工控网络实训平台示意图

3. 形成贴合实际业务的 5.3.3 漏洞管理机制

由于漏洞的出现不可避免，单个信息资产对于漏洞的处置未必及时有效，因此非常有必要在集团层面进行统一管理。在发现漏洞时，企业需要第一时间分析评估漏洞对企业网络安全的影响，尽快与网络设备、安全设备、系统建设与运维等供应商定最优处置方案，在不影响业务情况下对系统完成相关整改动作。

加强对信息资产漏洞的管理，应重视漏洞管理流程、漏洞扫描、虚拟补丁技术与前置的安全措施，通过管理手段将漏洞管理机制运转起来。

当前对漏洞的生命周期的主流思路是划分为 5 个环节:漏洞产生、漏洞发现、漏洞公开、漏洞评估、漏洞修复。但对企业而言，真正需要关注的是在获取漏洞信息后的漏洞评估与漏洞修复环节。

漏洞的产生、发现与公开环节，在企业具体实践中，可通过风险评估、渗透测试、漏洞扫描、情报接入、手工导入等方式完成漏洞的识别。漏洞的管理还应与上文提到的信息资产管理进行关联，这样识别的漏洞才有关注的价值和修复的可能。新识别的漏洞需要通过评估确定影响、修复方案与时间要求，因此也需要制定相应的流程管理规则，让各方可以形成漏洞评估的共识。

在漏洞修复环节，具体还包括漏洞跟踪和回归测试的任务。由于系统和设备的停机计划不一致、补丁影响业务运行、缺少运维支持或其他原因，往往会出现漏洞长时间无法修复的实际状况，也就导致漏洞跟踪成为一项必不可少的定期任务。在顺利的情况下，系统和设备完成了相关漏洞修复动作，也需要进行漏洞的回归测试，确定不会出现无效的整改措施。

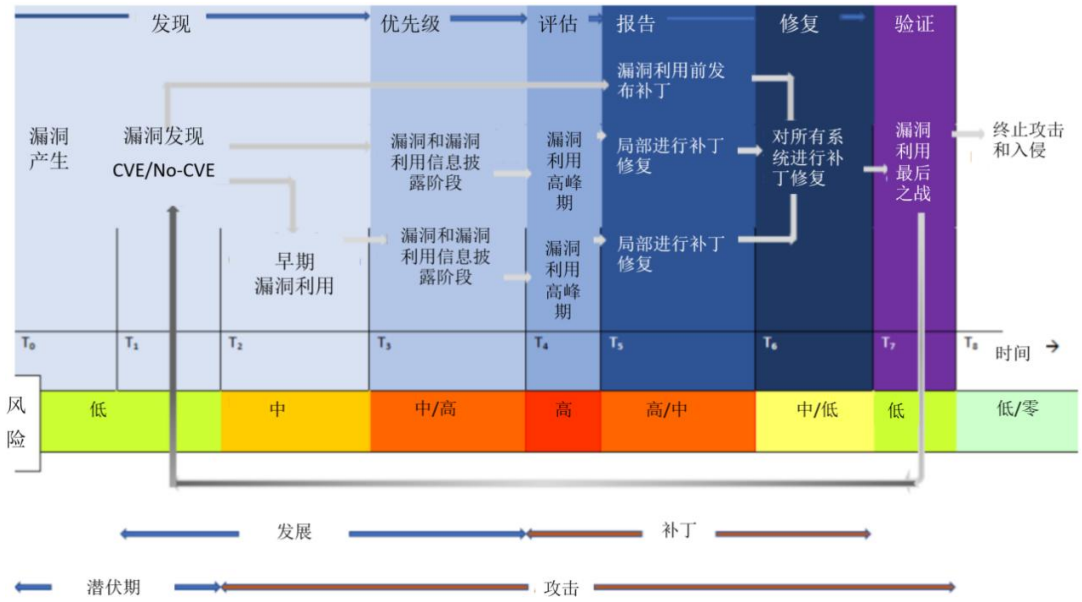


图 6-8 漏洞全生命周期管理示意图

2.7.4 方案创新点和实施效果

1.项目先进性及创新点

（1）拥抱 PKS 体系，打造“中国芯”软硬一体化解决方案

军工行业网络安全十分重要，本方案采用的软硬件均自主安全可控。针对软硬件运行环境所依赖的 CPU、操作系统、底层架构服务组件、数据库、中间件等运行必备功能组件进行国产化适配，积极拥抱“PKS”体系，打造“中国芯”软硬一体化解决方案。

（2）采用自适应安全框架，实现安全防御机制自优化

工控安全防护体系采用自适应安全框架，从预测、防御、检测、响应四个维度，强调安全防护是一个持续处理的、循环的过程，细粒度、多角度、持续化的对安全威胁进行实时动态分析，自动适应不断变化的网络和威胁环境，并不断优化自身的安全防御机制。

（3）构建企业安全运营中心，提升安全闭环自动化处置能力

安全运营中心通过大数据架构设计的流式关联分析引擎，能够实时关联多维度数据，包括多数据来源的日志、威胁情报数据、资产管理数据、资产漏洞数据、关注的 IP 列表数据、可访问端口列表和可访问域名、URL 列表等，对告警进行有效降噪。通过安全运营中心可实现资产台账、威胁分析、响应闭环、日常巡检、

安全检测、安全日报和应急响应等功能，降低运维人员工作负荷极大的提升工控网络安全自动化程度，保障工业生产系统安全稳定运行。

2. 实施效果

项目实施后，可有效解决该核燃料产业企业工业控制系统的网络安全风险问题问题，实现了以安全运营中心为基础，建设检测中心、防御中心、回溯中心三大中心。检测中心专注于事前检测，防御中心专注于事中防御，回溯中心专注于事后回溯。四中心联动形成“预测、防御、检测、响应”闭环流程，保障工控系统网络安全，持续护航安全生产。

项目建成后，工业控制系统防护水平可满足等保三级的安全防护要求；方案同时充分考虑了用户后期智联融网的建设需求，做好了技术准备工作，并预留了相关接口；

系统投运以来，安全平稳运行，各项技术指标优良，达到预期目标。安全运营平台累计发现安全威胁事件 30 余件、安全漏洞 5 项，通过平台成功处置安全突发情况 3 次。

2.7.5 单位基本信息

浙江木链物联网科技有限公司（以下简称“木链科技”）深耕工业互联网安全领域，业务涵盖军工、电力能源、钢铁冶金、轨道交通、智能制造、市政水务、石油石化、烟草等行业，拥有工信一所、信通院、中国电子、中国船舶、国家电网、中石油、中石化、中广核、中能融合、中天钢铁、普天铁心、昆明铁路等重要客户伙伴。公司为中天钢铁集团构建的安全运营生态平台项目收获国家级和省级双重荣誉，国网电科院实验室建设项目摘得中国工业信息安全大会优秀应用案例，中船集团实验室项目提速船舶行业工控安全研究进程，核能行业协会 CTF 安全竞赛项目成为重要里程碑节点。在“十四五”背景下，木链科技积极做好新时期新形式下的工业信息安全工作，以安全技术创新为抓手，构建安全价值生态，保障中国工业信息化建设稳固前行，切实维护国家安全和人民利益。

2.8 案例七：免改造应用的工业互联网数据安全防护案例——免改造交付多重安全能力，实现安全与业务有机融合，护航工业互联网数据安全

数字经济时代，产业结构优化拉动新业态的涌现，工业涉及配方、工艺、图纸、数模等核心数据正逐步由中低附加值向中高附加值转变，《“十四五”数字经济发展规划》提出“建设可靠、灵活、安全的工业互联网基础设施，支撑制造资源的泛在连接、弹性供给和高效配置”。因此，保护数据安全成为核心要务。

炼石网络作为一家以“免改造”为核心创新特色的数据安全产品厂商，自研可灵活挂载多种数据安全能力的免改造平台，通过可适配企业应用架构的一系列数据控制面，对流动数据高覆盖率识别与控制，横向覆盖广泛应用、纵向叠加识别、加密、去标识化、检测/响应、审计追溯等多阶安全能力，在数据收集、存储、使用、加工、传输、提供等各环节提供有效数据保护，帮客户打造领先的数据安全保护体系，同时敏捷交付国密合规改造，保障数据监管合规，促进数据有序流通，打造安全机制与业务处理紧密融合的实战化数据防护体系，助力工业领域数据安全防护水平的提升。

2.8.1 方案概述

本项目基于免改造应用工业互联网数据安全防护案例建设，立足于实战化和新合规的双重要求，以免改造数据安全技术为核心，将安全能力叠加渗透到工业互联网业务全流程，敏捷实施细粒度数据保护，打造实战化数据安全密码防护体系，实现数据开发利用和数据安全保护二者兼得，保障业务应用中数据开发利用安全。

1. 方案背景

工业互联网作为新质生产力的关键组成，通过实现人、机、物的深度互联，以及全要素、全产业链、全价值链的紧密相连，正在逐步重塑传统制造业的固有形态。在这一变革中，数据已然成为生产制造和服务体系的核心驱动力，对于提升制造业的生产力、竞争力和创新力起着举足轻重的作用。然而，工业互联网数

据由于其泛在互联和资源汇聚的特性，让数据的暴露面更广，攻击路径更加多样化，敏感数据的巨大价值成为黑客和恶意分子的主要攻击目标，导致工业互联网数据安全面临多重风险与挑战:

（1）技术风险

伴随工业互联网新业态的兴起，网络黑客与恶意分子所采用的工具及攻击手段亦随之不断演进。举例来说，分布式拒绝服务（DDoS）攻击通过生成庞大的网络流量淹没目标系统，导致其服务不可用；SQL 注入攻击则针对后端数据库的安全漏洞，通过注入恶意 SQL 命令来非法获取或篡改数据；跨站脚本（XSS）攻击利用网站安全缺陷，在用户浏览器上执行恶意脚本，窃取用户信息或破坏网站功能。攻击手段的日益翻新，对工业互联网的数据安全性构成了严峻挑战。鉴于此，工业互联网相关企业亟需加强安全防护体系。

（2）管理挑战

随着企业数字化转型步伐的加快，工业互联网正面临着前所未有的安全挑战。在此过程中，传统的网络安全边界已显不足，无法满足新形势下的安全需求。为此，企业必须制定和实施更为精准的安全策略，确保能够应对日益复杂的网络攻击。在数据管理层面，确保在整个数据流转过程中，包括收集、存储、使用、加工、传输、提供和公开等七个环节中的安全。

（3）法律风险

重要数据保护应遵循合规要求。《网络安全法》首次提出了“重要数据”的概念，并对其出境传输提出了要求；《数据安全法》明确了数据分类分级管理的要求，对重要数据的识别、保护和监管提出了具体规定；《个人信息保护法》涉及个人信息的收集、存储、使用、加工、传输等环节的安全管理，保护个人隐私权益。因此，企业对重要数据应严格保护，以防止数据泄露风险，危及国家安全。

2. 方案简介

炼石打造的工业互联网数据安全防护方案，实现了在免改造应用的前提下，为工业互联网构筑数据安全屏障。本方案融合免改造数据安全技术，实现了对数据的精细化管理与防护，确保了安全措施与业务应用的技术独立性，辅以数据识别、防护、检测/响应、追溯等安全技术，不仅助力企业构建卓越的密码安全能力，满足合规性要求，更能满足实战防护需求，显著提升工业数据安全的防护水

平。此外，本方案覆盖事前事中事后的安全防控，为用户数据安全体系建设提供技术支撑，增强数据安全保障能力。总体上，在数据安全实战场景中，以数据流动为核心业务体现，以数据控制面作为关键着力点，重构安全规则，从而达到消减风险的目标，实现安全与业务在技术上解耦、能力上融合。

3. 方案目标

（1）实现工业互联网设计、制造、检测全链条闭环安全保护

本方案通过设计的数据安全架构，实现了对工业互联网中设计、制造、检测三个关键环节的闭环数据安全保护，确保了数据的传输和存储都在严密的安全控制范围内。本方案采用免改造数据安全技术，对数据进行端到端的保护，无论是在设计阶段的创意草图、详细设计文档，还是在生产过程中的工艺参数、生产日志，以及检测环节的质量报告和分析数据，均实现了加密传输和安全存储。

（2）实现工业互联网运行中的实时状态、管理数据、报警信息、维修信息全实时安全监控

本方案建立全面安全的监控体系。本方案确保在生产运营阶段所有关键信息的机密性和完整性，通过引入免改造加密技术，监控系统能够即时对设备状态、管理数据以及报警和维修信息进行加密处理，防范未经授权的访问和信息篡改。进一步本方案实施严格的访问控制机制，只有授权人员才能够实时获取和查看相关监控数据，保障信息的隐私和安全。

（3）实现人员分级的权限管理和操作防错管理

本方案通过引入细粒度的权限管理机制，系统可根据用户的角色和职责分配不同级别的权限，确保用户只能访问和操作其所需的功能和数据，避免未经授权的信息访问。同时，本方案融合身份验证机制，可有效确认用户身份，保证只有合法用户能够访问系统。

为了防范误操作，系统实施操作防错管理，通过提供清晰的界面设计、人机交互指南以及培训和教育，确保用户了解正确的操作流程和最佳实践，减少意外事件的发生。

（4）强化个人信息保护与管理规范

本方案致力于加强个人信息保护。《个人信息保护法》要求“告知-同意”为核心的个人信息处理规则，要求处理个人信息应当在事先充分告知的前提下取

得个人同意。同时，法律还规定了个人信息处理者应当采取必要措施保障个人信息的安全，包括制定内部管理制度、实行分类管理、采取加密和去标识化等技术措施。本方案明确界定个人信息的收集、使用、存储和共享范围，确保个人信息仅在合法授权和必要的情况下进行处理。同时，完善个人信息管理制度，规范个人信息的处理流程，防止个人信息被滥用或泄露。

2.8.2 方案实施概况

免改造应用工业互联网数据安全防护方案，实现安全与业务有机融合，在防范数据安全风险的同时，也能保障企业满足相关合规要求，助力业务高速发展。

本方案由多个免改造数据控制面、数据安全管理平台以及 KMS 密钥管理系统组成，通过数据资产管理系统提供数据发现、分类分级等功能，再结合旁路部署的数据安全管理平台，并在这些控制面上对流转数据施加加密、访问控制、风险监测、审计追溯等保护能力，构建可适应企业级应用架构的防绕过数据保护机制。炼石免改造数据安全产品对应用是透明的，应用无需改造，也不改变之前的运行机制，不影响企业现有系统的稳定性，确保企业业务不中断；可将应用内的用户身份、字段或文档级数据结合起来，提供“主体到应用内用户，客体到字段级”的细粒度安全防护，保障结构化和非结构化数据安全。

本方案可实现面向运维侧，防范内部 DBA、外包人员、黑客等安全威胁；面向用户侧，防范业务人员越权访问、风险操作以及数据泄露等威胁。典型场景包括政企客户的个人信息保护、企业商业数据保护、政府、央企、金融等行业国密整改、军工与保密行业数据保护等，可针对单个应用防护，也可以针对几十个应用批量保护。

1. 方案总体架构和主要内容

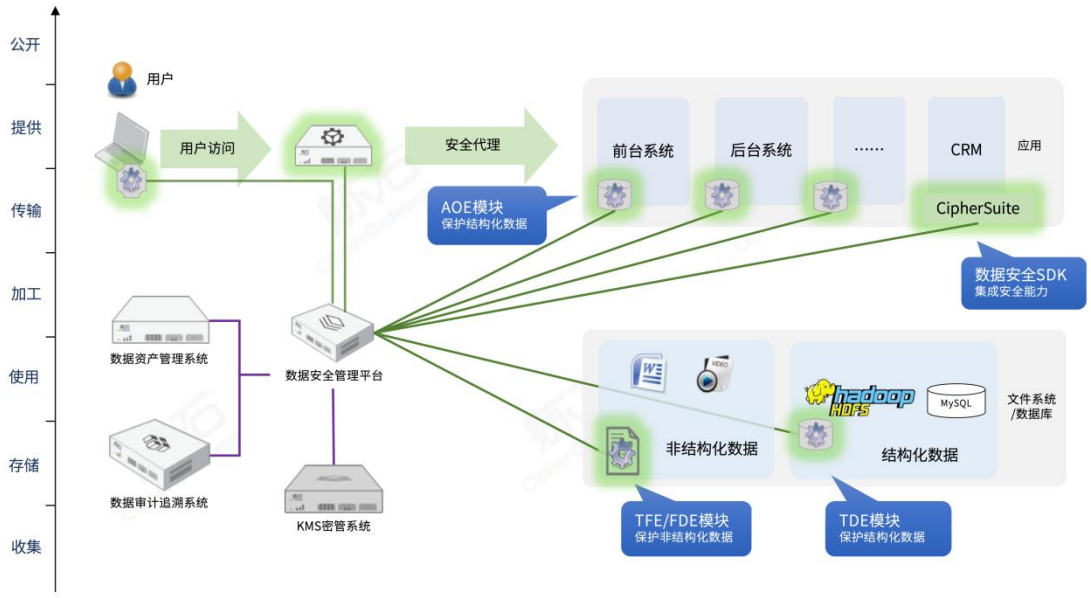


图 7-1 炼石构建实战化数据安全防护

（1）方案整体介绍

本方案基于工业互联网各类场景数据包括生产数据、控制数据、设备数据、应用系统数据、企业数据、用户个人数据等不同类型，通过面向切面安全技术，将安全与业务在技术上解耦、但又在能力上融合交织，实现主体到应用内用户、客体到字段级的防护，在应用层实现免开发改造的、可敏捷实施的高性能数据安全防护。支持结构化/非结构化数据保护，可与应用开发解耦，灵活性高。可支持分布式部署、集中式管控，既可针对单个应用防护，也可以针对上百个应用的批量保护。同时，提供细粒度的身份访问控制、多种脱敏策略以及审计功能，打造“以加密和去标识化技术为核心，融合数据识别、防护、检测/响应、追溯等多种安全技术”的实战化数据安全防护体系，为客户提供全面有效且易于实施的数据安全保护。

（2）构建基于数据安全主平台

本方案基于数据安全主平台可统一数据资产管理、集中安全策略管控。主平台基于免改造数据安全技术，无需改动目标应用系统代码，即可实现为应用系统叠加强化数据保护能力；免改造数据安全技术内含功能性安全模块。数据安全主平台针对业务应用提供多种安全能力供给，通过多安全模块组件下发、策略管理、功能监测，全面覆盖应用系统、数据库、文件系统、磁盘、终端等数据流转多层级，以及数据全生命周期各环节，并支持在高覆盖率的免改造控制点灵活施加数

