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

工业互联网安全解决方案案例汇编

（2024年）

工业互联网产业联盟（AII）
2025年11月

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

工业互联网安全解决方案案例汇编

（2024）

工业互联网产业联盟（AII）

2025 年 10 月

目 录

前　言

工业互联网作为新一代信息技术与制造业深度融合的产物，通过对人、机、物的全面互联，构建起全要素、全产业链、全价值链全面连接的新型生产制造和服务体系，是数字化转型的实现途径，是实现新旧动能转换的关键力量。自 2018 年以来，工业互联网连续 8 年写入政府工作报告；其中 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；2024 年出台稳定工业经济运行、支持先进制造业举措，提高重点行业企业研发费用加计扣除比例，推动重点产业链高质量发展，工业企业利润由降转升；2025 年指出加快工业互联网创新发展的重要性。

当前我国工业互联网核心产业规模超过 1.5 万亿元，带动经济增长近 3.5 万亿元，工业互联网已拓展至 49 个国民经济大类，实现了 41 个工业大类全覆盖，为发展新质生产力、建设现代化产业体系提供了重要支撑。为了促进工业互联网产业安全的发展，近三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、量子计算等新技术与工业互联网融合导致攻击面扩大；另一方面，供应链攻击、AI 生成式攻击等新型威胁占比持续增长，传统防护手段面临失效风险。

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范的优秀案例。通过案例征集，组织专家评审，最终评选出 8 个优秀案例汇编入《工业互联网典型安全解决案案例汇编(2024)》。本报告汇编了有关 5G 专网、5G 泛终端、物联网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。主要参与单位有：杭州安恒信息技术股份有限公司、宁波市宁数安全科技有限公司、中国移动通信集团广东有限公司、广东云百科技有限公司、北京浩瀚深度信息技术股份有限公司、斑马网络技术有限公司、中国移动通信集团安徽有限公司、安徽古井集团有限责任公司、启明星辰信息技术集团股份有限公司、中国联合网络通信有限公司研究院、四川长虹新能源科技股份有限公司、中国移动通信集团山东有限公司、山东中烟工业有限责任公司、中国石油天然气股份有限公司长庆油田分公司、恒安嘉新(北京)科技股份公司、中国移动通信集团河南有限公司、比亚迪汽车工业有限公司、北京启明星辰信息安全技术有限公司。

本报告的参编人：张峰、柯皓仁、陶耀东、李江力、王雨晨、于乐、马禹昇、李艳东、刘晓曼、闫霞、李雅璇、付超、井柯、白小愚、林文锋、孙际勇、王君诚、何梦靖、柳兴、王哲、李超峰、崔晓雷、李建元、李海波、马岩、牟君、郑绪、艾红伟。

工业互联网产业联盟 安全组

二〇二五年十月

1. 工业互联网安全概述

1.1 工业互联网安全形势

据工信部最新数据显示，我国工业互联网已拓展至49个国民经济大类，实现41个工业大类全覆盖，标识解析注册量突破6500亿个，连接工业设备超1亿台套，为发展新质生产力、建设现代化产业体系提供了重要支撑。工业互联网核心产业规模已突破1.5万亿元，带动经济增长近3.5万亿元，产业规模持续壮大，赋能转型升级作用不断显现。

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:

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。

2024 年 1 月，由工业和信息化部发布《工业控制系统网络安全防护指南》，指南是为适应新时期工业控制系统网络安全（以下简称工控安全）形势，进一步指导企业提升工控安全防护水平，夯实新型工业化发展安全根基而制定。指南在安全管理、技术防护、安全运营、责任落实四个方面提出了指导性建议，并明确指出“使用、运营工业控制系统的企业适用本指南，防护对象包括工业控制系统以及被网络攻击后可直接或间接影响生产运行的其他设备和系统”，指导工业企业提升工控网络安全水平，为新型工业化的高质量发展提供网络安全保障。4 月，工业和信息化部印发《工业互联网安全分类分级管理办法》旨在加强工业互联网安全分类分级管理，落实企业网络安全主体责任，提升工业互联网安全防护水平，促进工业互联网深度融合应用。2024 年 12 月，工业和信息化部、国务院国有资

产监督管理委员会、中华全国工商业联合会印发《制造业企业数字化转型实施指南》，指南鼓励龙头企业强化产业链供应链安全预警分析，提升风险联动预测和协同处置能力，增强产业链供应链韧性和风险防范能力，切实提升工业数据安全防护水平。同月工业和信息化部发布《打造“5G+工业互联网”512 工程升级版实施方案》，强调要加强“5G+工业互联网”应用安全技术产品研究，满足不同场景下安全保障需求，建立健全网络安全监测发现、预警通报、应急处置技术体系。

2025 年 4 月，工业和信息化部组织开展 2025 年工业互联网一体化进园区“百城千园行”活动，深入实施工业互联网安全分类分级管理，引导园区企业接入国家安全态势感知平台。此外，工业和信息化部办公厅还印发了《2025 年护航新型工业化网络安全专项行动方案》，提出建立完善工业领域网络安全防护重点企业清单，面向不少于 800 家工业企业开展网络安全贯标达标试点，有效提高重点企业综合防护水平；深化工业控制系统网络安全评估，探索开展工业控制产品安全检测认证；组织全国范围新型工业化网络安全政策标准宣贯，切实增强工业领域网络安全意识和保障能力，以高水平网络安全护航制造业高质量发展。

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）数据显示，近三年工控漏洞持续增长 2022 年新增漏洞 33 条，2023 年新增漏洞 92 条，2024 年新增漏洞 84 条；截止目前工控漏洞总数达 3000+，其中高危漏洞 1500+。工业互联网安全整体呈现出高危漏洞多、风险持续存在的现状，行业整体面临着五大安全挑战。

一是信息域物理域深度融合，跨域攻击危害大。随着工业化与信息化融合的快速发展，信息空间和物理空间的边界日益交叠，网络安全威胁也从信息域渗透到物理域。一旦信息域遭到攻击，造成敏感信息、重要数据、设计图纸、试验方案被远程控制或篡改，就可能引发物理域工业控制系统故障，轻则造成生产停滞、装备缺陷，重则造成基础设施破坏、人员伤亡、环境灾难，甚至可能导致社会动乱，危害国家安全。从 2010 年针对伊朗核电站控制系统的震网病毒事件，到 2022 年的乌克兰电力系统安全事件，全球已经发生大量由网络攻击造成的核电厂、水

设施、电网、石油生产和轨道交通等关键基础设施破坏的安全事件，工业互联网面临的安全威胁日益严峻。

二是产品服务供应链日益复杂，系统攻击面不断扩大。工业供应链由单一链条上企业的单线链接转向网络化、多层次的全方位链接，科研生产需要众多供应商参与，提供高度专业化的零部件和技术支持。供应商的产品安全可影响大量上下游企业，直接威胁到工业网络的安全。供应商的软硬件产品可能存在漏洞，亦或被恶意植入后门，一旦被黑客利用，就可能入侵企业工业网络，获取机密信息或破坏关键信息基础设施。2022 年日本丰田公司的主要供应商之一的小岛工业公司受到了勒索软件的攻击，导致丰田汽车不得不关闭部分的生产流程。我国的工业科研生产核心设备及工控系统主要依靠进口，在短时间内无法实现全部国产化替换的情况下，供应链安全将对工业网络安全形成持续威胁。

三是工业领域各行业差异，网络安全建设成本高。工业互联网不仅涉及制造业、电力、交通等众多行业，也涉及装备、控制系统、数据、网络、应用等层面，针对不同行业的工业互联网化需要开发不同的软硬件产品，相对应的，这些软硬件产品都需要定制化进行网络安全防护，这种定制化的安全开发成本高。此外，工业互联网涉及研发设计、生产制造、产品流通及售后服务等全产业链多个环节，运营单位、工业互联网平台提供商等多方主体在保护工业互联网安全方面的法律责任和义务划分模糊，监管职责分散于各个行业主管部门，建立责权清晰的监管体系需要企业各部门及人力资源的支持。

四是传统工业领域行业局限性明显，安全防护水平难以快速提升。工业领域有其自身的行业特点，相比于安全性，更注重实时性和可靠性，漏洞修复、系统防护软件升级等安全措施难以快速更新迭代，导致工业系统维护能力不足。此外，工业设备升级换代周期长，生产装备、操作系统滞后于时代发展，无法适配新型安全防护技术及机制等。从企业角度看，工业企业普遍存在重发展轻安全的情况，对工业互联网安全缺乏足够认识，安全防护投入较低，安全产品、安全解决方案应用水平不高，实力薄弱的中小企业更是缺乏配套资金及人力部署安全措施。