据识别、防护、检测、响应、恢复、反制等保护能力，实现横向覆盖广泛应用、纵向叠加多阶安全能力，保障数据全生命周期安全。此外，主平台可有效保障结构化和非结构化数据安全，面向 SQL 语句的结构化数据识别和保护，支持按列保护、按规则匹配的行保护等字段级安全；面向 OS 文件驱动层的非结构化数据识别和保护，支持文档级防护。

图 7-2 数据安全主平台核心能力示意图

本方案以数据安全主平台为核心，外延加密模块、去标识化模块、异常行为分析、灾备系统、API 安全等其他安全能力的多层次防御体系，是集网络、平台、数据高度联动的整体防御能力，具有灵活机动（安全模块敏感部署、快速应用）、综合能力强（安全能力作用于数据控制点）、威慑效果好（多层安全防御），可以贴合业务、为数据流转提供有效的连续保护。这种防御体系可以类比“航母战斗群”。在以航空母舰为中心，配置巡洋舰、驱逐舰、护卫舰、潜艇、补给舰，形成航空母舰战斗群的外防区、中防区、内防区三层防御体系。以大型航母为核心，集海军航空兵、水面舰艇和潜艇为一体，是空中、水面和水下作战力量高度联合的海空一体化机动作战部队，可以在远离军事基地的广阔海洋上实施全天候、大范围、高强度的连续作战。

数据安全主平台的核心能力在于对流动数据的高覆盖率识别与控制，实现安全机制与业务流程的有机融合。主平台以数据为建设核心，以业务为作用点，不仅具备丰富的单体作战能力，面向复杂业务数据流程的关键环节，把识别、防护、

检测、响应、恢复、反制等多种安全能力，灵活组合并全面覆盖于收集、存储、使用、加工、传输、提供、公开等数据处理各节点，实现安全逻辑与业务应用相互交织、深度融合，提升数据安全的覆盖度和连接能力；还可以整合、协同其他旁路和外挂数据安全设备，比如可为数据资产治理系统，提供实时敏感数据资产访问；为异常行为监测系统，提供安全策略调整情报等，打造可外延其他数据保护能力的多层次防御体系，为数据流转提供有效的连续保护。

2. 网络、平台或安全互联架构

本方案以工业互联网服务终端数据平台为例，其在数据基础平台、计算分析、业务使用等各个模块、各个阶段的安全需求点整理如下图：

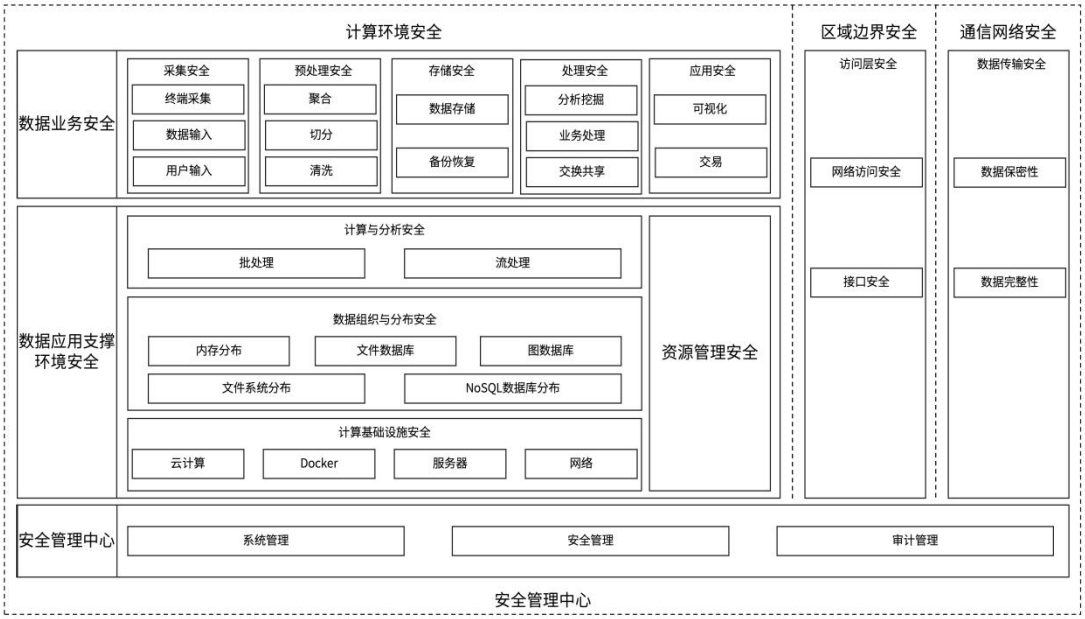


图 7-3 数据安全需求

面向图中区域边界、通信网络等模块方面，利用现有的、常用的、粗粒度的安全产品难以奏效。因此，需要在数据模块内部，将密码技术与措施紧密融合。结合上图安全需求梳理如下：

采集安全需求：工业互联网中设备种类的广泛性和数据采集过程的复杂性，传统的加密措施已不足以应对所有潜在风险。因此，需要考虑设备端实施前置加密，以确保数据在采集过程中不被篡改或窃取，维护数据的真实性、完整性和抗抵赖性。

传输安全需求：工业互联网数据的传输通常涉及大量的实时数据，如传感器

数据、生产线数据等。这些数据的传输不仅要求加密，还需要考虑数据的实时性和可靠性。因此，在传输过程中，除了使用密码服务中间件外，还应考虑使用专用的工业网络安全协议，确保数据在传输过程中的安全。

存储安全需求：工业互联网数据涉及的数据量巨大且类型多样，对存储和保护机制提出了更高的要求。结构化数据，如数据库中的表格记录，与非结构化数据，如传感器生成的日志和图像，加大了工业互联网数据的安全防护的复杂性。

处理分析使用安全需求：工业互联网数据在处理和分析工业互联网数据时，需要确保数据的真实性和完整性。这要求在处理过程中使用可信的验证服务，防止数据被非法篡改。同时，还需要考虑数据的隐私保护，避免敏感信息泄露。

共享交换需求：工业互联网数据的共享和交换是提升数据价值的关键。在共享数据时，应提供一系列密码服务来确保数据的安全性和隐私性。同时，还需要考虑数据的访问控制和审计功能，确保只有授权的用户可以访问数据。

归档或销毁安全:工业互联网处理不再使用的数据时,需要进行归档或销毁。在归档过程中，应确保数据的完整性和可恢复性。在销毁数据时，应使用专业的数据销毁工具和方法，确保数据被彻底删除，无法恢复。

综上所述,工业互联网数据的安全需求涵盖了数据的全生命周期,包括采集、传输、存储、处理、共享和销毁等环节。为了确保工业互联网数据的安全性和隐私性，需要采取一系列的技术和管理措施来应对各种风险和挑战。

（1）数据安全技术框架 DTTACK

1）DTTACK 的设计思路

网络安全持续的变化，攻防之间的博弈在不停的进化，已有的网络安全能力的度量逐步显露出局限性和不适用性。数据安全建设领域亟待出现新的安全能力度量方式，以应对不断变化的网络与数据安全发展趋势。

如果说 ATT&CK 的出现，是让攻击手法拥有通用语言，那么 DTTACK 的诞生便是对数据本身进行主动式防护，为防护模式打造了通用技术库。DTTACK 不是网络服务器或应用程序安全性的模型，它更强调数据本身的安全性，并从对数据的应对式防护向主动式防护转变，重视从业务风险映射视角列举数据保护需求，也可以为信息化建设、企业业务架构设计提供数据安全能力参考。

目前，炼石已初步梳理 6 个战术，31 个技术，83 个扩展技术，145 个方法，并持续更新迭代，致力于打造数据安全领域的专业技术框架。

2）DTTACK 的设计理念

重视从业务风险映射视角列举数据保护需求。安全本质上是一种业务需求，“传统业务需求”侧重于“希望发生什么”，而“安全需求”侧重于“不希望发生什么”，从而确保“发生什么”。而数据安全需求重点是数据的机密性和完整性。

当前版本的 DTTACK，在数据安全技术列举方面，参考了工信部相关机构正在编制的行业标准《电信网和互联网数据安全管控平台技术要求和测试方法》，将 114 个具体技术流程分类并对号入座，为数据安全建设提供技术支持。

结合 NIST 安全能力模型、安全滑动标尺模型。DTTACK 框架的构建，以 NIST 安全能力模型和安全滑动标尺模型为参考，并做了整合与精简。基于此，DTTACK 最新版本选择了六大战术作为基本结构: IDENTIFY（识别）、PROTECT（防护）、DETECT（检测）、RESPOND（响应）、RECOVER（恢复）、COUNTER（反制）。

安全滑动标尺模型为企业在威胁防御方面的措施、能力以及所做的资源投资进行分类，可作为了解数据安全措施的框架。模型的标尺用途广泛，如向非技术人员解释安全技术事宜，对资源和各项技能投资进行优先级排序和追踪、评估安全态势以及确保事件根本原因分析准确无误。该模型包含五大类别: 基础结构安全、纵深防御、态势感知与积极防御、威胁情报、攻击与反制。这五大类是一个非割裂的连续体，从左到右，具有一种明确的演进关系，左侧是右侧的基础，如果没有左侧基础结构安全和纵深防御能力的建设，在实际中也很难实现右侧的能力有效发挥。从左到右，是逐步应对更高级网络威胁的过程。

（2）面向失效的安全设计

针对数据安全漏洞的攻击变得体系化加大了防御的难度，但获利环节让攻击暴露更多细节，使得防御者有了更加精准的防护切入点。在数据安全防护过程中，不存在一招制敌的战法，基于 DTTACK 的防御纵深，将凭借先发优势、面向失效的设计、环环相扣的递进式设防，成为百战不殆的有效战术。

1）面向失效的设计

面向失效的设计原则是指，任何东西都可能失效且随时失效。需要考虑如前面一道防御机制失效了，后面一道防御机制如何补上后手等问题，考虑系统所有可能发生故障或不可用的情形，并假设这些可能都会发生，倒逼自己设计出足够健壮的系统。是一种在悲观假设前提下，采取积极乐观的应对措施。

面向失效的设计是防御纵深的关键。整体思路，从传统静态、等待银弹的方式转向积极体系化的防御纵深模式。分析进攻者的进入路径，基于面向失效的设计原则，打造多样化多层次递进式的防御“后手”。

2）数据安全纵深防御

“纵深防御”是一种应该体现在数据安全防御体系设计各个方面的基本原则，而不是一种“可以独立堆叠形成的解决方案”。

从安全能力构建数据防御纵深。“IPDRRC”体现了数据保护的时间顺序，基于时间维度，可以有机结合多种安全机制。识别是一切数据保护的前提，在数据识别与分类分级，以及身份识别的前提下，针对数据安全威胁的事前防护、事中检测和响应、事后恢复和追溯反制等多种安全机制环环相扣，协同联动，可以有效构建出面向失效的纵深防御机制。

从数据形态构建数据防御纵深。数据大致可以分成传输态、存储态和使用态，而身份鉴别及信任体系则是对数据访问的补充或者前提，基于“数据三态”可延伸出数据全生命周期。围绕数据形态，可以构建多种安全机制有机结合的防御纵深。

在传统网络安全防护中，边界是非常重要的概念，边界上可以构建防火墙或IDS 等规则。但数据防护过程中，数据没有边界，如果应用密码技术，则可以起到一种虚拟边界的作用，从而在虚拟边界基础上对数据实施保护，形成有效保护作用。在数据存储和使用态的切换中，如果不经过数据加密，只进行访问控制和身份认证，当明文数据在数据库或归档备份时，数据访问容易被绕过。但当我们在数据流转的关键节点上，对数据进行加解密，并结合用户的身份信息和上下文环境做访问控制，可以构建防绕过的访问控制、高置信度的审计，进而在数据存储、使用形态上形成防护纵深，构建出密码安全一体化的数据防护体系。

从技术栈构建数据防御纵深。信息系统的技术栈体现了空间维度，这也可以作为数据保护的纵深。沿着数据流转路径，在典型 B/S 三层信息系统架构（终端

侧、应用侧、基础设施侧）的多个数据处理流转点，综合业内数据加密技术现状，总结出适用技术栈不同层次的数据保护技术。继续前文所述的 IPDRRC 中数据防护段的密码技术，保护数据存储态，再结合典型信息系统的技术栈分层，可以从技术栈维度构建数据防御纵深。

综上所述，从安全能力、数据形态、技术栈等多个不同维度上，有机结合多种安全技术构建纵深防御机制，形成兼顾实战和合规、协同联动体系化的数据安全新战法。

3. 安全及可靠性

（1）安全性

1）免改造数据安全技术促进工业互联网数据依法有序安全流动

本项目基于免改造数据安全技术建立了完善国密防护体系，保障内部多平台间数据共享渠道安全，确保工业互联网相关企业数据的机密性、完整性和可用性。通过国密技术避免数据滥用和非法获取，推动跨系统、跨部门、跨地区的数据融合和创新应用，确保数据依法有序安全流动，充分释放数据的价值，为数字经济做强做优做大提供有力支撑。

2）免改造数据安全方案满足工业互联网法规标准合规要求

本项目严格遵守《网络安全法》《密码法》《数据安全法》《个人信息保护法》GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等法律法规和标准规范要求，确保安全防护工作的合规性。通过定制化免改造数据安全方案，配合安全管理机制、风险评估和合规检查工作，确保数据的收集、存储、传输和使用等各个环节均符合法规要求，提升企业合规能力。

3）国密技术保障工业互联网个人信息与数据安全

本项目采用高性能国产商用密码技术、数据脱敏、访问控制和审计追溯等多种安全技术，打造安全易用、场景覆盖完整的国密支撑体系，可以防范数据泄露和未经授权的访问，提高网络和数据安全防护的自主可控能力，切实解决工业互联网涉及的相关企业运行过程中的各类安全问题，提高数据安全性和个人信息保护能力和技术水平，增强企业的市场竞争力。

4）面向工业互联网领域打造国密应用标准化试点示范

本项目可作为标准化、模块化、可复制、易推广的典型示范，快速在企业内部开展平台建设、试点应用、复制推广，为工业互联网相关企业注入国密安全创新的新动力，有助于推动国产密码与工业互联网领域业务相融合的创新商业模式，带动企业提高效率、提升效能、提增效益，拉动上下游产业链发展、提振产业链韧性提供重要保障。

（2）可靠性

1）免改造数据安全技术建设结构化数据保护能力

工业互联网拥有生产、设备、订单、财务和供应量等海量结构化数据，如何实现结构化数据的高效流转和安全保护成为行业挑战。传统的磁盘存储加密技术虽然对工业互联网业务性能影响不大，但颗粒度较粗，很难有效保护结构化数据安全。分级隔离技术虽然能够有效管控数据风险，却会间接影响数据的共享。

想要兼顾结构化数据流转与安全防护，最好的方法是将免改造数据安全技术融合到业务流程中，第一，可以根据工业互联网实际的业务场景，制定针对性的免改造应用方案，第二，工业互联网需要采用高性能的密码技术，将安全机制与现有流程无缝对接，在不改变原有操作习惯，不伤害用户粘性，不影响结构化数据的流转性能的前提下，实现两者之间的动态平衡。

2）构建基于国密的非结构化数据存储加密能力

工业互联网的业务架构往往非常复杂，涉及大量非结构化数据，在国密部署实施过程中，非结构化数据对加解密性能要求极高。如果部署国密技术而影响到工业互联网业务系统的正常运转，将会导致大量企业的权益受到损害。传统技术路线一般会基于密码机硬件设备提供 SDK 对业务系统进行密码整改，一方面给工业互联网中企业的系统的应用开发人员增加了负担，另一方面也带来了较大的业务风险。

工业互联网可以利用高性能国密技术的特性，并结合透明文件加密等安全技术，实现整体安全方案的敏捷实施，最终实现非结构化数据的批量快速部署。工业互联网在确保方案安全可靠的前提下，可以实现方案在多场景、多地域下的快速复制，从而能够实现工业互联网在安全能力方面的快速升级迭代，以更好地适应新技术下的安全挑战。

3）面向敏感数据构建基于国密的“多写操作”

工业互联网拥有海量敏感数据，且具有复杂多变的业务需求，传统全量数据加密在查询、使用、共享、流通等方面具有一定的局限性，不利于高效率业务处理。面向敏感数据构建基于国密技术的“多写操作”，在密码技术的基础上，将模糊化技术、访问控制、审计等多种安全技术相结合，满足敏感数据保护及业务高效处理的双重要求。该功能支持基于模糊化资料表的一般查询和特殊场景下的明文查询，满足工业互联网复杂多变的业务需求。通过模糊化处理，既可以满足一般查询需求，又保护了商业秘密。具备高效同步，利用密文方式同步中心文件，提高数据同步的效率和安全性。分批上线策略，考虑到工业互联网业务连续性的重要性，采用分批上线的策略，逐步推广加密存储，降低对业务的影响，确保系统的稳定性和可靠性。

2.8.3 下一步实施计划

本方案通过试点建设，后续将持续推广，逐渐覆盖工业互联网涉及原材料、装备、消费品、电子等制造业各大领域，以及采矿、电力、建筑等实体经济重点产业应用。在推广过程中，通过免改造数据安全技术确保数据不被未授权访问或篡改，强调用户身份信息、供应链数据和生产过程信息的综合安全管理。

2.8.4 方案创新点和实施效果

1. 方案先进性及创新点

本方案兼容多、交付快、防护好、成本省。兼容多，适应大多数的企业应用架构，如 JAVA、C 等主流开发语言、兼容开放协议的关系型数据库和非关系型数据库、兼容 Linux/信创 OS/Windows 等。交付快，通过免改造应用增强数据安全保护能力，实现敏捷交付。防护好，密码安全一体化，炼石免改造数据安全产品面向应用系统，在应用层以数据为抓手实现数据安全保护，基于“密码安全一体化”，覆盖事前事中事后，实现“主体到人、客体到字段”的细粒度实战防护。成本省，免改造技术在建设期节约了应用系统的开发改造成本，在运维期通过灵活策略节约应用系统的规则适配成本。

2. 实施效果

本方案通过创新的技术手段，可以在较短周期内、以较低风险实现数据安全防护效果。具体来说，本方案采用了先进的加密技术和访问控制机制，确保数据在传输和存储过程中的安全性，同时不需要对原有系统进行大规模的改造，避免了可能带来的业务风险。