五是运维人员权限高，商业机密保护难度大。工业互联网通常涉及智能制造、电子装联、测试试验等复杂业务，科研生产中需要使用大量专业化工业控制系统

和仿真设计软件。为了确保网络的正常运行，需要配置工作人员进行设备维护、网络运维、监督管理等。这些运维人员往往被赋予了较高的访问控制权限，以便进行系统配置、监控和维护。人是网络安全工作的主体，也是网络系统的脆弱点，内部人员的恶意或过失行为可能造成重要机密信息的泄露，在设备调试、升级维护过程中信息安全保密隐患极大。

2. 典型安全解决方案

2.1 案例一：某大型电力股份有限公司全网域网络安全态势感知项目——管理信息和生产控制区网络安全态势融合

引言：中国某电力股份有限公司是国内领先的电力生产和运营商，其业务范围涵盖电力生产、传输、配送等环节，是国家关键基础设施的重要组成部分。随着电力系统信息化程度的不断提高，网络攻击手段也日益复杂多样，电力系统面临着前所未有的安全挑战。

为贯彻落实国家关于关键信息基础设施安全保护的法律法规，并应对日益严峻的网络安全形势，该公司决定建设一套基于管理信息大区与生产控制大区的网络安全态势感知系统。该系统旨在通过整合两大安全区域的安全数据，实现对全网域网络安全态势的实时监测和预警，并提升应急处置能力，保障电力系统安全稳定运行。

2.1.1 方案概述

1.方案背景

近年来，电力系统面临的网络威胁日益增加，面临的攻击更加复杂、多样、隐蔽、系统和持续，安全事件频繁发生，国家层面高度重视网络安全，特别是关键信息基础设施的安全保护。电力行业属于国家关键基础设施领域，涉及到国家安全、经济命脉和人民群众的生产生活，一旦受到攻击，可能引发人员伤亡、社会动荡等灾难性的后果。

中国某电力股份有限公司（以下简称“公司”）作为国内领先的电力生产和运营商，肩负着保障国家关键基础设施安全稳定运行的重要使命。为贯彻落实《中华人民共和国网络安全法》、《国能安全〔2015〕36 号文》、《电力信息系统安全检查规范》（GB/T 36047—2018）、《电力监控系统安全防护规定》、《国家能源局关于加强电力行业网络安全工作的指导意见》（国能发安全〔2018〕72 号）等国家和行业指导文件要求，提高电力业务系统的安全性和管理质量，消除、

降低当前存在的安全风险，公司推动建设基于管理信息大区与生产控制大区全网域网络安全态势感知系统（以下简称“态势感知系统”），树立管理信息网和生产控制网网络安全工作“一盘棋”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，实现管理信息大区与生产控制大区在安全监测、预警、防护、通报、响应和追溯工作的一体化、实时化，全面提高公司网络安全防护水平，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

本项目由安恒信息专业团队建设，基于公司安全管理现状和需求，结合电力行业特性及政策合规要求，构建了一套集管理信息大区与生产控制大区安全数据统一汇聚、融合分析、监测预警及响应处置于一体的综合监测预警体系。

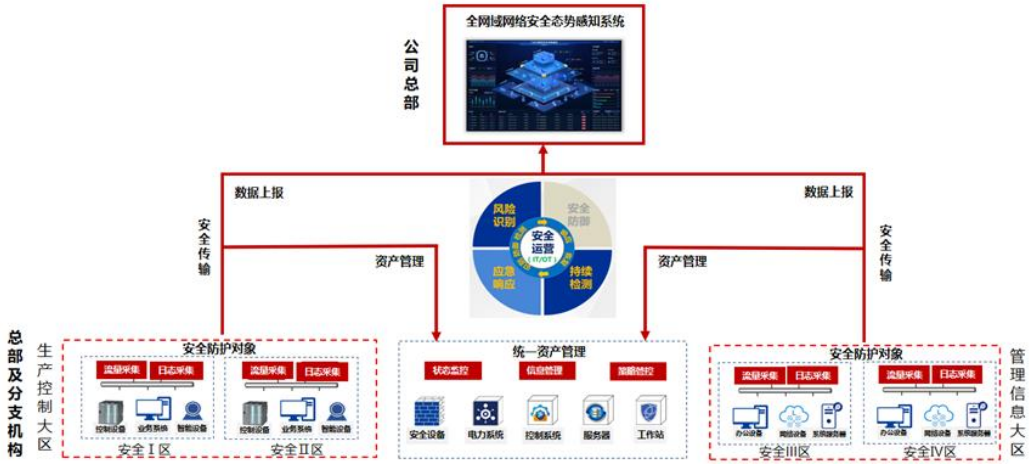

图 1-1 网络部署示意图

态势感知系统整合管理信息大区和生产控制大区业务系统各类安全日志与全流量数据开展全网域安全监测预警，实时掌握各区域关键信息基础设施、重要工业系统、重要业务系统的网络安全态势；实现 7*24 小时全天候的安全监测预警能力，精准识别网络威胁，利用态势感知系统集成的安全分析工具，可发现更深层次的问题，及时通报预警重大网络安全威胁，组织相关人员快速处置，降低网络风险发生的概率，实现“网络看得见、攻击防得住、网情控得住、敌手抓得住、危险止得住”，为公司网络安全管理工作提供有效的技术支撑，推动公司网络安全应急协调工作向深层次发展，提升网络安全防护水平，通过建立跨地域、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，保障公司业务的安全运行。

2.1.2 方案实施概况

1. 总体建设思路

通过对各区域安全环境的安全设备数据、能力调研、梳理与评估，形成全局网络安全运营方案建设；构建安全数据中台，对安全数据资产进行采集、处理、治理、分析等，形成安全数据服务目录，形成安全数据服务总线，持续利用安全数据资源，赋能上层业务应用；构建安全能力中台，对设备能力、服务能力等进行全面梳理整合，形成安全能力服务目录，供上层安全应用进行统一调度；建立安全应用中心，形成资产管理、安全监测、安全分析、响应处置、态势感知、运营管理六大应用中心，全面满足客户安全运营建设需求。

2. 总体技术架构

本项目通过前期对各地域安全监测数据的调研工作，掌握全面的数据采集方式、采集范围、采集对象和采集内容，以安全数据中台为核心，以安全合规为前提，统一接入各地域管理信息大区与生产控制大区安全监测数据，将各类异构数据格式范示化，对数据进行融合分析，开展对各地域安全大区的监测预警与态势感知工作。

图 1-2 总体技术架构图

3. 安全数据采集调研

实现对管理信息大区与生产控制大区的统一监测预警与态势感知，需要全面掌握各地域两个安全大区的数据采集现状。两大安全区域由于业务不同，在网络

架构与协议、数据特性差异和安全需求上存在很大差异。通过本次调研，我们详细分析了两大区域的差异与特点，并据此形成了全面的调研报告和数据接入评估方案，全面阐述了各地域的数据采集现状、存在的问题以及相应的优化建议，为后续的系统建设和安全管理工作提供了重要依据。

（1）差异与特点

■ 网络架构与协议差异

网络架构不同：生产控制大区主要包括变电站自动化系统、分布式能源接入系统等，其网络架构以工业控制系统为主。这些系统通常是封闭的、专用的网络，对实时性和可靠性要求极高。例如，在变电站自动化系统中，保护装置与测控装置之间的数据传输需要在几毫秒内完成，以确保故障时能快速切除故障线路。

管理信息大区的网络架构则更类似于一般的企业信息网络，包括办公自动化系统、电力营销系统等，主要用于信息管理和业务流程处理，对实时性要求相对较低，但数据量较大且数据类型复杂。

协议复杂多样：生产控制大区采用大量的工业控制协议，如 IEC 61850（用于变电站通信）、DNP3（分布式网络协议）等。这些协议设计初衷是为了满足工业控制的高效性和稳定性，通常没有考虑网络安全因素，而且协议的解析和理解需要专业的工业控制知识。

管理信息大区主要采用常见的互联网协议，如 TCP/IP 及其相关应用层协议，如 HTTP、SMTP 等。这些协议虽然有较成熟的安全机制，但也容易受到各种网络攻击。统一监测预警需要同时处理这两类差异巨大的协议，难度较大。

■ 数据特性差异

数据格式和内容差异：生产控制大区的数据格式较为固定，主要是设备的状态信息（如电压、电流、开关状态等）和控制指令（如断路器的开合操作）。这些数据的变化通常具有一定的规律，并且与电力系统的物理过程紧密相关。