本方案的实施过程也非常简便，只需要在原有系统上安装相应的安全模块，并进行简单的配置，就可以实现数据的全面防护。目前，本方案已经在数十个工业场景中完成实施交付，并在客户现场运转正常。这些客户涵盖了制造业、金融业、医疗等多个领域，让商业秘密得到了有力的保护，同时也满足了国家关于数据安全、密码应用相关政策合规要求。

除了数据安全防护效果显著外，本方案还有其他显著优势。首先，本方案提高了企业的数据安全水平，降低了因数据泄露而带来的损失和风险。其次，由于不需要对原有系统进行大规模的改造，节省了企业的时间和成本。最后，本方案还提升了企业的竞争力，使其在激烈的市场竞争中保持领先地位。总之，炼石应用系统免改造的方案是一种高效、低风险的数据安全防护方法，不仅能够在不影响业务运行的前提下保障数据安全，还能够为企业带来多方面的收益。随着数字化进程的加速和数据安全需求的提升，本方案将在更多领域得到应用和推广，为企业的数据安全保驾护航。

展望未来，数据安全领域还将面临更多的挑战和机遇。一方面，随着云计算、大数据、人工智能等技术的快速发展，数据的规模和复杂性将不断增加，数据安全防护的难度也将随之提升。另一方面，随着国家对数据安全法规的不断完善和执行力度的加强，企业对于数据安全的重视程度也将不断提高。在这样的背景下，炼石应用系统免改造的方案将继续发挥其优势，为企业提供更加全面、高效的数据安全防护服务。同时，本方案还将不断创新和完善，以适应不断变化的数据安全需求和技术发展趋势。

2.8.5 单位基本信息

炼石网络成立于2015年，是一家以“免改造”为创新特色的数据安全产品厂商，自研可灵活挂载多种数据安全能力的免改造平台，帮政企客户打造领先的数据安全保护体系，保障数据监管合规，促进数据有序流通。先后获得安天、国

科嘉和、腾讯、重庆科技成果转化基金、朗玛峰创投等投资，为政府、金融、运营商、交通、教医旅、工业等用户提供个人信息保护、商业数据保护、数据安全合规改造、国密合规改造。

2.9 案例八：5G+多租户虚拟专网安全解决方案——安全可控的 SDWAN 组网

在数字经济大发展的时代背景下，如何实现企业数字化改造并保障港口安全成为全球港口共同的诉求。北部湾港作为中国西部沿海唯一的保税港区，致力于通过基于 5G 多租户虚拟专网的安全技术方案推动港口数字化升级和变革，提高港口的生产效率并保障港口安全。依靠 5G 低时延、大带宽、边缘计算及切片能力，该港口实现轮胎吊、轨道吊、岸桥等港机的生产环节的远程作业控制改造，解决了传统远控作业难度大、成本高、光纤容易老旧及断裂等问题。但是，新技术和新业务模式给运营者带来了新挑战：首先，企业上云越来越复杂，且各应用对企业网络提出更精细化的管理需求，企业网络存在容易失控、难以管理、服务等级协议（Service Level Agreement，SLA）能见度不足等问题；其次，应用中引入边缘计算业务，而边缘平台靠近用户处于相对不安全的物理环境；最后，企业管理控制能力减弱，容易发生非法访问、敏感数据泄露、分布式拒绝服务攻击（Distributed Denial of Service attack，DDoS）攻击以及物理攻击等安全问题。为了应对以上安全挑战，中移（上海）信息通信科技有限公司以“可信接入、智能连接、安全守护”为设计理念，打造钦州港 5G+多租户虚拟专网安全解决方案，实现轮胎吊、轨道吊和岸桥等港机的生产环节的远程作业控制及端到端安全保障，生成安全可控的 SDWAN 组网方案。

2.9.1 方案概述

1. 方案背景

广西钦州港属于国家级经济技术开发区，2020 年货物吞吐量达 1.365 亿吨，作为中国西部沿海唯一的保税港区，钦州港致力于通过 5G 技术实现港口智慧化升级与变革，提高港口生产率和效率并确保竞争优势。智慧港口建设中，港机远控、自动驾驶、高清视频、数据采集等业务场景，迫切需要高带宽、低时延、高可靠性的 5G 网络，但 5G 对于智慧港口行业是机遇也是挑战，它在降低网络部署成本的同时，增加了更多的攻击面和新的安全需求。随着国家《数据安全法》的颁布与施行，5G 安全也受到更多的关注与重视。

2. 方案简介

钦州港智慧港口 5G+多租户虚拟专网项目采用 Hub-Spoke 架构，总部数据中心为 Hub 节点，各码头分支站点为 Spoke 节点。总部数据中心部署两台有线接入高性能虚拟专网网关，支持双机备份；各分支码头接入侧部署带有 5G 模组的虚拟专网网关，支持双模，无论是处于 SA 组网或 NSA 组网均可自动接入，若无 5G 信号会自动降级为 4G，网络功能不受影响。

项目于 2021 年 5 月完成部署。总部数据中心两台虚拟专网核心网关作冗余备份，容灾建设，网关下连用户交换机，智能理货服务器和视频数据服务器与交换机相连，现场机械臂 17 路高清摄像头采集高清视频数据，将数据存储在视频服务器中，通过 SDWAN 边缘网关与核心网关之间的加密隧道将高清视频数据高效回传到数据中心。通过现场测试不断发现并修正验证测试中发现的各类问题，最终交付完成后，实现钦州港 5G 轮胎吊 17 路高清视频的实时回传和远程实时控制，同时实现 5G MEC 与网络切片的成功应用，通过设置视频和控制两大切片，分别保证了大带宽和低时延需求，MEC 实现数据本地传输处理，降低控制时延，提升网络效率。

3. 方案目标

随着钦州港智慧港口的建设，新技术与新业务模式给运营者带来了以下三方面的挑战：

（1）当前应用云化使得企业上云越来越复杂，且各应用对企业网络提出更精细化管理需求，企业网络存在容易失控、难以管理，SLA（Service Level Agreement）能见度不足，混合云架构复杂，网络性能难以预测，网络安全威胁等问题。原有的企业组网技术难度大、周期长、成本高，例如采用专线会遇到企业跨区域、跨机构专线组网时建设周期长的问题，增减节点也不灵活。随着企业上云成为趋势，云网协同难度日益升高，构建一体化混合云组网的同时保障云网安全成为了难点。此外，传统的网络设备成本高：多种独立设备硬件价格高，以路由器为代表的传统设备遇到了新的瓶颈，安装和运维人工成本也居高不下。现有网络设备的网管通常基于设备进行管理，难以做到对网络和业务的可视化便捷管理，导致拥有多个分支机构的企业总部对网络缺乏统一的管理手段。

（2）随着 5G 的发展，现有网络将会面临更多上述业务场景下业务连接与处理能力的需求与挑战。由于移动边缘计算平台和移动边缘计算应用部署在通用服务器上，并且靠近用户，处于相对不安全的物理环境、管理控制能力减弱等，导致移动边缘计算存在移动边缘计算平台和移动边缘计算应用遭受非授权访问、敏感数据泄露、(D)DoS （Distributed denial of service attack）攻击，物理设备遭受物理攻击等安全问题。

- 针对以上痛点，充分剖析需求，总结以下四点需求及项目目标:
  - 视频数据不出港口，且实现数据分流
  - 视频数据安全入云、可靠传输（典型安全问题）
  - 实现云间、节点间互联互通
  - 云网运维统一集中管控

2.9.2 方案实施概况

钦州港 5G+多租户虚拟专网建设方案应用 SDN+NFV 技术，采用 5G SA 网络架构，依靠 5G 工业互联网低时延、大带宽、边缘计算及切片技术及能力，实现对港口和数据中心的集中管控，对港口港机远控无线业务进行关键流程分析和业务场景摸查，对各类应用端到端时延和流程提供资源保障，协同网络进行资源编排和动态调整，支撑港口业务监测和预警。系统能做到监测港机工作状态和性能，及时故障报警，防范运行风险，提高运维效率。其核心价值在于通过无关路由服务链技术编排安全能力，灵活地满足不同的安全需求，实现业务层、设备层、网络层等多维度、端到端安全保障，形成“可信、可管、可控”安全 SDWAN 组网方案。

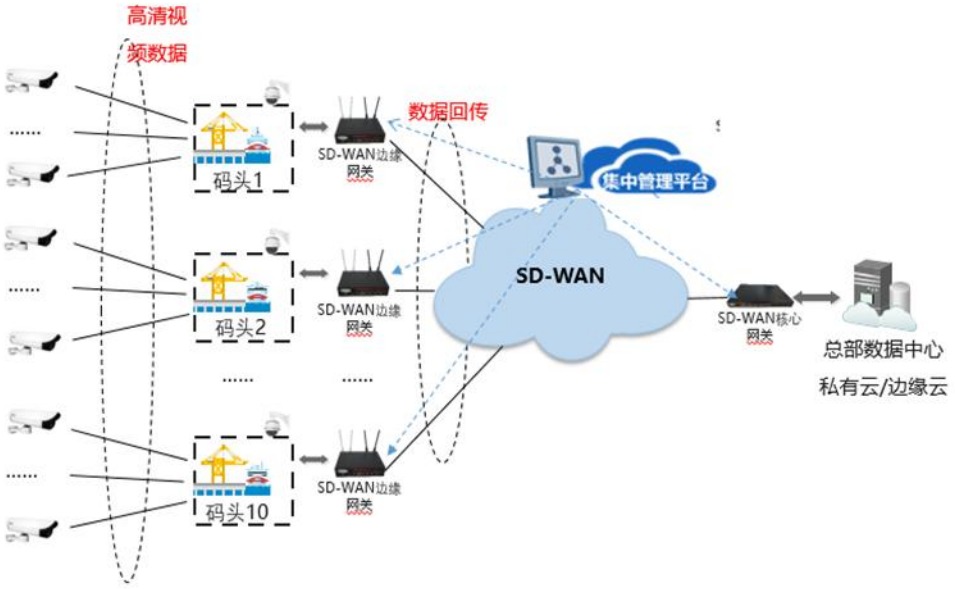


图 8-1 SDWAN 组网方案

1.项目总体架构和主要内容

（1）项目总体架构

钦州港 5G+多租户虚拟专网安全解决方案，在终端层利用终端识别、身份认证等技术保障 5G 终端安全，网络层利用链路遥测技术进行 SLA 质量保证；在业务层通过数据加密隧道和智能安全栈搭建对 5G 行业应用的保护屏障，最后，在展示层对威胁等进行统一展示分析，有助于运维人员及时定位风险，提高工作效率。

详细技术设计框架如图 8-2 所示：

图 8-2　钦州港 SDWAN 组网详细技术设计框架

（2）主要功能及内容

多租户虚拟专网解决方案在 5G 基础网络上搭建 5G 虚拟专网，可助力该港口实现终端可信接入、总部数据中心与各分支互联互通，对网络集中进行可视化管控，能为用户提供动态链路监控分析、基于应用的流量调度、网关设备主备保护（虚拟路由冗余协议）以及链路端到端安全加密等服务。首先，通过负载均衡和动态智能选路等高可用功能，为客户优化线路，提高网络性能；其次，通过虚拟化安全能力和加密隧道能力，保障数据云传输过程中的安全性；再次，应用多租户虚拟专网产品，可实现高清视频和总部数据中心专网的互通；最后，通过 5G 高清视频回传和数据实时采集分析预警来提升作业效率和安全可靠性，降低事故的发生率。

1）终端可信接入

终端梳理：通过钦州港口的摄像头、远控终端等数据采集设备(RTU)特征指纹识别、自动学习等技术，发现设备类型、用户、操作系统等信息，并自动归类形成“一机一档”管理体系，同时在边界部署终端感知探针，进一步增强终端接入多租户虚拟专网发现的感知能力，扩大全网终端的感知范围。

终端可信接入：基于终端梳理的基础上，感知范围内的数据采集终端通过超级 SIM 卡、口令验证、数据签名验证等方式进行身份验证，根据身份验证结果，进行相应的授权，才能正常进行上行数据传输和信令交互。当有非法终端仿冒接入网络，迅速发现并通过制定安全策略等手段进行处置，如工业防火墙直接拒绝该设备的访问请求等，防止非授权设备访问或者授权设备访问越权等安全风险；通过指纹特征信息，防止设备接入身份的伪造，保证多租户虚拟专网终端可信接入。

2）多租户管理

a.租户管理

对于多租户的支持是云计算的主要特性，各个云计算租户能够自行登录虚拟专网管理平台进行组件的申请、安全策略的配置。

5G+多租户虚拟专网管理平台原生支持多租户结构，管理员可以在虚拟专网管理平台本地创建多个租户，并添加多个子账号。在实际使用中，为了减少手动

创建租户的工作量，虚拟专网管理平台也支持对接云平台，定期同步云平台内的账号信息到本地，用户可以直接使用云平台内的账号登录虚拟专网管理平台。账号同步后，用户所有账号的创建、删除、编辑工作都在云平台内完成。

b.租户安全隔离

多租户虚拟专网还支持通过分权分域的组织管理实现对流量的安全隔离。创建组织时自动生成一条 VR（Virtual Router，虚拟路由），每个组织对应不同的 VR，实现租户流量天然隔离，同时结合 IPSec over Vxlan 技术对隧道流量进行加密处理，满足业务流量安全隔离需求。

3）数据安全回传

a.安全加密合规传输

多租户虚拟专网 CPE 侧采用 IPSec VPN 自动组网技术，自动组建加密传输网络。IPSec VPN 加解密算法不仅支持国际主流的 3DES、AES 算法，同时还支持由国家自主设计的国密算法 SM1/2/3/4。可保障数据传输安全，防止通讯过程中出现数据泄漏及数据篡改问题，不仅满足等级保护中对通讯网络要求采用密码技术来实现组网的要求，亦能满足采用经国家密码管理局核准算法的要求。

b.基于业务的安全网络隔离

对于重要业务数据，支持通过采用不同的隧道与普通业务数据进行逻辑隔离，相互之间可形成不同的安全领域，具备不同级别的安全策略。各业务数据通过不同的切片网络进行传输，避免不同的业务之间数据及流量的干扰，确保数据传输的安全性，是合作伙伴接入、不同行政机构接入场景中典型的安全需求。

c.多维动态特征异常检测引擎

多租户虚拟专网 CPE 入侵防御采用先进的多维动态特征异常检测引擎，抛弃原有的异常行为特征码静态表达的方式，结合人工智能深度学习技术将异常行为、恶意行为特征码通过多维度提炼，动态进行表达，使得特征表达更加全面、精准、有效，极大提高了入侵防御检测引擎的命中质量，解决了传统设备检测命中率高，但是误报率同样高的问题。

4）业务质量探测与流量调度

a.业务质量探测

多租户虚拟专网解决方案采用基于 IPSec 隧道封装的隧道链路遥测机制，其通过构造专有的探测报文并将探测报文封装入隧道内转发就如同隧道内的正常转发流量一样，这样探测流量就可以反映出实际业务的通断，并且在探测的过程中还会持续收集隧道链路探测的数据计算出隧道链路的质量数据包括隧道链路丢包率、时延、抖动、跳数信息用于业务的链路调度，保证关键业务优先在高质量链路上传输。

b.智能选路

多租户虚拟专网基于 SDN 的网络编排可以统一调度所有网络资源。这种智能化网络结构，降低了架设广域网的运营成本。并且将广域网及应用变为了可视化，智能路由能够根据用户的外线带宽以及实时网络状况，通过动态调度实现网络内的流量负载均衡和访问路径优化，并且用户可自主设置应用级别，智能流量调度会优先保证用户重要应用的网络质量。基于网络环境的实时状态，将各种应用的数据智能调度到适合的链路上，保障了数据分发的高效性和通讯的实时性，并且管控平台还可以灵活部署在总部侧或者云端。

5）智能安全栈

传统的服务链技术一般都是通过路由串接来实现的，需要创建多个 subnet（子网）把多个 VNF（Virtual Network Function）连接起来，并且无法针对不同的业务选择不同的服务链，性能和易用性较差。

多租户虚拟专网安全栈采用无关路由服务链技术，减少路由环节，非常简单的将不同的 VNF 组、不同业务拼接成多条服务链，性能高效、配置简单灵活。

通过安全栈强大的服务链编排能力，可以根据客户业务需求，自由编排服务链顺序，例如：通过简单的操作即可实现指定业务（HTTP 和 HTTPS）流量先流经 IPS，再流经 WAF，而其他流量流经 IPS，直接流经其他安全设备。

6）集中可视化管控

多租户虚拟专网管控平台可实现全网安全网关及业务状态采集、日志采集，并支持对全网的网络状态、业务数据、网络质量、威胁态势进行集中可视化展示，以及日志审计、数据库审计等安全审计能力。

2.安全互联架构

（1）安全互联架构

本项目以“可信接入、智能连接、安全守护”的安全架构设计理念，为钦州港智慧港口建设保驾护航，实现端到端安全互联保障，安全架构如图 8-3 所示：

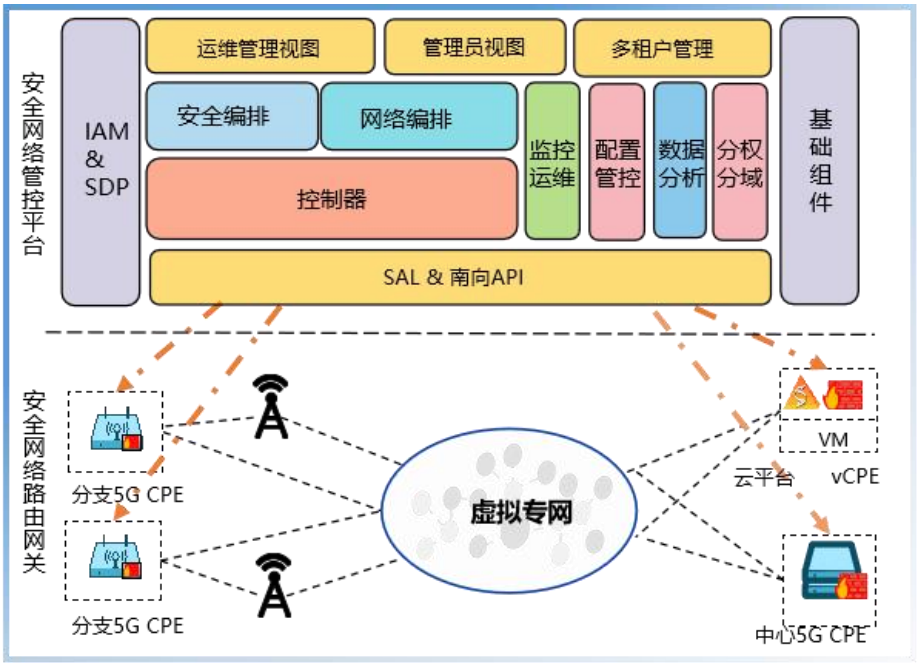


图 8-3　钦州港 SDWAN 组网安全互联架构

a. 可信接入

由于 5G 中 uRLLC 和 mIoT 场景将引入大量新型终端，在带来业务便利的同时，也带来了终端管理的安全难度，如本次研究的钦州港智慧港口项目，该项目采用了大量的摄像头、远控终端，设备的身份验证及访问控制问题是首要解决的安全问题。在本方案中，在身份验证方面，通过超级 SIM 卡、口令认证、基于设备特征指纹等身份验证技术，对接入设备的身份进行有效验证，实现非法访问识别与处置，从而具备终端接入发现、终端识别、仿冒防护、接入异常监控、身份认证能力。在访问控制方面，对已知威胁进行阻断，制定网络阻断策略，防止 DDoS 攻击，结合人工智能深度学习算法，形成行为状态监控预警、设备合规评估和入网追溯能力。并且通过多租户虚拟专网网关与安全栈系统协同联动，实现安全策略自动执行。

b. 智能连接

基于 SDN（Software Defined Network）的网络编排及智能选路：多租户虚拟专网基于 SDN 的网络编排可以统一调度所有网络资源。这种智能化网络结构，降低了架设广域网的运营成本，并且将广域网及应用变为了可视化。智能路由能够根据用户的外线带宽以及实时网络状况，通过动态调度实现网络内的流量负载

均衡和访问路径优化，并且用户可自主设置应用级别，智能流量调度会优先保证用户重要应用的网络质量。基于网络环境的实时状态，将各种应用的数据智能调度到适合的链路上，保障了数据分发的高效性和通讯的实时性，并且管控平台还可以灵活部署在总部侧或者云端。

基于虚拟专用网的链路遥测（探针）技术：采用基于 IPSec 隧道封装的隧道链路遥测机制，其通过构造专有的探测报文并将探测报文封装入隧道内转发就如同隧道内的正常转发流量一样，这样探测流量就可以反映出实际业务的通断，并且在探测的过程中还会持续收集隧道链路探测的数据计算出隧道链路的质量数据包括隧道链路丢包率、时延、抖动、跳数信息用于主备隧道的智能选路。

c.安全守护

数据采集终端和管理平台之间的数据传输安全也是工控系统不得不考虑的安全威胁之一，本方案通过对控制平面、系统平面、组网网络、业务数据四个方面进行安全管控，实现业务数据传输全流程安全管控。

控制平面安全：为防止中间人攻击，多租户虚拟专网 CPE 上线设备准入处理需进行双向认证。认证过程如下图所示：

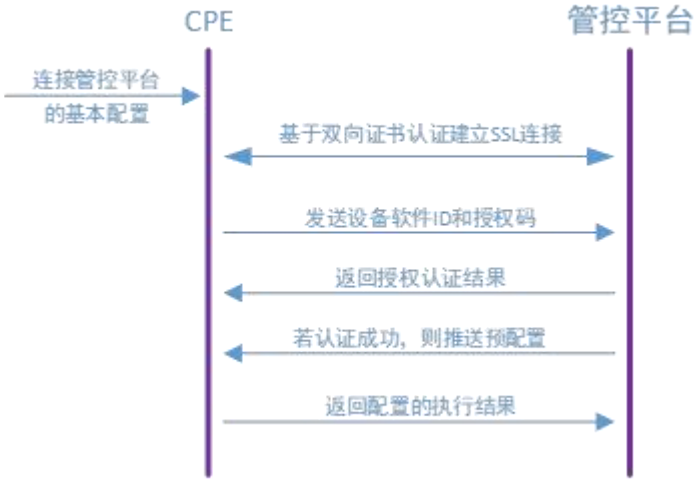


图 8-4　控制平面安全

系统平面安全：采用我司自主研发的多租户虚拟专网产品，该产品由专业的网络安全攻防团队进行全面的安全测试评估，确认产品对漏扫及注入攻击、暴力破解、CC 攻击等安全威胁有优秀的防护作用。

组网网络安全：独特的基于策略的流量牵引技术，可以轻松实现港口业务流量的按需分类防护，避免了各 VNF 对无关流量的重复检测，让 VNF 各司其职，提

高了 VNF 的工作效率；同时提供有状态的服务链编排，提前预判 VNF 健康状态，智能选择服务链；根据用户业务安全需求，灵活组合不同安全能力的 VNF，真正实现按需编排，配置简单高效。多租户虚拟专网安全栈内置了多种安全组件，可供用户根据业务安全需求选择不同的 VNF，实现 vFW、vIPS、vWAF、vScan、vSSL VPN 等安全防护能力。

业务数据安全：IPSec VPN 自动组网技术，实现基于广域网络自动组建加密传输网络，IPSec VPN 加解密算法不仅支持国际主流的 3DES、AES 算法，同时还支持由国家自主设计的国密算法 SM1/2/3/4。可保障数据传输安全，防止通讯过程中出现数据泄漏及数据篡改问题，不仅满足等级保护中对通讯网络要求采用密码技术来实现组网的要求，亦能满足采用经国家密码管理局核准算法的要求。对于港口重要业务数据，支持通过采用不同的隧道与普通业务数据进行隔离，相互之间可形成不同的安全领域，具备不同级别的安全策略。

3.具体应用场景和安全应用模式

5G+多租户虚拟专网安全解决方案，通过设备发现等技术，主动获取感知范围内的设备信息，避免工业互联网组建中设备的遗漏。在此基础上，采用身份认证、访问控制、逻辑隔离等安全技术，实现接入设备安全可控。并采用 IPSec VPN 等技术实现业务数据安全，实现整个工业系统的一体化安全防护。

当前 5G 应用已初具规模，中国移动 5G 专网建设逐渐趋于成熟，截至今年 7 月底，中国移动已建设超 50 万个 5G 基站，在这样的大背景下，虚拟专网更是具备了成熟的发展条件。而且网关部署操作便捷，不会对网络架构、人员技术能力有较严格的要求，因此项目可复制性和可推广性强，应用广泛，无论是大型企业异地分支互联需求还是中小型企业降本增效需求，都能一套满足。

5G+多租户虚拟专网安全解决方案应用后，客户只需了解一些简单的网络知识和安全知识，便可以通过集中可视化管理平台便可对整体的安全情况进行管理，降低了管理的技术门槛和安全工作量。

4.安全及可靠性

（1）智能高效的服务编排

本项目中利用虚拟专网网关产品独特的基于策略的流量牵引技术，为钦州港口实现业务流量的按需分类防护，如漏洞防护、攻击防护、病毒防护、数据加密

传输、终端准入认证、权限集中管控、威胁深度识别等，避免了各 VNF 对无关流量的重复检测，让 VNF 各司其职，提高了 VNF 的工作效率；同时提供有状态的服务链编排，提前预判 VNF 健康状态，智能选择服务链；根据用户业务安全需求，灵活组合不同安全能力的 VNF，真正实现按需编排，配置简单高效。

（2）全自动组建加密虚拟专用网保障通讯安全

多租户虚拟专网通过 SDN 技术及 SD-WAN 技术，实现了钦州港口与总部全自动组建加密虚拟专用网的能力，运营人员只需关心业务访问策略如何配置，由管控平台下发业务访问策略时，会自动基于业务访问策略实现自动组建基于该业务的虚拟专用网（VPN）。相比传统方案，采用 VPN 组网的过程对管理员不可见，管理员不需要具备专业的配置 VPN 的技能。实现在互联网上自动搭建安全隔离的虚拟专用网的同时，大大提高了安全网关上线、运维的工作效率，保障通讯安全。

另一方面，重要设施监测数据安全传输不仅实现了国际算法标准模式下的全自动安全加密组网，同时基于 SD-WAN 能力结合符合国家密码管理局要求，经商密检测中心核准的国密模式，实现了国密模式的全自动安全加密组网。

国密模式的全自动安全加密组网可以对接入的安全网关设备进行双向认证，基于 PKI 技术实现一体化证书申请、颁发、安装、更新。并通过 SD-WAN 的网络编排能力实现基于链路质量探测的智能选路。

（3）服务质量保障

多租户虚拟专网安全网关为本项目提供了 Internet、4G、5G、MPLS、MSTP 等多种广域出口的方式与其它安全网关互联，当其中一个广域网出口出现故障时，可以切换到其他正常的广域网出口，保证数据传送服务不受影响，为访问业务提供服务质量保障。

运用具备专利的应用识别技术，利用 DPI 深度包检测技术，智能识别 3000+应用，实现精准的业务感知。支持基于业务的重要性为业务定义优先级并指定保证带宽，在自动组网的过程中，可结合业务质量需求和带宽需求，按需实时调整业务优先等级并动态分配带宽，按需进行路径优选和流量调度。这样的方式，可在网络出现抖动时，最大限度的保障高优先级的业务的可靠性。

管控平台支持遥测（探针）技术，通过监测整个广域网的端到端服务质量，支持基于跳数、时延、带宽等多维度的智能选路，实现基于应用的路径优选和质

量保证。

（4）基于设备特征指纹的身份认证技术

多租户虚拟组网方案中采用设备特征指纹的身份认证技术，从设备物理层面降低了设备伪造风险，极大提升了设备接入的身份可信度。此外，结合口令认证、超级 SIM 卡等技术，实现终端可信接入，从源头上避免 DDOS 等安全风险。

5.其他亮点

（1）分权分域多级端到端组网编排

由于大部分重要基础设施多采用分级组网结构，因此在管理上也需要实现按照多级组网的行政区域划分管理权限，导致不同管理域间的网络编排独立不统一，容易出现因人工配置引入的故障点。本项目采用端到端编排理念，将 SD-WAN 的网络编排能力以端到端的方式连贯展现，让不同管理域间互联需求的组网编排不再各自独立，用户可以通过端到端方式实现组网编排，避免两侧管理域的管理员各自编排网络引起的配置不一致问题。

（2）项目实用性及可推广性

虚拟专网市场空间广阔，据权威机构预测 2021 年全球市场规模可达 80.5 亿美元。中国移动上海产业研究院充分利用中国移动 5G 的优势和能力，积极探索与研究 5G+多租户虚拟专网解决方案，满足智慧工业企业的数据本地化管控需求，并逐渐像交通和金融等垂直行业进军。该项目成功应用对 5G 机器视觉、5G AR 等工业应用场景有着非常重要的示范拉动效应。从安全角度而言，没有网络安全，就难有 5G 产业应用，项目提出了“可信接入、智能连接、安全守护”设计理念和应对思路措施，对后续加强各方互信合作，加速推动我国 5G 安全发展与提出了新的思路和方案。

2.9.3 下一步实施计划

1. 实施计划一

该方案计划商用以后，可按照两种模式提供服务，即公有云服务和私有云服务:

- 公有云服务：通过统一运营云管平台和控制器，在客户侧部署网关设备，提供组网服务，按部署硬件数计费;

- 私有云服务：本地化部署云管平台、控制器和网关设备，按部署套数与硬件数计费。

	公有云	私有云
云管平台+控制器	针对中小企业价格敏感特性，通过上研院统一运营云管平台和控制器，客户侧部署网关设备，提供组网服务，**按部署硬件数计费** 售卖形式：服务（费用均摊到网关内）	针对大中型企业数据敏感特性，本地化部署云管平台、控制器和网关设备，**按平台部署套数与硬件数计费** 售卖形式：资产
	移动云部署的平台及控制器提供给客户免费使用，相应资产归属于上研院，**每客户免费开通 1 个一级账户**	一次性收费模式(云管平台+控制器)，相应资产归属客户所有
网关（CPE、vCPE）	售卖形式：服务	
	以包年订购关系为依据按年、按节点收费模式，设备作为上研院资产以服务方式提供。	

推广方式：和中国移动省公司通过框架协议进行合作推广，签署框架协议后直接走 ESOP 订购流程进行推广；产品形成标准化优势后，可逐步实现甩单式销售模式。

除钦州港外，正在向整个北部湾港口企业推广，成功落地防城港等其他港口，且以智慧港口行业为圆点，逐渐扩散到其他省市的工业领域、政府类企业领域，目前虚拟专网已在广西、河南、重庆、江苏等 4 个省市实现落地商用，项目收益上千万，且不断有新的商机涌现。

2.实施计划二

优化安全产品：该产品研发团队会关注最新的攻击手段和漏洞利用方式，不断更新攻防能力，确保产品自身安全，为用户提供安全防护能力的基础必须建立在自身安全完备可靠的基础上，方可真正实现对于上层业务数据的安全保障。

3.实施计划三

该方案的安全架构模式可以同步推广到整个工业互联网领域，其中的无关路由服务链能力，可以复用到其他工业互联网场景，如钢材制造等领域，推动工业互联网的整体安全提升。

2.9.4 方案创新点和实施效果

1.方案先进性及创新点

1）业内首次编制统一接口规范，支持第三方系统接入，实现多厂商控制器统一纳管;

2）采用 IPSec VPN 自动组网技术，基于 5GC 组建加密传输网络，加解密算法不仅支持国际主流的 3DES、AES 算法，同时还支持由国家自主设计的国密算法 SM1/2/3/4。防止通讯过程中出现数据泄漏及数据篡改问题，对于高清视频等港口重要业务数据，采用单独隧道与普通业务数据进行隔离，杜绝越权行为及非授权访问行为;

3）安全栈采用无关路由服务链技术，基于策略的流量牵引，对业务流量分类检测防护，避免了对无关流量的重复检测，同时可提前预判 VNF 健康状态，智能选择服务链;

4)云管平台支持 DPI 深度包检测技术及遥测（探针）技术，智能识别 3000+工业协议及工业应用，实现精准的业务感知，通过监测端到端服务质量，支持基于丢包、抖动、时延、带宽等多维度的智能选路;

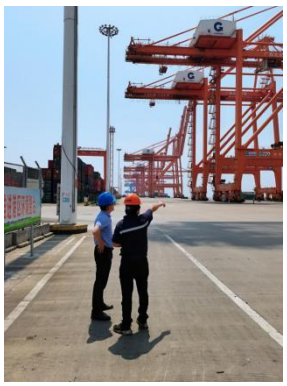
2.实施效果

（1）业务效果实现:

- 实现 5G 轮胎吊 17 路高清视频的实时回传和远程实时控制
- 实现对港口和数据中心的集中管控
- 对港口港机远控无线业务进行关键流程分析和业务场景摸查
- 对各类应用端到端时延和流程提供资源保障
- 协同网络进行资源编排和动态调整

（2）安全功能实现:

- 通过虚拟化安全能力和加密隧道能力，保障数据上云传输过程中的安全性
- 支撑港口业务监测和预警，监测港机工作状态\性能，及时报警，防范风险，
- 通过 5G 高清视频回传，数据实时采集分析预警提升作业效率及安全可靠性，降低事故发生率

（3）项目获奖情况：

- 2021 年，该项目荣获工信部第四届“绽放杯”应用安全专题赛典型案例奖

第四届“绽放杯”5G应用征集大赛应用安全专题赛

荣誉证书

获奖项目：5G+多租户虚拟专网安全解决方案

获奖等级：典型案例

牵头单位：中移（上海）信息通信科技有限公司

联合单位：网神信息技术（北京）股份有限公司、中国移动通信集团有限公司信息安全管理与运行中心、广西北港大数据科技有限公司、中国移动通信集团广西有限公司钦州分公司

“绽放杯”5G应用征集大赛组委会

二〇二一年十月

证书号：2021-29-5

- 2023 年，该项目荣获第二届“光华杯”千兆光网应用创新大赛三等奖


“光华杯”
千兆光网应用创新大赛

第二届“光华杯”千兆光网应用创新大赛

荣誉证书

获奖项目：基于千兆光网+安全组网的北部湾智慧港口建设项目

获奖等级：全国三等奖

获奖单位：中国移动通信集团广西有限公司防城港分公司
中移（上海）信息通信科技有限公司、北部湾港防城港码头有限公司
中国移动通信集团有限公司信息安全管理与运行中心
工业互联网创新中心（上海）有限公司、杭州大拇指信息技术有限公司

主要完成人：黄鹏程、熊诚锋、李伟渊、唐双林、张峰、王轩轩、
陈志豪、秦峰、郝锦瑄、杨成

“光华杯”千兆光网应用创新大赛组委会
二零二三年七月
证书号：2023-ZHGK-3423

2.9.5 单位基本信息

中移（上海）信息通信科技有限公司（对内称“中国移动(上海)产业研究院”）是中国移动通信集团有限公司出资 20 亿组建的全资子公司，位于浦东新区金桥开发区，是中国移动面向 5G 和人工智能，引领工业能源、交通和金融等领域数字化服务的专业研发机构。目前中国(上海)信息通信科技有限公司现已获得“国家高新技术企业”、“国家测绘甲级资质”、“上海市重点企业”、“浦东新区企业研发机构”资质认证，发表专利 500 多篇，其中已授权 150 多篇，授权软著 130 多项，参与标准建设 10 余项。中国移动上海产业研究院主要研发方向分为三个领域：在智慧交通领域，将发挥上海国际航运中心区位和产业优势，积极支撑集团布局智慧交通新生态，研究 5G、北斗高精度定位、自动驾驶、大数据和人工智能、物联网、云计算、边缘计算等技术在交通行业的应用产品和解决方案。在工业互联网及能源领域，围绕工业设计、生产和服务环节及能源采集、生产、传输、使用等环节，打造面向工业互联网及智慧能源的有竞争力的产品和解决方案。在金融科技领域，打造智慧无人网点、3D 云渲染平台、金融风控、供应链金融、无感支付等行业金融应用场景。

2.10 案例九：“工业互联网+安全风险智能化管控”智慧化工园区解决方案——基于工业互联网平台的业务优化和模式创新

十四五期间化工行业是一个 “由大到强”的转换过程，化工园区已成为化工产业高质量发展的重要载体，国家陆续发布了多项针对化工园区建设的“指南”，这些标准规范有效的规范和指导了化工园区的建设方向。2019 年开始国家开始整治化工领域的重大风险，2021 年六部委印发《化工园区建设标准和认定管理办法（试行）》，指导园区深化发展，对化工园区安全和环境监测管理、封闭化管理、应急管理等提出了更高要求。为满足化工园区高质量发展，卡奥斯化智物联聚焦“工业互联网+安全风险智能化管控”，以“工业互联网+园区管理”为理念，结合“云计算、人工智能、大数据、物联网、移动互联网”等新技术，基于统一平台，建设一个覆盖园区安全、环保、能源、应急救援、封闭化、公共服务和保障体系等领域，一体化集成的信息管理平台，实现安全风险精准识别，监管手段真实有效，数据服务及时可靠，平台功能落地实用，将智慧园区安全管控平台建设落到实处。