管理信息大区的数据内容则更加多样化，包括结构化数据（如用户信息表、财务报表等）和非结构化数据（如电子邮件、文档等）。数据的格式和内容因业务系统的不同而千差万别。

数据量和流速差异：生产控制大区的数据量相对较小，但数据流速要求高，需要实时处理和分析。例如，在电力监控系统中，每隔几秒钟就需要采集一次实时运行数据，并且要及时做出控制决策。

管理信息大区的数据量可能非常大，尤其是在涉及大数据应用的场景下，如电力客户行为分析系统。但数据的流速相对较灵活，不需要像生产控制大区那样严格的实时处理。

■ 安全需求差异

安全目标测重点：生产控制大区的安全重点是保障电力系统的物理设备安全和运行稳定性，防止因网络攻击导致电力系统故障，如电网停电事故。其安全需求主要围绕电力生产的连续性、可靠性和实时性展开。

管理信息大区更关注数据的保密性、完整性和可用性，重点防止数据泄露、篡改和非法访问，以保护企业的商业机密和用户隐私。

风险容忍度差异：生产控制大区对风险的容忍度极低，因为任何微小的网络安全事件都可能引发严重的电力系统事故。

管理信息大区虽然也重视网络安全，但在一定程度上可以通过数据备份、恢复等措施来降低风险的影响，相对而言风险容忍度稍高。

（2）调研报告

开展对各区域管理信息大区和生产控制大区的调研工作，制定调研方案，从调研目的、对象、时间、方式、内容进行有序规划，掌握各地域和各安全大区的业务资产情况、重点监测对象、监测范围，以及各安全设备、监测装置/平台的监测内容，数据规范格式等内容，以便为输出数据接入评估方案提供数据支撑。

（3）数据接入评估

根据调研结果，开展数据接入评估工作，输出数据接入评估方案，主要包括如下内容：数据上报对象、数据接入范围、数据接入内容、数据接入方式、总体数据接入评估方案。

4. 安全数据中台

安全数据中台实现对接入的所有安全监测数据、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。

5. 应用系统设计

应用系统是以安全数据中台提供的数据服务为核心，为用户提供资产管理、安全监测、安全分析、响应处置、安全运营和态势感知等应用。

（1）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。

（2）安全监测

■ 安全告警感知

事件监测以丰富的工业威胁模型识别、全面的检测策略、智能机器学习、高效的沙箱动态分析，以及云端威胁情报匹配能力为基础，以安全事件为切入点，以威胁对象为聚合条件，动态梳理当前热点安全场景，将海量告警转化为几十条甚至十几条事件，无需关注搜索、过滤、聚合之间的逻辑差异，通过点击数据得到期待的分析结果，帮助用户聚焦热点安全问题，并对热点场景类型进行重点监测，大大减轻用户分析负担。事件监测具备丰富的 IT 和 OT 威胁监测能力，完整覆盖整个 APT 攻击链，能有效发现 APT 攻击及各种常见攻击。

■管理信息大区事件监测

通过对管理大区的全流量、日志数据监测，分析提取网络交互关键信息，包括时间、源/目的地址、传输层协议、应用层协议、连接或断开状态、上下行报文数和流量、告警数、数据来源等。能够针对 http、dns、FTP、邮件、Telnet、数据库操作、登录、文件、SSL/TLS、社会账号、ICMP、接口流量进行细粒度深度解析，掌握安全管理对象的实时状态和资源使用信息，能够及时监测 web 攻击、

邮件攻击、文件攻击、DNS 异常攻击、漏洞攻击、可疑行为、基线告警行为等进行实时监测。

■ 生产控制大区事件监测

通过对生产控制大区的全流量、日志数据监测，对 S7、Modbus/TCP，Profinet，Ethernet/IP、IEC104，DNP3、OPC、GE-SRTP、GE-EGD、BACnet、Fox、FINS、MELSEC、MMS、Hart IP、Goose、SV 等十多种工控协议的深度解析，分析提取网络交互关键信息，包括时间、源/目的地址、传输层协议、应用层协议、请求指令、请求服务、响应状态、响应指令、数据来源等。掌握安全管理对象的实时状态和资源使用信息，能够及时监测工控异常报文、工控关键事件、工控基线行为事件和工控漏洞攻击等进行实时监测。