2.10.1 方案概述

基于工业互联网平台，为化工园区量身定制“工业互联网+安全风险智能化管控”智慧化工园区整体解决方案，打造智慧化工园区管理平台，根据政策要求结合业务工作开展实际需要，全面提升化工园区信息化智慧化管理水平。服务化工产业和高耗能行业高质量发展需求，进一步提高工作质量和效率。建设对园区内化工企业产业管控，引导和支持企业建立安全、环保、应急等相关模块的智慧化工园区管理平台。加强化工生产企业过程控制与数据共享，对重点监管的危险化学品、危险化工工艺以及重大危险源，实施自动化监控，为化工园区和园区内企业数字化赋能，打造一个安全、便捷、高效、节能、智能的数智化工产业园区。

1. 方案背景

多级政策为导向建设智慧化工园区管理平台满足安全监管要求，

1）国家加大力度引导化工园区智慧化发展：十四五期间，中国由化工大国向化工强国转变，化工产业发展由大到强，化工园区成为行业发展重要载体，国家大力引导化工项目退城入园，并陆续出台政策推动智慧化工园区建设。

2）政府不断出台新政策，智慧园区建设标准不断提升：近年来《智慧化工园区建设指南》、《化工园区建设标准和认定管理办法（试行）》、《化工园区安全风险智能化管控平台建设指南》等政策指南的颁布，对化工园区安全及智慧化建设提出了更高的要求和标准。

3）工业互联网赋能化工园区高质量发展：中央全面深化改革委员会第十四次会议审议通过了《关于深化新一代信息技术与制造业融合发展的指导意见》，会议强调，加快推进新一代信息技术和制造业融合发展，加快工业互联网创新发展，加快制造业生产方式和企业形态根本性变革。要求充分利用工业互联网等新一代信息技术提高重点行业安全风险智能化管控水平。

基于此结合园区安全风险智能化管控实际需要，建设涵盖安全、环保、应急等相关模块的智慧化工园区信息管理平台，对园区内化工企业安全生产管控，加强化工生产企业过程控制与数据共享，对重点监管的危险化学品、危险化工工艺以及重大危险源，实施自动化监控。

2. 方案简介

以云计算、物联网、大数据分析、移动应用等新一代信息技术为支撑，基于卡奥斯工业互联网平台，以“工业互联网平台+安全风险智能化管控”为升级方向，通过“园区 OS+工业 APP”模式为化工园区打造新一代智慧化工园区管理平台，聚焦运营、安全、环保、应急、能源、封闭化管理、办公、循环产业等 9 大场景，整合园区多种业务场景于一体化管理平台。通过将园区、园区内企业各类数据的全面集成和数字协同联动，解决园区安全风险防控能力较低、园区安全管理和服务效能和水平较低、数据量大利用率低等核心痛点问题。数智结合驱动园区管理方式创新，以“安全一张图”的管理形式实现园区“全感知”、“全连接”、“全场景”，全面升级园区安全管理体系，形成可视化、立体化、敏捷化的安全管理体系，提升安全园区运营、监管效能。通过工业互联网平台实现“监管+服务”双向推进，创新“园企共建”模式，聚焦人、机、物、环、管，针对企业端、园区监管端进行双端建设，多维度、全要素打造一个多层的智慧安全化

工园区体系，实现对园区企业基本情况、装置开停车、园区风险分区、重大危险源、风险隐患、特殊作业、人/车/物流、公共区域异常情况、应急救援等多形式、多模式、多维度的可视化监测预警、统计分析和智能化管控调度，实现园区企业安全生产数据化、流程化的动态监管，全面提升园区企业安全风险智能化管控管理水平。

多模块：搭建基于工业互联网的安全、环保、应急、封闭化、能源、公共服务和循环产业等一体化智慧园区运营平台。

安全智能化：基于云计算、物联网、大数据、AI 场景化等新一代信息技术全方面降低人力监管投入，提高园区安全智能化水平。

可靠高效：围绕“人机环物”四方面要素，实现安全风险动态感知、事故隐患即时告警，实现安全风险的智能监管全覆盖；通过大数据分析和云计算准确识别安全隐患并及时采取对应的减害措施，实现安全生产的业务全过程闭环式安全管理。

3. 方案目标

1）基于国家对建设化工智慧园区各项方案、指南的要求和目标，结合园区实际业务情况，以有效防范化解重大安全风险为目标，打造实现化工园区企业安全生产全要素数字化管理的智慧安全化工园区管理平台，实现化工园区内重点监管的危险化工工艺，重点监管的危险化学品、重大危险源、重点装置、重点设备和重点场所等基础信息的统一管理，并可在电子地图上显示上述信息;对视频监控区域内重点监管对象的运行状态、环境状况及人员安全行为进行识别、监测和报警;对基础信息、监测信息和报警信息等进行多维度数据统计与分析，通过图表方式展开统计分析结果。

2）基于智慧化工园区管理平台，将监管方式变被动为主动，实现对园区内安全基础、重大危险源安全、双重预防机制、特殊作业、封闭化、应急等一体化管理，全面提升园区对重大危险源的智能感知、动态监控能力及效率，全盘掌控园区安全态势，为园区各级管理部门提供信息的实时数据采集、事故的科学分析、资源的高效调动等各类数据服务，实现园区“全感知”、“全连接”、“全场景”，形成可视化、立体化、敏捷化的管理体系，全面提升园区安全监管效能。

2.10.2 方案实施概况

聚焦人、机、物、环、管，针对企业端、园区监管端进行双端建设，多维度、全要素打造一个多层的智慧安全化工园区体系，实现对园区企业基本情况、装置开停车、园区风险分区、重大危险源、风险隐患、特殊作业、人/车/物流、公共区域异常情况、应急救援等多形式、多模式、多维度的可视化监测预警、统计分析和智能化管控调度，实现园区企业安全生产数据化、流程化的动态监管，全面提升园区企业安全生产管理水平。

1. 方案总体架构和主要内容

（1）平台总体架构

搭建基于工业互联网的安全、环保、应急、封闭化、能源、公共服务和产业分析等一体化智慧园区运营平台。基于“园区 OS+工业 APP”的模式，聚焦安全、环保、应急、能源、循环等 9 大场景，全面整合园区信息资源与技术平台，布局园区综合一张图、安全生产一张图、环境管理一张图、应急管理一张图、经济能源一张图，将安全、环保、应急救援、能效分析、封闭管理、物流跟踪、公共服务、产业链分析等多种业务集成于单一平台，全面整合园区信息资源与技术平台，将大数据与 GIS、物联网等技术融合，通过数据可视化方式管控全局、实时监测，实现园区智慧化管理与高效运营。创新“园企共建”模式，以轻量化 SaaS 产品赋能园区内企业，实现园区和企业数字化转型升级。

1）园区 OS-通用 PaaS 层

基础层是将计算资源、存储资源、网络资源等物理资源进行整合，按照云服务模式和云架构建立共享资源池，形成可按需动态扩展的高性能计算环境、大容量存储环境。本项目建设基于政务云平台基础设施的建设，充分利用现有基础，根据需要补充前置机、防火墙等必要设备，满足海量数据存储、信息共享查询需要。

2）园区 OS-BaaS 层

BaaS 层包含化工行业产业体系的工艺技术、运营管理、行业知识与模型等可重复使用的数字化基本单元，具有独立性、通用性和可移植性。还包括知识组件、工具组件和应用组件等组件类型，知识组件是指数据集、知识图谱、规则模型等可用于深度挖掘开发的数据知识资源，工具组件是指图深度学习推理、领域

知识规则推理、统计推理引擎等认知计算工具资源，应用组件是指应用中间件、标准化产品如工业 APP、系统集成解决方案等数字化服务资源。

3）应用层

应用层是以友好的界面为客户提供所需业务所需的各项应用软件和服务。应用层直接面向客户需求，向园区和企业客户提供安全、环保、应急等场景下的应用。工业 APP 是一个低内聚松耦合的应用，旨在解决具体的业务场景问题，通过工业 APP 的组装和组合，能够快速高效的解决园区和企业监管、服务的问题。

4）标准规范体系

标准和制度保障体系包括数据和应用服务方面和技术标准规范及管理制度，确保智慧化工园区综合监管平台各组成部分之间，以及平台与外部系统交互能够有效衔接，规范运转。

5）统一运维体系

统一运维体系包括数据、应用服务与硬件方面的统一运维，实现运维管理工作的规范化、体系化。

6）安全保障体系

安全保障体系包括安全管理制度、安全基础设施、网络安全、主机安全、应用安全、数据安全等内容，保障数据存储、传输、访问、共享的安全。

图 9-1 智慧化工园区管理平台功能结构

（2）主要内容

智慧化工园区管理平台采用了先进的智能设备与管理系统，通过智能化手段主动感知、整合各类安全生产监督管理要求和信息资源，建立安全生产监督管理

系统，实现日常安全生产管理、事故防范以及事故发生时应急救援指挥于一体的动态综合安全监管功能，从而以更加全面、精细、动态和科学的方式提供安全管理服务，园区的智能化建设也推着企业的自动化改造升级。

平台采用重大危险源监测预警、安全风险分区、人员在岗在位、企业全流程等模块，促使企业在安全生产管理过程中实现智能化，便于企业的日常管理，在风险出现之前，平台已有预警功能，可以降低人员的伤亡概率，使企业职工在工作过程中安全感比以往更强。

人员在岗在位功能，使企业对于人员的工作状态以及活动轨迹更有把控性，尤其是在应急救援过程中，人员在位在岗模块的使用起到了决定性作用，从而避免了出现事故后不知人员位置，使受困人员在第一时间得到救治，避免了盲目救援的情况。

重大危险源监测预警模块的使用，在重大危险源场所设置了监测设备，监测设备集中在园区工业互联网平台上，数据实时传送，出现预警信息，自动第一时间推送平台，使值班人员第一时间掌握发生预警信息的资料，及时通知现场人员巡检或撤离，避免事故的发生。

企业生产全流程模块的使用，从人员、物料、设备、培训、应急等方面制定了详细的规划，在使用过程中，更有针对性、逻辑性，便于企业在生产经营中做好统计分析等工作。

企业的数据与园区工业互联网平台对接后，园区可以用大数据进行分析，极大提升园区安全、环保管理水平，并对园区各企业智慧化发展起到很好的指导作用。

此外，平台基于卡奥斯工业互联网平台，打造“园区 OS+工业 APP”新模式，园企共建，为企业提供低成本、轻量化的 SaaS 产品，并能为园区提供产业发展分析，产业知识图谱+产业大数据支撑园区产业优化升级。

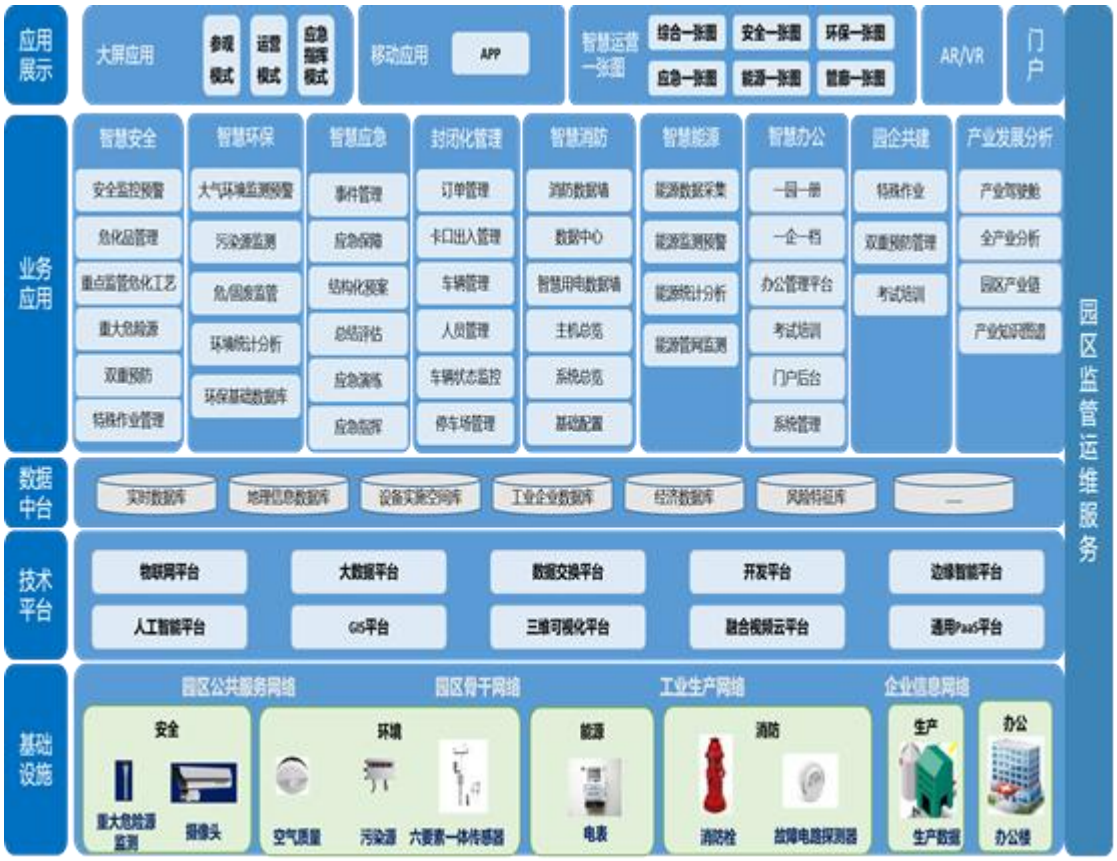


图 9-2 园区监管运维服务

2. 网络、平台或安全互联架构

（1）安全架构

依据国家信息安全战略的方针政策、法律法规、制度，按照行业标准规范要求，结合园区自身的安全环境，制定完善的信息安全策略体系。信息安全策略体系覆盖信息安全工作的各个方面，对管理、技术、运维体系中的各种安全控制措施和机制的部署提出目标和原则。

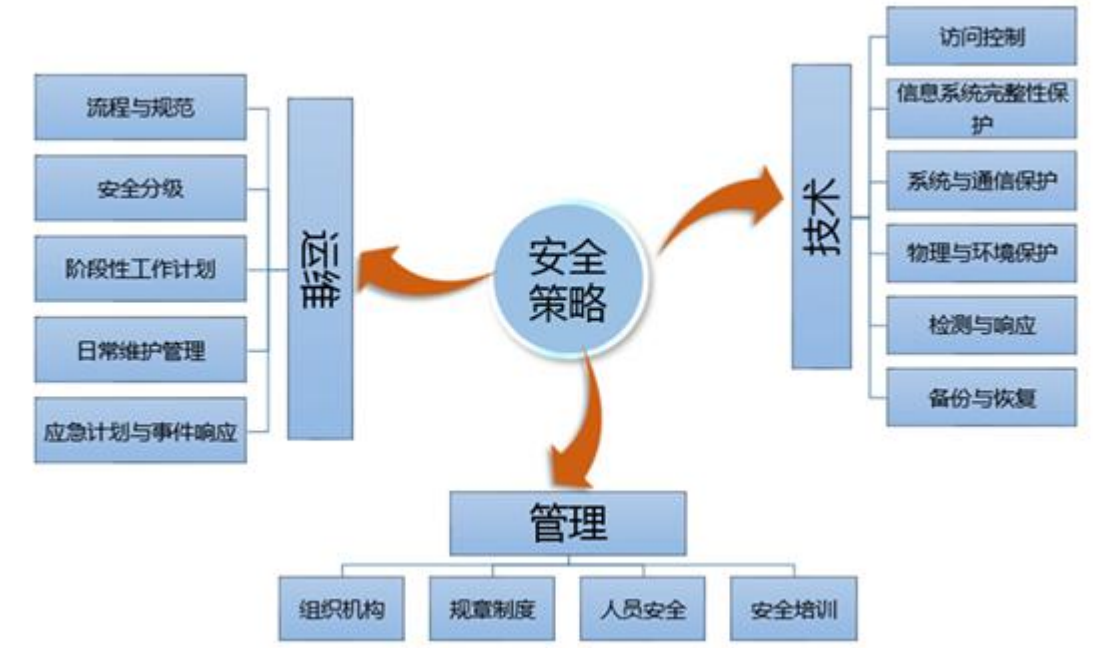


图 9-3 安全架构图

在管理方面，按照相关文件的有关要求，将“安全策略”提出的目标和原则形成具体的、可操作的信息安全管理制度，组建信息安全组织机构，加强对人员安全的管理，提高全行业的信息安全意识和人员的安全防护能力，形成一支过硬的信息安全人才队伍。

在技术方面，按照 P2DR2 模型——Policy（安全策略）、Protection（防护）、Detection（检测）、Response（响应）和 Recovery（恢复），通过对网络与边界安全、主机与终端安全、审计、应用安全、数据备份与恢复及物理安全的规划建设，全面提升信息安全防护、检测、响应和恢复能力，保证信息系统保密性、完整性和可用性等安全目标的实现。

身份认证与访问控制：引入强密码策略，要求用户设置复杂密码，并定期更新。使用双因素身份认证，例如结合密码和生物特征识别。实施访问控制策略，根据用户角色和权限设置不同的访问级别。

网络安全：建立网络防火墙，限制入站和出站流量，防止未经授权的访问。使用加密通信协议，如 SSL/TLS，保护数据在传输过程中的安全。定期更新和维护网络设备的安全补丁，以防止已知漏洞的利用。

数据安全：实施数据备份和灾难恢复计划，确保数据的完整性和可用性。使用数据加密技术，对敏感数据进行加密存储，以防止数据泄露。制定数据访问和

共享策略，限制对敏感数据的访问权限。

应用安全：对平台进行安全审计和漏洞扫描，及时发现和修复潜在的安全风险。引入安全开发生命周期（SDLC），确保在开发过程中考虑安全性。实施应用程序防火墙（WAF），监控和过滤恶意请求和攻击。

物理安全：控制物理访问权限，通过门禁系统和视频监控等手段，限制未经授权的人员进入关键区域。定期进行安全巡检，确保设备和设施的安全状态。建立紧急响应计划，以应对突发事件和安全漏洞。

日志和监控：实施日志管理和事件响应系统，及时监控和检测安全事件。建立安全信息与事件管理（SIEM）系统，集中管理和分析安全日志和事件。实施实时监控和报警机制，对异常活动进行及时响应和处理。

安全性能：部署防火墙和入侵检测系统（IDS/IPS），监控和阻止潜在的攻击行为。实施安全审计和漏洞扫描，及时发现和修复安全漏洞。建立安全事件响应机制，对异常事件进行及时响应和处理。

在运维方面，制定和完善各种流程规范，制定阶段性工作计划，开展信息安全风险评估，规范产品与服务采购流程，同时坚持做好日常维护管理、应急计划和事件响应等方面的工作，以保证安全管理措施和安全技术措施的有效执行。

（2）网络架构

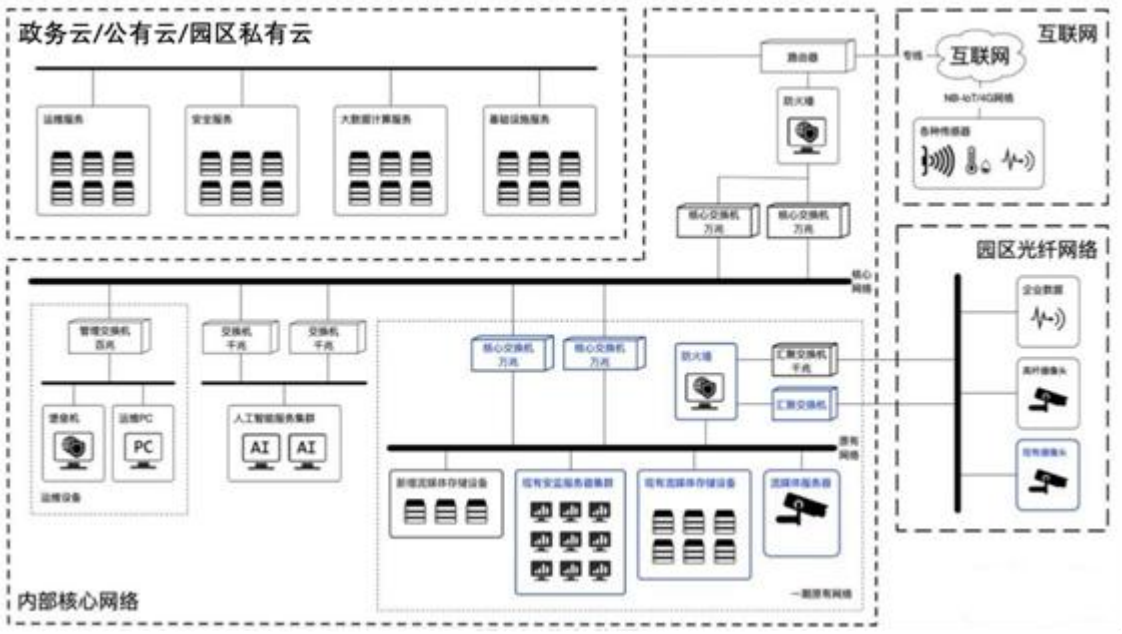


图 9-4 智慧园区系统网络架构图

3.具体应用场景和安全应用模式

（1）安全、应急、封闭化管理模块是智慧化工园区管理平台的重要组成部分

智慧安全模块围绕“人机环物”四方面要素，实现安全风险动态感知、事故隐患即时告警，实现安全生产的智能监管全覆盖；通过大数据分析和云计算准确识别安全隐患并及时采取对应的减害措施，实现安全生产的业务全过程闭环式安全管理。

智慧应急模块针对公共安全事件的事前预防、事发应对、事中处置和善后管理过程，构建横向互联纵向贯通的应急体系；实现信息采集网格化、预案管理数字化、预测预警智能化、联动指挥精准化、多方会议视频化。

封闭化管理模块对化工园区关键卡口、企业厂区周界、人员轨迹、建筑物的关键区域（危化品存储、重要设施等）进行全方位管控，实现全态感知、全域监控。端到端识别。在第一时间、第一现场发现问题、解决问题。

通过安全、应急、封闭化等管理模块的应用，园区安全应急处置能力提升，安全应急事故管理从事后报警单方处理转变为事前预警、多方协同，安全风险管控能力提升 50%，应急指挥效率提升 50%，安全巡检效率提升 45%，人工投入较原先降低 45%。

（2）运用智能化手段打造一体化安全、智能监管的化工园区

基于智慧化工园区管理平台，将监管方式变被动为主动，实现对园区内安全基础、重大危险源安全、双重预防机制、特殊作业、封闭化、应急等一体化管理，全面提升园区对重大危险源的智能感知、动态监控能力及效率，全盘掌控园区安全态势，为园区各级管理部门提供信息的实时数据采集、事故的科学分析、资源的高效调动等各类数据服务，实现园区“全感知”、“全连接”、“全场景”，形成可视化、立体化、敏捷化的管理体系，全面提升园区安全监管效能。

建设重大危险源监测预警，实现重大危险源实时监控、报警处置的闭环管理。借助平台的物联能力，实现对园区内重大危险源可燃/有毒有害气体，重大危险源液位、浓度、压力、温度等实时数据 7*24 小时的在线监测。建立重大危险源分级预警方案和分级预警指标设计各种动态分析模型，套用模型进行计算，判断

危险源状态、判断是否需要报警及报警级别行，在危险源报警后也要循环反复计算危险源状态，判断是否状态升级。

（3）采用“一张图”的形式，将园区内安全生产、应急救援、封闭化等信息纳入可视化平台管理

- **“安全一张图”**

依据园区安全业务需求，通过数据分析模型实现园区安全监管和园区基础两个专题的展示。安全监管主要包括企业风险承诺公告、两重点一重大、物联监测、双重预防、特殊作业及报警预警的展示和统计分析。基于GIS地图采用分图层的方式对园区边界、园区安全控制线、企业风险区域、重大危险源、特殊作业、隐患、视频等直接映射在地图上，实现相关安全业务数据与地理信息融合，方便快捷的查看安全的业务数据。也可通过GIS地图上的企业点位查看企业安全基本信息或进入企业安全一张图，对企业安全业务数据进行更多查看。园区基础主要包括园区的十有两禁、企业分布、第三方单位、执法、安全生产许可等信息，实现对相关安全基础数据进行统计展示。

主要功能包括:

1）展示园区内企业、危化企业数、安全重点监管企业的统计信息;

2）展示企业每日风险承诺公告统计信息及各企业承诺信息;

3）展示园区重大危险源、重点监管化工工艺、重点监管危险化学品等信息，并对重大危险源监测信息、产生的隐患、隐患处理率、装置开停车备案情况等进行统计展示。

4）通过物联监测展示园区内的在线监测情况及报警信息、报警趋势、报警处理情况、关键参数预警指标分析信息。

5）展示园区内的双重预防风险分级管控及隐患排查统计信息，对企业双重预防运行效果进行展示。

6）展示园区内不同类型的特殊作业统计信息;

7）展示园区内安全相关的报警统计信息;

8）展示园区内安全相关的视频监控统计信息;

9）基于GIS地图采用分图层的方式对园区边界、园区安全控制线、视频、重大危险源、特殊作业、企业风险区域等等直接映射在地图上，并可点击查看相

应的业务数据信息。点击企业点位，若想了解更多的安全相关信息，可进入企业安全一张图进行查看；

10）展示园区的十有两禁、规划档案、安全管理体系信息；

11）展示园区内第三方单位统计信息；

12）展示园区内企业的执法统计信息；

13）展示园区内企业的安全生产许可统计信息；

图 9-5 “安全一张图”

- **“应急一张图”**

依据园区应急指挥调度日常工作和应急响应工作业务需求，建设包含日常模式和应急模式的应急一张图。在日常模式中，实现园区应急救援力量、应急预案、应急事故的综合分析和展示。在应急模式中，实现园区应急救援力量、应急事件的展示，通过应急事件列表和应急指挥按钮，快速启动应急响应，实现应急调度的综合管控。基于 GIS 地图，将园区应急资源、保护对象、避难场所、危险源、事故点位、消防设备和视频监控的位置直观的展示在地图上，通过点击对应的点位信息可以查看相应的详细情况，实现对园区的应急日常值守情况进行全方位管控。

主要功能包括：

1）园区应急救援力量展示，包括应急队伍、应急人员、应急专家、应急车辆的台账综合展示；

2）园区预案演练统计分析，包括园区预案类型分布、应急演练统计分析;

3）园区事故分析统计;

4）通过应急事件列表和应急指挥按钮，快速启动应急响应，实现应急调度的综合管控;

5）基于GIS地图，将园区应急资源、保护对象、避难场所、危险源、事故点位、消防设备和视频监控的位置直观的展示在地图上，通过点击对应的点位信息可以查看相应的详细情况，实现对园区的应急日常值守情况进行全方位管控。

图 9-6“应急一张图”

- **“封闭化管理一张图”**

封闭化一张图综合分析展示车辆和人员的实时存在情况、出入量、卡口吞吐量、报警信息等封闭化管控态势信息。结合GIS地图动态监测定位出入化工园区的人员、车辆，实现化工园区人流、车流和物流出入管控，确保区域安全风险有效隔离，切实防范外来输入风险。

图 9-7 “封闭化一张图”

4. 安全及可靠性

平台已实现对园区内的企业、重大危险源、不同种类危化品、储罐、安全风险点的实时在线监测，自动感知生产设施运行状态，自动辨识操作工人作业行为，自动监测生产物料属性变化。封闭化管理系统布置监控视频，其中包括高空瞭望、交通管控、危废倾倒，实现对园区全方位动态监控及车辆运行全过程轨迹还原。有毒有害气体环境风险预警体系，布置有毒有害气体检测、废水废气监测设备，实现对重点企业及园区环境指标各项临界值的监测。系统实现对园区内企业风险分析对象、风险事件在线管控，完善了重大危险源全要素生产数据实时在线监测和智能监控，建成了涵盖一线生产人员的人员定位系统，夯实危化品企业生产储运全流程安全监管基础数据的统计运用。

5. 其他亮点

（1）工业互联网+新技术

充分依托于云计算、互联网、物联网、大数据分析、移动应用等最新的 IT 前沿技术和设计理念，聚焦园区数据量大、利用率低、安环监管难、产业规划弱、信息孤立等痛点，全面整合园区业务数据，基于 GIS+大数据分析，多维数据融合，对平台既有海量数据进行全方位、多维度处理，围绕安全、环保、应急、能源、产业链等场景建设具有工业互联网特性的智慧化工园区解决方案。

依托卡奥斯工业互联网平台，建设云计算、物联网、工业大数据、工业机理模型、应用开发和微服务组件等一系列前沿技术能力，同时将化工行业知识、工艺、机理、算法等最佳实践沉淀为 BaaS 引擎，构建专业的化工园区操作系统。

（2）创新“园区 OS+工业 APP”模式

“园区 OS+工业 APP”模式打造的智慧化工园区管理平台。在平台之上建设智慧运营、智慧安全、智慧环保、智慧能源、智慧应急、封闭化管理、智慧服务、产业分析等 9 大应用场景，借助园区 OS 底层基座能力部署运行工业 APP，依托平台上优质的工业 App，同时满足政府部门对于企业的监管需求，融入企业自身管理需求，提升化工园区安全、环保、应急、监管、处置等能力水平和效率。

1）园区 OS：作为建设智慧化工园区的平台底座，园区 OS 具备强大的底座能力，为应用场景的优化和创新提供了通用开放的开发环境，又具有丰富的生态兼容性。园区 OS 包括容器管理、开发运维一体化、设备物联、工业大数据、工业机理模型、数字孪生体、知识图谱、工业智能等能力，向上能够支撑业务应用，向下能对资源进行调度和管理，为园区及企业赋能。

2）工业 APP：借助园区 OS 的通用开发环境，结合园区和园区内企业实际应用场景，快速响应开发适应不同场景的工业 APP，为园区和企业提供 SaaS 服务。部署在园区 OS 上的工业 APP 可自由组件，增强了平台的柔性，为园区和企业提供海量选择，实现灵活组装和快速部署，满足不同园区个性化应用的需求，低成本满足园区内企业数字化转型需求。

（3）打造数据管理中心

基于“园区 OS+工业 APP”模式建设智慧化工园区管理平台，打造智慧园区的大数据管理中心，建立数据交换共享、更新维护等标准规范与机制，实现各部门数据的统一接入、统一存储、统一管理、统一共享，打破各部门间的数据孤岛与信息壁垒，确保数据的安全、真实、有效，为业务的管理提供数据支撑。

（4）创新“园企共建”模式

平台创建“园企共建”新模式，聚焦园区和企业共性需求，实现园区、企业协同联动，促进园区、企业协同发展。园企共用平台资源，同时为园区和园区内企业提供全方位的云服务，为企业提供 SaaS 化软件服务，节约企业软件建设成本，提升企业智能化水平，打通园区、企业数据孤岛，数据实时共享，降低企业

数据上报成本，提升园区监管实时性和效率，使园区和企业之间的联接更加紧密，创建服务型园区真正实现园区及企业人、事、物统一管理。

（5）产业布局高质量发展，招商引资精准力度提升

平台通过建设园区产业发展分析、产业知识图谱等模块，分析园区产业结构合理性、园区企业产业链接紧密性、产业创新性等指标分析，实现对化工园区产业发展规划、产业链优化，帮助园区精准招商提升园区入园率，高价值，高产值，强耦合发展。

（6）底层数据集成加速，协同管理效率大幅度提升

园区工业互联网平台的建设使底层数据集成能力加速，园区通过云边端一体化管理平台实现数据统筹与管理，横向集成园区内部不同系统，纵向实现上级政府-园区-企业三级贯通，对接上级山东省智慧化工综合管理平台和下级企业，大幅度提升协同管理效率。

（7）建设“低碳”园区，打造园区绿色产业链

平台围绕能源管控、环境管控等领域实现园区能源的精细化管理，全面准确掌握环境质量变化趋势、污染源状况、环境风险等，支撑绿色园区发展建设，加大“低碳”园区建设力度，助力打造园区绿色产业链。

2.10.3 下一步实施计划

1.完善提升智慧园区大数据应用工作

汇聚园区现有安全生产、环境保护、应急管理、能源利用、封闭管理、物流运输等各业务系统的相关数据，根据园区决策需要，将实时监测数据、静态数据、业务数据、研判分析数据等集中展示，利用大数据技术进行建模综合计算，辅助园区进行科学决策。构建园区和企业安全生产指数预警模型，结合企业安全标准化情况、两重点一重大情况、风险隐患信息、物联网动态监测数据、执法检查相关数据等实际要素，动态监测园区内安全生产态势。根据园区基础设施、企业效益、园区产能、环保、产业链、物联网动态监测数据等相关因素研发园区发展指数，衡量园区和企业的综合质量。

2. 完善园区工业互联网平台

基于卡奥斯工业互联网平台，打造园区 OS，为园区和企业提供工业互联网软件与应用订阅、安装、运行与上架销售等服务的增值分享生态平台。通过园区工业互联网平台，园区和企业可以快速高效的浏览、获取、使用工业软件，丰富的工业软件帮助企业达到、降低生产成本、优化排产效率、稳定安全生产的效果。另外通过园区工业互联网平台提供的强大的组件，第三方服务企业和园区内有相应研发能力的企业可以基于平台开发相应的应用软件，更好的服务园区和企业的管理。

3.持续推进智慧安全园区建设工作

智慧安全化工园区内涵丰富，不是简单的软硬件堆积，不可能一步到位，下一步还要深入思考智慧安全化工园区的核心内容，重点考虑系统的协同集成、信息的交互共享、资源的优化配置以及智慧化工园区的经济效益和社会效益。智慧园区建设需要聚焦安全生产、环保保护和封闭化管理等功能板块，同时融入智慧消防功能板块，提高各功能板块实际利用能力，做到各子平台既能参与到日常管理，提高精细化管理水平，又能在应急状态下发挥指挥调度作用。

2.10.4 方案创新点和实施效果

1. 方案先进性及创新点

（1）工业互联网+安全风险智能化管控，实现园区安全全面管控及智能预警

充分依托于云计算、互联网、物联网、大数据分析、移动应用等最新的 IT 前沿技术和设计理念，聚焦园区数据量大、利用率低、安环监管难痛点，全面整合园区业务数据，基于 GIS+大数据分析，多维数据融合，对平台既有海量数据进行全方位、多维度处理，围绕安全、环保、应急、能源、产业链等场景建设具有工业互联网特性的智慧化工园区解决方案。项目的建成实现了对园区安全的全面管控，完成了从“看不见不可控”到“可视化可预警”的转变。

通过对园区企业危险源数据库的建立，实现了对两重点一重大数据的实时在线监测，有效地协助安全监管人员全面掌控重大危险源实时状态，及时发现并处理异常，将安全隐患扼杀在萌芽阶段，将重大危险源的危险性大大降低。通过对园区企业重点区域视频库的建立，实现了对企业生产作业情况的监管以及异常情况的智能分析做到了实时监测预警，实现了园区安监业务信息化和平台监管智能

化，强化了日常监管，增强了风险防控手段，减少了人力成本投入，提高了监管的连续性和准确性，及时、准确预防安全隐患，提升园区整体安全管控能力。降低了监控研判的时间，提高了救援效率，提升了园区整体安全系数，有效的支撑了化工园区的安全管理、控制工作，化工园区整体管理能力得到有效提升。

（2）多源汇聚，一图尽显安全信息

基于GIS+大数据分析，多维数据融合，将平台既有海量业务数据，建设安全一张图、应急一张图、封闭化管理一张图等。通过统计图表、分布图、关系图、空间统计图、空间分布图、空间关系图等数据可视分析图表，进行海陆空、全方位、多维度分析研判，为政府、园区和企业管理者决策提供全面的、科学的、准确的数据支持。

三维+GIS全景数字化重构化工园区及周边主要的化工企业采用与实景1:1的建模。正确还原道路、建筑、装置、罐、管廊的外形、材质和特征。前端采用WebGL技术结合工业三维引擎，无需在浏览器安装任何插件即可运行程序。大场景全尺度还原、大范围时空态势显示，还原真实场景的视觉体验。

（3）特殊作业全方位掌控，双重预防管理

1）特殊作业情况全方位掌控

实现园区当日作业情况、历史作业票量、预警和报警次数、作业类型等的多维度统计分析与查询功能，支持园区内特殊作业按不同企业、不同时间、不同作业类型等多维度进行统计分析，以及特殊作业信息在园区电子地图上实时显示和快速查询。

2）特殊作业流程可配置

按照法律法规、国家和地方标准规范，结合园区内不同企业的实际业务管理进行安全风险分析、管控措施确认、作业许可审批业务流程的配置，各级各岗位人员按管理要求填报相关信息，并履行审批流程，以满足企业的业务需求。

3）特殊作业全流程监管

实现园区当日作业情况、历史作业票量、预警和报警次数、作业类型等的多维度统计分析与查询功能，支持园区内特殊作业按不同企业、不同时间、不同作业类型等多维度进行统计分析，以及特殊作业信息在园区电子地图上实时显示和快速查询。

4）双重预防管理

以风险分级管控和隐患排查治理为主要建设机制，从风险识别到隐患排查治理、从隐患排查治理到风险再评估，形成完整的 PDCA 双闭环。将安全管理具体措施细化到各层级安全管理人员、操作人员，建立重大风险管控清单，并与日常安全工作清单和智能巡检相融合，最终落实到各层次、各岗位的具体安全管理工作上，实现隐患登记、隐患处理、隐患验收、隐患统计、隐患考核等全过程管理。

（4）构建横向互联纵向贯通的应急体系

以“平战结合”为主导思想，基于 GIS，结合监测预警对风险产生全过程的严密监控，集成突发事件监测监控、智能方案、指挥调度、专家会商等手段融于一身，实现应急事前、事中、事后的全过程、全方位、多维度的全面掌握。

实现园区和园区内企业对泄漏、火灾、爆炸等事故的应急救援资源进行管理，包括对专业队伍、储备物资、救援装备、通信保障和医疗救护等应急资源的动态管理，是对应急资源的基本信息、位置信息进行分类管理，包括对应急资源动态数据的获取、数据维护，要求能够准确地描述出资源的分布情况和使用情况，并能够实现对资源状态的监控及直观展示。

2. 实施效果

（1）经济价值

通过安监预警、风险评估手段，及时发现企业各类安全隐患并督促整改，提升企业本质安全，企业安全生产事件逐年下降，大大减少安全事故带来的经济损失。平台对园区安全监控，通过重大危险源、重点生产工艺、重点危险品以及园区所有罐区的自动化 AI 监控，实现预警事件的秒级响应及风险事件的快速闭环。有效的提高了园区安全生产的效果，园区安全应急处置能力提升，安全应急事故管理从事后报警单方处理转变为事前预警、多方协同，安全风险管控能力提升 50%，应急指挥效率提升 50%，安全巡检效率提升 45%。通过全面提高园区的风险预警能力，减少园区风险事故发生的概率以及安全环境事故带来的经济损失。

（2）解放人力

人工投入较原先降低 45%。提升园区应急指挥能力，通过视频联动、烟感火警的 AI 识别，以及发生事故后的紧急救援措施，节省了人员投入的基础上加强

了“平”“战”结合以平为主的理念，应急指挥效率提升 50%，安全巡检效率提升 45%。

（3）提升园区安全管理

提升安全管理效率：平台能够集成和管理园区安全资源和业务流程，如设备管理、人员管理、双重预防管理等。通过自动化和数字化的安全管理方式，提高安全管理效率，减少人力资源和时间成本。

提升安全管理水平：实现对园区的实时监控和预警。通过数据分析和智能算法，可以识别异常行为和潜在风险，提升园区的安全管理水平。

2.10.5 单位基本信息

卡奥斯化智物联科技（青岛）有限公司成立于 2017 年，是卡奥斯数字科技（青岛）有限公司全资子公司，海尔集团成员企业，公司运营的海智化云平台是卡奥斯旗下化工行业工业互联网平台，也是全国领先的化工行业综合性服务平台。公司始终坚持化工行业工业互联网技术的研发、应用和推广，为政府、园区、企业提供基于大数据的全流程解决方案，拓展大数据在化工领域的应用，打造全球引领的化工行业解决方案专家。深耕化工行业市场，聚焦化工园区及化工企业客户，整合行业优势生态资源，与化工行业的生态各方形成了紧密的经济联合体，服务体系已日渐成熟，销售版图主要包括山东、安徽、四川等 10 余个省 30 余个地市，其中在化工行业领域已成为细分行业的龙头，已赋能全国 10 家以上化工园区，100 家以上化工企业。此外，卡奥斯化智物联还具备专业运营运维服务团队、科学的运维保障体系，不仅在项目建设期提供高质量服务，还提供长期持续的运营运维服务，既保障平台能够长期、稳定、高效的运行，又满足国家、省市对化工园区建设与管理的标准和要求。

2.11 案例十：面向智慧水务关键信息基础设施网络安全建设——构建水务工控网络安全能力闭环，打造城市安全防线

党的二十大报告指出，要“加强城市基础设施建设，打造宜居、韧性、智慧城市”。智慧水务是智慧城市的重要组成部分，是支撑社会经济发展、保障居民生活和工业生产的基础性产业。近年来，在我国数字化转型战略推进下，各水务企业相继开展信息化建设工作，以“智慧水务”为发展目标，积极探索并推进水务行业数字化转型。随着数字化转型工作的深入，水务企业逐步向数字化、智能化方向发展，水务工控系统从封闭、孤立状态走向开放与互通，由此带来的安全风险也与日俱增。

此外，水务行业作为国家关键信息基础设施的重要组成部分，我国相继出台了《"十四五"期间推进智慧水利建设实施方案》《关于大力推进智慧水利建设的指导意见》《水利网络安全保护技术规范》等政策文件，明确提出需强化关键信息基础设施安全防护、强化网络安全保障体系、加强网络安全监督等。

因此，在合规要求及安全形势双轮驱动下，提升智慧水务工控网络安全保障能力，确保水务关键信息基础设施、重要业务信息系统和关键数据资源安全，已经成为政府机构、企事业单位所关注的重点之一。

2.11.1 方案概述

本方案针对某水务集团及其下属饮用水厂、水质净水厂生产企业工控网络面临的安全问题，按照《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》《SL/T 803-2020 水利网络安全保护技术规范》等国家及行业相关政策标准要求，建设了覆盖水务集团的工业安全态势感知平台及其下属生产企业的工控网络安全防护系统，构建了智慧水务工控网络安全防御、安全监测及安全响应一体化的协同防御体系，实现了对智慧水务工控网络全方位、全天候的态势感知，全面提升了智慧水务工控网络安全防护水平。

1.方案背景

水务工控系统是我国重要的关键信息基础设施，在当前新技术融合发展和快速应用的背景下，工业化和信息化融合愈发密切，网络信息空间的边界不断向关键信息基础设施领域延展，导致水务工控系统也因此面临着严重的网络安全威胁。

某水务集团是以自来水生产、供水、污水治理为主营业务的城市公共服务提供商，目前已形成了集供排水、资源循环利用为一体的现代综合服务产业链。该水务集团各水厂工业控制系统由 PLC、工业 PC、工业通讯网络等组成，PLC 通过以太网形式连接接入交换机，组成厂区内环网。各水厂区运行数据通过以太网实时传输至企业中控室，并接受中控室的控制命令，水务集团总部进行集中监控。整体网络结构较为复杂，由多个生产工艺流程构成，并且网络资产类型较多，难以采用单一的防护策略进行安全建设。因此需根据水务集团的实际业务情况，对整个工控网络的安全风险进行深入分析，找出风险点和脆弱点，从不同角度及层次进行多种安全策略的综合设计。

目前工信部、公安部及水利部先后出台一系列工业信息安全和水务行业网络安全相关法律条例，对工控网络安全建设做出了指导与要求。2019 年、2020 年水利部分别印发《水利部关于印发水利网络安全管理办法（试行）的通知》《水利网络安全保护技术规范》等规范，要求开展工控网络安全纵深防御、安全监测预警、应急响应等能力的建设。

因此，在水务工控网络的安全防护建设中，需严格遵循国家和行业相关标准，结合生产企业具体业务情况和安全需求进行规划与建设。

2.方案简介

通过分析水务工控网络所存在的安全问题，依据国家及行业等相关法律法规及要求，遵循以适度防护为核心，以生产可用性优先的原则，从业务的角度出发，采用协议深度解析、白名单防护、数据变化率检测、大数据分析、态势感知等多项技术，为水务工控网络构建了贴合实际业务的集安全防护、安全运营、安全服务于一体的综合性解决方案，实现对水务工控网络威胁实时感知、安全策略集中审计、安全事件快速处置等能力，赋能水务集团工控网络安全建设，打造水务集团纵深防御体系。

3.方案目标

项目建设以保障水务工控网络安全为出发点，结合各水厂生产流程及业务特点，重点围绕网络安全、应用安全、控制安全等维度进行主动式安全防御体系建设，目的为有效抵御水务工控网络面临的恶意代码、APT 等攻击威胁，降低安全事件发生的概率。项目具体实现的目标如下:

（1）提升智慧水务工控网络边界安全防护能力

智慧水务网络边界主要存在于互联网与办公网、办公网与工控网络以及工控网络内部。目前互联网与办公网之间安全防护措施相对较为完善，但是工控网络内部及与其他网络之间普遍缺乏安全防护措施，存在很大的安全隐患。结合各水厂生产业务情况，按照“纵向分层次、横向分业务”的原则，对水厂工控网络进行安全域划分，并在安全域边界应用技术隔离手段，构建边界安全防护能力，打造安全可信的工业网络环境，防范网络攻击与安全威胁，保障智慧水务工控网络安全水平。

（2）构建动态综合安全防御体系

结合当前该水务集团各水厂工控网络安全现状及发展趋势，通过构建基于边界防护、入侵检测、运维审计、日志审计、流量审计、漏洞检测、配置核查、态势感知等一体化的动态综合安全防御体系，形成智慧水务工控网络安全防护与主动预警的综合保障能力。

（3）提升智慧水务工控网络态势感知与监测预警能力

当前工业领域网络安全形势日益严峻，安全风险呈现多元化特征，安全隐患发现难度更高。因此，网络安全监测手段也需同步进行补充与提升。基于当前智慧水务工控网络安全防护手段众多、资产混乱、安全态势不可视的现状，通过构建覆盖净水、供水、污水处理等环节的工业安全态势感知平台，综合异构数据采集、协议深度解析、模型分析、用户画像、大数据分析等技术，采用威胁情报及安全事件关联分析的机制，实现对智慧水务工控网络安全态势全局掌控。在出现安全威胁时，通过协同联动网络中各类安全设备及时进行抑制，防止安全威胁的进一步蔓延，对水务集团及下属各水厂提供安全保障。

2.11.2 方案实施概况

通过深入了解各水厂业务特征和安全需求，构建贴合水务业务场景的行为基线，以行为分析、应用分析为基础，结合“白名单”防护措施及黑名单技术手段，建立贴合行为基线的安全防护策略，形成针对水务集团及各水厂构建安全合规的综合防御体系，实现网络监测预警和快速响应需求，确保国家关键信息基础设施安全运行。

1.项目总体架构和主要内容

（1）项目总体架构

项目总体架构以全面管控、纵深防御的防护理念为核心，对水务集团及下属水厂进行网络安全防护。在各水厂工控网络采取边界隔离、终端防护、入侵检测、流量审计等多种安全防护手段，通过对业务流程的全面梳理以及全网安全日志、流量的集中分析，构建基于通信、指令的安全模型，快速发现网络中的异常通信行为、违规指令及“合法操作行为下的非法指令”等操作，实现对智慧水务工控网络设备、资产、应用等防护对象的全面管控。

集团部署的态势感知系统将网络中各类安全设备作为安全数据采集的探针，通过底层海量数据采集及分析能力，形成工业网络安全底图，实现对下属各水厂工控网络全面的态势研判，借助第三方威胁情报等综合判定网络安全风险，实现对网络安全事件的通报预警和协同处置，从多个维度实现企业安全生产运营。

图 10-1 总体技术架构

（2）防御体系建设

该方案设计主要采用体系化建设应用，通过安全防护检测体系、安全态势分

析体系以及安全服务响应体系等内容，深度构建动态闭环的安全防护体系能力。

安全防护检测体系以行为基线为中心，提供基础安全防护能力，包括访问控制行为分析、白名单识别、工业设备安全管控等。同时作为安全数据来源，将各个节点的安全数据、异常数据等上报至安全态势分析体系，用作安全环境、安全基线的分析，展示分析结果的同时，将生产网络、应用系统运行状态传递至安全服务响应体系进行统一的运维监控。

安全态势分析主要作用于安全数据的统计与分析，通过部署应用的安全设备作为安全数据的采集探针，以及大数据存储分析等技术手段对网络安全事件、未知威胁信息进行多维度统计。结合统计数据进行业务安全威胁建模，分析存在的脆弱性、威胁源等导致安全事件发生的可能性，以及由此产生的后果和影响。构建安全事件自动处置体系，动态管控安全检测防护策略。

安全服务响应体系承担安全支撑、监测服务、运维服务、风险评估等各项服务响应能力，为整体安全防护体系提供事前评估预警、事中分析处置、事后溯源提升的安全能力。同时安全服务响应体系与其他两大体系互为支撑赋能，共同建设动态安全防护体系。

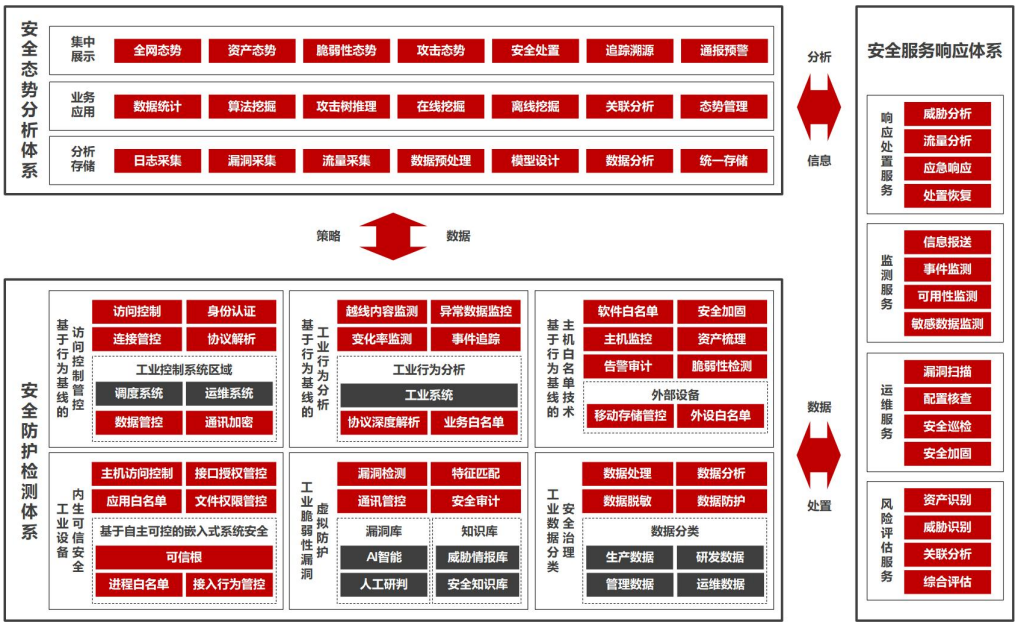


图 10-2　纵深防御体系

（3）主要技术说明

■ 协议深度解析

通过对工控协议“协议完整性”、“功能码”、“地址范围”和“工艺参数范围”进行深度检测和过滤，及时发现可疑指令和恶意数据，保障控制指令及生

产网络安全。

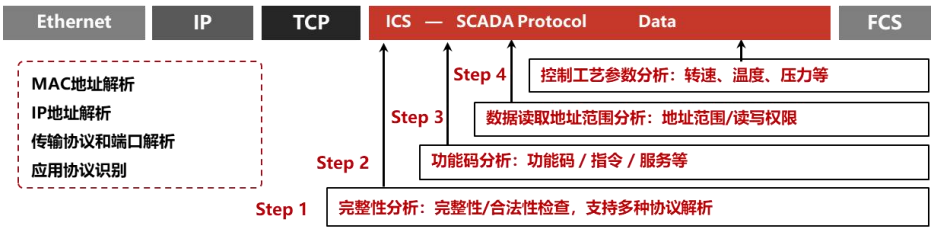


图 10-3 协议深度解析

■ 智能 AI 协议识别

基于协议深度解析技术，通过单包特征匹配、多包特征匹配、统计特征匹配、算法插件匹配等模块进行流量解析，实现对协议的识别。

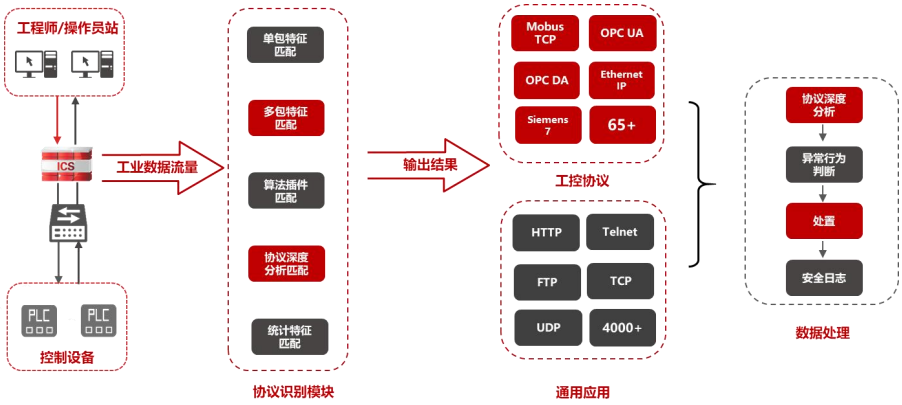
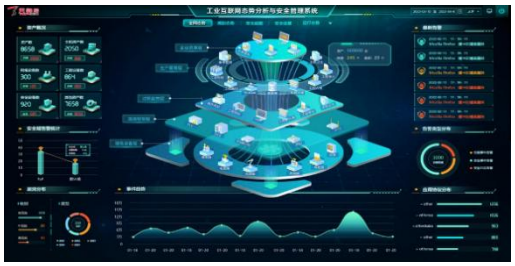


图 10-4 智能 AI 识别

■ 安全态势全方位展示



全网态势

威胁态势

漏洞态势

运行态势

图 10-5 全方位安全态势

■ 全方位威胁防御

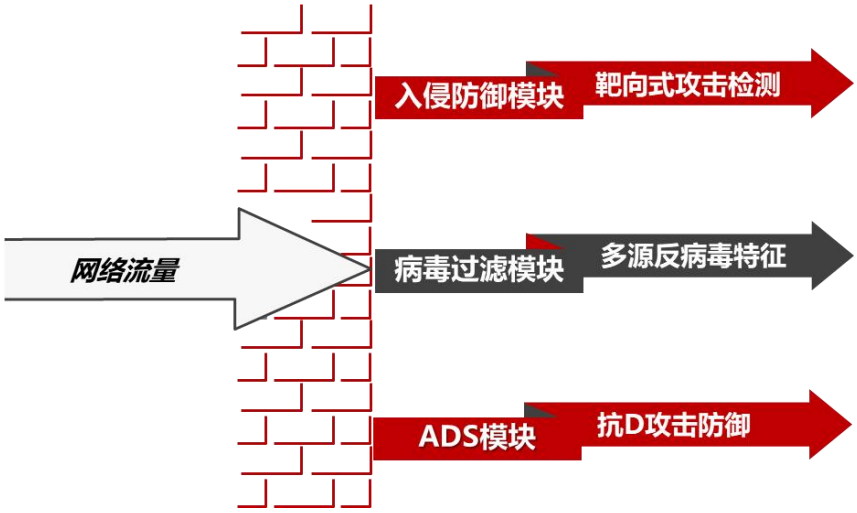


图 10-6 全方位威胁防御

■ 全方位资产管理

图 10-7 全方位资产管理

2.网络、平台或安全互联架构

（1）网络互联架构

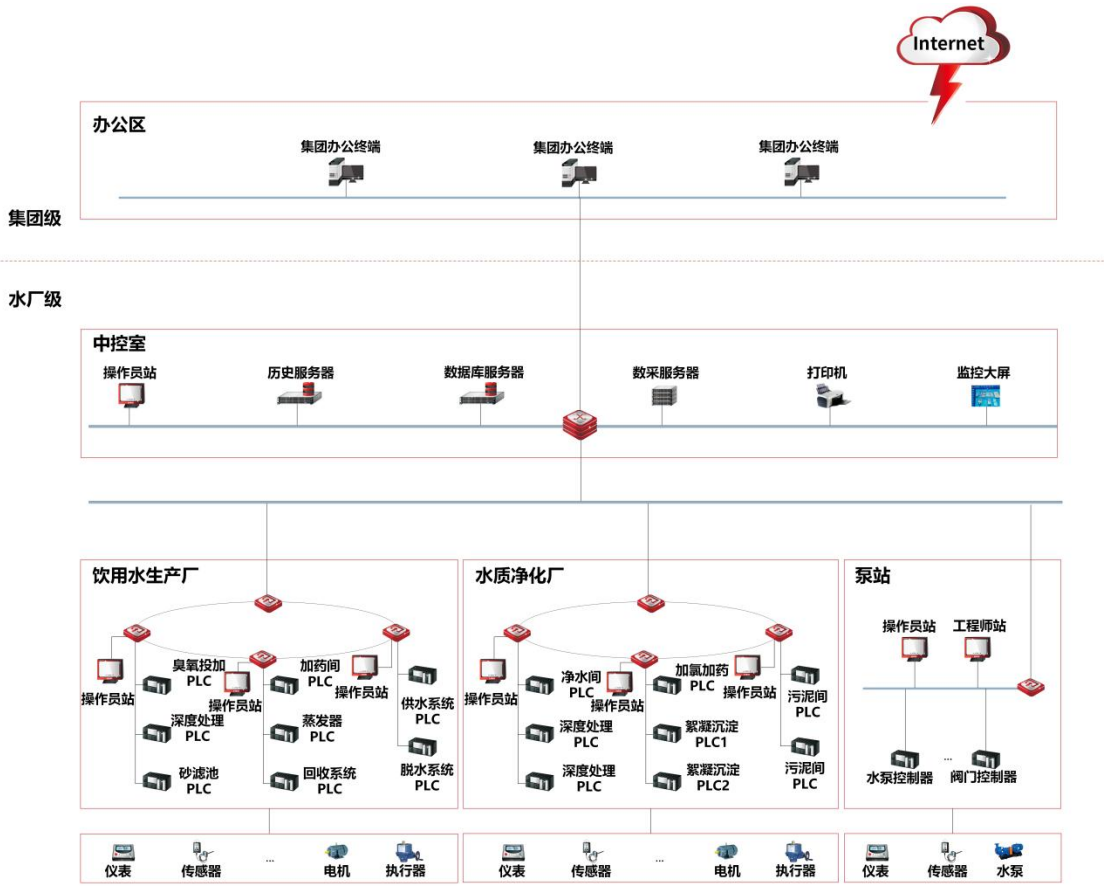


图 10-8 网络互联架构

水务集团各水厂工业控制系统由 PLC、工业 PC、工业通讯网络等组成，PLC 通过以太网形式连接接入交换机，组成厂区内环网。各水厂区运行数据通过以太网实时传输至企业中控室，并接受中控室的控制命令，水务集团总部进行集中监控。

（2）建设内容

结合当前业务结构特点，本方案针对智慧水务中控室与办公网之间的数据交互采取单向技术隔离手段；各水厂、泵站等控制系统间访问行为建立安全访问策略；对工业主机采取基于“白名单”技术的安全防护手段，构建应用、进程白名单，并对移动外设进行管控；对外界入侵攻击行为进行检测与审计；对运维人员的运维操作行为、命令进行审计记录；同时利用态势感知技术，形成智慧水务集团和下属各水厂协调联动的网络安全处置工作机制。

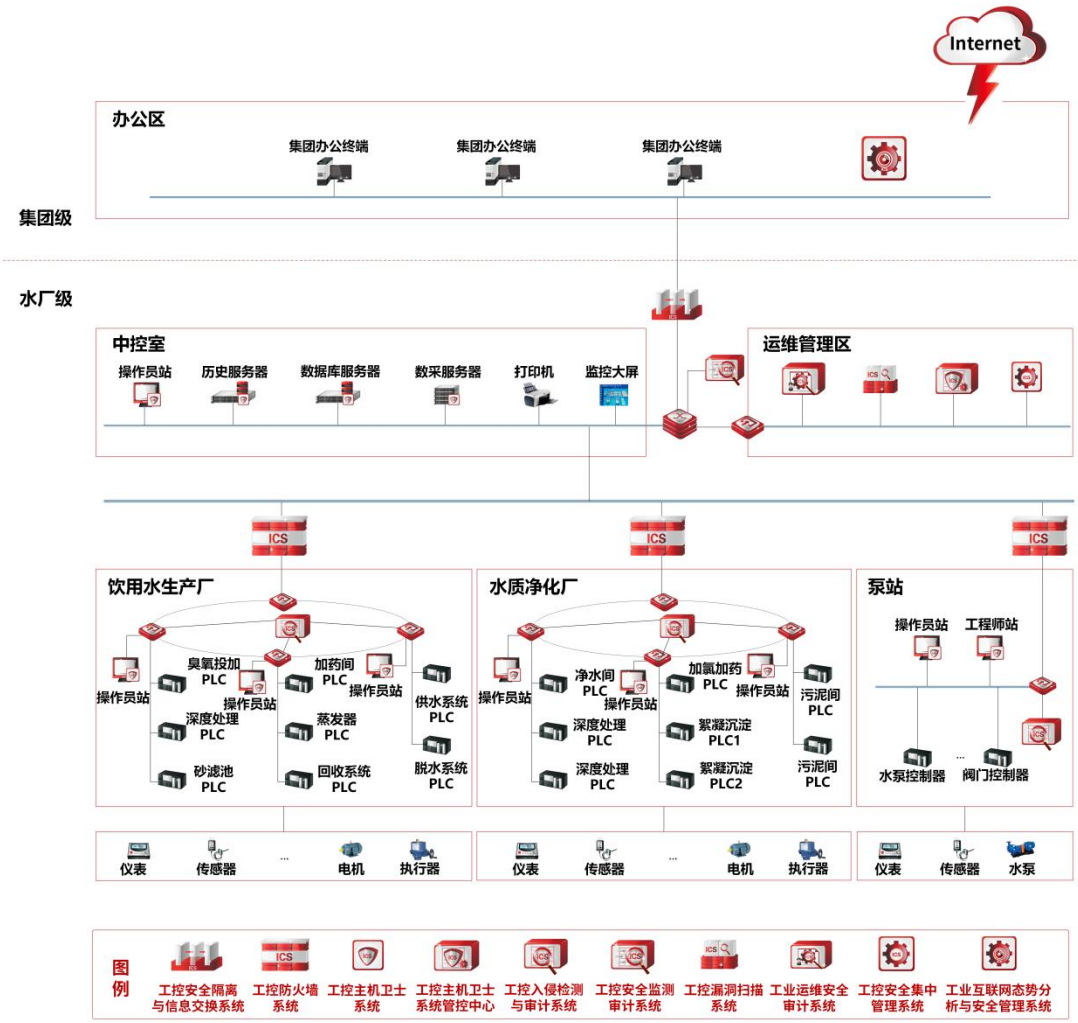


图 10-9 安全防护架构图

■ 中控室和办公网区域边界安全防护设计

根据智慧水务现场实际业务需求，对中控室与办公网之间数据交互进行细粒度访问控制，通过采用单向隔离传输机制，对生产办公网的边界流量进行单向技术隔离，防范病毒、木马、蠕虫等恶意程序在生产内网传播。

■ 饮用水生产厂、净水厂、泵站等系统边界安全防护设计

通过基于工业协议的深度识别，对饮用水生产厂、净水厂、泵站等系统间的访问行为进行访问控制，精准定位安全威胁，阻断病毒跨区域攻击各厂站工控系统，全面提升智慧水务工控网络抵御入侵及各类网络攻击的能力，保障设备稳定运行。

■ 智慧水务工控网络入侵行为检测与恶意程序识别能力设计

通过在智慧水务工控网络核心交换机处应用入侵检测手段，根据业务功能需求制定白名单策略，采用攻击规则检测+业务白名单两种方式，对智慧水务工控

网络捕获的数据包进行相应的行为匹配，及时发现来自智慧水务工控网络内外部攻击威胁，可根据不同业务系统的安全需求，制定符合应用场景的安全策略，对安全事件详情进行记录和报文留存，为安全事件调查提供基础依据，真正做到事前预警、事中监控和事后追溯。

■ **智慧水务工控主机病毒防范能力设计**

通过在智慧水务工控网络中操作员站和服务器等设备中安装基于“白名单”的工控主机安全防护产品，对终端运行进程、服务等以白名单方式进行识别，策略范围外进程、服务禁用。服务端对移动存储介质进行授权，非授权介质从驱动层面禁用。

■ **智慧水务工控网络中操作行为安全审计设计**

通过在智慧水务各水厂级泵站应用网络安全监测和审计手段，对下属节点数据变化及写操作内容进行审计；自动进行工控网络资产梳理，形成直观、清晰的网络拓扑图，协助用户了解网络异常趋势。同时可作为态势感知重要探针，实现日志信息上传，制定主动防御策略，实现联动防御，动态调整安全防护措施，避免发生安全事故。

■ **智慧水务工控网络运维人员操作过程监管设计**

通过在智慧水务工控网络中应用运维安全审计手段，对工控网络的安全运维进行审计记录，以及包含对账号、授权、认证和综合审计等的一体化管理。通过权限的管理，实现对每个资产、账号，中间件指令的精确控制，避免交叉运维操作、资产和账号的越权违规操作。明确运维责任，降低安全事件发生概率。

■ **智慧水务工控网络脆弱性检测设计**

在智慧水务工控网络中应用脆弱性检测技术，通过离线方式，定期开展针对智慧水务工控网络的非运行状态以及未上线前主机、应用以及控制器的脆弱性扫描，实现对网络及控制系统的脆弱性识别。

■ **智慧水务工控网络中安全设备、安全策略集中管控能力设计**

在智慧水务工控网络中建立安全管理中心，提供统一策略配置，实现对安全设备的统一管理，可集中收集日志统一统计分析，实现工控网络安全联动与整合，及时对网络攻击与异常行为进行快速处置。同时方便运维人员对不同设备的运维管理工作。

■ 智慧水务工控网络安全态势监测与运营设计

通过在智慧水务集团侧建立安全运营中心，应用工业互联网态势感知技术，依据安全基础能力的建设，形成安全策略联动、动态感知的安全分析能力，实现对全网业务态势监测预警及安全事件快速处置，通过事件监测、威胁预警、攻击溯源等多种手段相结合的方式提升智慧水务工控网络的安全运营水平。

3.具体应用场景和安全应用模式

（1）应用场景

本方案适用于工业企业工控网络安全防护、威胁识别及溯源、态势感知呈现等典型应用场景。且相关安全应用场景已经过真实业务测试验证，各项性能安全稳定，为后续向水务行业及电力、煤矿等其他行业安全建设积累足够的建设经验。

（2）安全应用模式

方案针对水务集团厂区级及集团级开展安全防护设计，实现不同层级的用户应用场景的安全需求。依托在厂区级、集团级各级安全能力构建，实现多级联动机制，通过多维安全数据联动交互，反映网络运行及安全状态，为安全处置提供决策支撑。

4.安全及可靠性

本项目方案设计贴合实际业务场景，围绕智慧水务工控网络厂级、集团级各层级开展全方位安全设计，通过事前、事中、事后多层次立体防御体系的建立，保障智慧水务工控网络抵御各种病毒、安全威胁，实现对智慧水务工控网络安全防护及预警。

（1）事前防御

通过应用工业漏洞扫描系统，采用系统漏洞检测、风险评估等技术手段，综合评估系统资产、安全状态、高危漏洞等信息，并针对系统中存在的漏洞和弱点，提供整改方法和建议，帮助客户修补漏洞，防御黑客通过漏洞入侵植入病毒，全面提升系统整体安全性。

（2）事中检测

通过边界隔离、入侵检测、白名单防护、行为基线等技术手段，对水务工控环境进行持续监控和检测，及时发现基于病毒、蠕虫、木马、异常流量、恶意程

序等的攻击威胁，一旦发现异常事件将第一时间进行告警推送，并进行告警阻断，防范威胁蔓延。

（3）事后处置

通过在集团建立应急响应和恢复程序，针对已经发生的安全事件进行日志留存、攻击取证，进而展开攻击行为分析，从而判断本次安全事件所利用的漏洞及攻击路径，并能够提供专业的处置建议，预防攻击的再次来袭。

5.其他亮点

（1）以可信技术构建安全运行环境

通过对智慧水务工控网络通信行为进行深度学习、分析，对各个网络节点的访问关系、流量行为进行建模、分析，建立可信通信模型，以便达到允许的可信访问指令、可信流量、可信的设备在系统间进行连接和访问。

（2）基于数据变化率监测技术

通过对智慧水务工控网络中流量的数据报文进行完整性还原，识别报文中的控制指令，依据业务的通信行为与指令进行关联分析，并建立业务的控制行为基线，通过行为基线构建深度分析体系，同时与态势感知安全信息进行匹配分析，识别异常控制行为。

（3）智能化工业资产识别

通过工业资产指纹识别技术，全面发现水务工控网资产，从工业设备、主机、应用、业务等多个维度建立资产库，并自动生成生产网络资产拓扑，对网内资产进行实时安全监控，呈现网络安全风险、脆弱性等安全信息。

2.11.3 下一步实施计划

1. 计划 1

通过本方案试点建设，下一步计划发挥龙头企业标杆案例示范影响效力，在水务行业及电力、矿业等其他行业中进行推广应用。方案中应用的入侵检测、主机防护、漏洞扫描、态势监测等安全能力可复制推广应用于各关键信息基础设施领域，实现安全能力行业赋能。

2. 计划 2

本方案以业务为核心开展安全防护技术手段的应用，后续根据业务之间关联关系，进一步强化安全防护策略，细化安全手段与业务的关联分析能力，从而完善更加贴合客户需求的安全方案，实现更为智能、快捷和有效的安全防护和感知，构建工控网络协同动态防护体系。

2.11.4 方案创新点和实施效果

1. 方案先进性及创新点

（1）安全能力集中管控

通过态势感知系统统一纳管访问控制、流量审计、入侵检测、基线核查、漏洞扫描等安全能力，通过策略采集、策略下发及安全编排等动作，实现对水务安全态势的全局掌控，支撑常态化安全运营工作开展。

（2）全面的安全分析能力

对网络中的资产数据、威胁数据、脆弱性数据及运行数据等进行统一收集，运用关联分析、用户画像、业务安全基线、模型分析、威胁情报等技术，进行多层次的安全分析和多维度的持续监测与评估，形成安全联动、动态感知的整体安全分析能力。

（3）全局态势全面掌控

基于安全态势监测分析能力，以全局视角对智慧水务工控网络安全数据进行收集、存储、分析、展示等，实现对水务工控网络全网态势、资产态势、威胁态势等全方位感知。同时结合最新的网络安全威胁情报，持续监测，准确及时地发现各种潜在威胁和攻击，并采取处置措施，达到最大限度降低水务工控网络面临的安全威胁的目的。

2. 实施效果

本项目建设完成后，全面提升了智慧水务工控网络整体安全性，确保了设备、系统、网络稳定及可靠性，保障生产连续性，提高智慧水务安全生产管理水平及工作效率等，同时可实现针对智慧水务行业网络安全建设复制推广以及参考的作用。

■ 动态进行安全防御，提升安全事件响应速度

通过联动网内各类安全设备，可以对发现的安全问题快速定位，并制定有效

的安全防御手段，利用系统的安全策略集中管理能力，可以动态调整设备安全策略，快速封堵安全漏洞，及时处置安全事件，最大程度的降低事件影响范围。

■ **全局视角监控网络安全现状，提升安全运营能力**

帮助智慧水务企业全面掌握安全运行数据和安全情报，全局洞悉智慧水务工控网络安全态势，并结合安全资源，及时发现可能面临的安全威胁和风险，帮助智慧水务企业对安全事件及时追踪溯源，提升安全运营能力。

■ **提升安全运维效率，助力企业降本增效**

通过安全设备集中管控，以及策略配置，实现安全管理的集中化、便捷化，提升安全运维效率，减少安全运维人员工作量，降低企业人力资源投入，促进企业降本增效。

2.11.5 单位基本信息

北京天融信网络安全技术有限公司（简称天融信）创始于 1995 年，是中国领先的网络安全、大数据与安全云服务提供商。亲历中国网络安全产业的发展历程，如今已从中国第一台商用防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。自成立至今为工业企业和工业互联网平台企业提供了大量优质的解决方案，覆盖电力、轨道交通、航空航天、军工、能源、石油化工、机械制造、国防工业、汽车、电子等行业领域。天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

3. 结束语

“编制工业互联网典型安全解决方案案例汇编”是工信部 2023 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+全链接、工业数字孪生、国密算法等新技术、新场景提供优秀安全实践，同时涵盖能源、汽车、水务等重要行业的安全解决方案，以及自适应安全防御体系、安全诊断系统的建设方案，与往年案例汇编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。