■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。公司系统简单易用，支持一键全方面钻取，降低运维成本，提高运维效率。

（3）安全分析

■ 模型管理

威胁模型展示了基于 IT、OT 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。

■基线分析

支持网络行为基线分析能力，可识别新资产上线、新网络行为、新网络连接通信等。

以机器学习的方法建立工控网络的通信基线模型，对工控系统网络环境建立四类安全基线：资产基线、访问关系基线、流量基线、行为基线。通过基线学习、异常检测的方式，可以对异常情况进行发现和预警，提前发现 APT 攻击的痕迹。

■文件分析

通过将上传文件，来对文件的威胁进行沙箱检测，支持木马病毒扫描、静态分析、动态模拟分析，展示文件名称、源文件类型、MD5、评级、监测结果、评分、处理状态、文件上传时间、监测完成时间、操作（预览、下载报告、删除）等内容。

■智能检索

智能检索分析用于对工控安全日志的检索分析功能，具体支持如下功能:

- 支持检索语句的中文、英文、拼音智能联想;
- 支持逻辑运算符与字段值的自动提示补全;
- 支持检索语句快速保存，保留检索语句历史记录;
- 支持检索语句可直接发布成统计指标、规则模型、关联模型、情报模型，对实时数据进行分析与告警;
- 支持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;
- 支持任意关键字、参数、和正则表达式进行过滤查询；并提供检索关键字排除功能;
- 支持可指定多个查询条件进行组合查询；可通过关键字、条件表达式、时间范围对事件及数据进行快速检索，快速定位到安全分析人员关注的威胁和上下文数据，并支持检索趋势统计;
- 支持以时间轴的方式展示检索结果，并支持时间轴钻取和追加搜索;
- 支持对检索结果追加检索，支持点击检索结果字段快速加入到检索条件;
- 支持对展示字段灵活定义，允许用户选择特定的字段显示;
- 支持将查询的条件存储为查询模版，方便再次使用;
- 支持检索结果导出（不少于10000条），至少支持excel或CSV格式。

具备如下日志分类检索功能，智能检索满足基本要求外，还提供以下特定功能:

- 原始日志检索：支持选择日志源进行检索;
- 安全告警检索：支持根据安全事件的处置状态、威胁等级、攻击意图、所处攻击链阶段等多个维度进行检索；支持检索结果进行处理，处理状态标签包括：未处理、处理中、处理完成、误报等;

- 安全事件检索：支持根据安全事件威胁等级、攻击意图、所处攻击链阶段等多个维度进行检索。

■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，对公司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。公司系统简单易用，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，公司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。

■情报查询

支持对 IP、域名、文件 HASH(MD5/SHA1/SHA256)、邮箱进行情报查询，展示相关情报标签、地理位置、置信度、情报类型、更新时间、运营商、危险等级、情报子类、创建时间、标记、情报源、组织名称及事件信息。

支持第三方情况链接，情报查询结果支持跳转第三方链接：安恒情报分析、Whios、VirusTotal，补充相关情报信息。

（4）响应处置

响应处置为用户提供了各类半自动化、自动化处置工具，能够帮助用户快速处置相关的工作，可通过白名单、关闭规则开展日常告警降噪处理；可通过安全策略管理开展安全设备联动处置工作；可通过自动化编排与响应处置开展自动化处置的条件编排，进行自动化处置工作。

■安全设备联动管理

安全设备联动管理是将安全设备联动能力封装成 APP，提供灵活的设备联动配置管理，包括安全联动设备 APP 在线下载、导入、更新、卸载等操作；并展示平台联动设备应用 APP，显示 APP 资产厂商、APP 版本号、开发语言、支持设备型号、开发者、更新时间、描述、资产联动数。

■安全设备集中管控

具备对工业安全设备统一管理，包括设备信息管理、在线状态监控、资源使用状态监控、数据接入状态监控、远程设备管理（时间设置、升级维护、设备重

启/关闭/恢复出厂和 SNMP 监控管理）、远程设备访问、查看设备原始日志和一键在线状态检测等。

具备对流量监测类、安全审计类、安全防护类等设备策略进行集中管控，包括对设备的策略下发、对象管理等。创建策略任务后联动的设备能够即刻生效。

■同时，基于联动设备 APP 管理技术，支持开放的工业安全设备策略 API，使平台能够支持第三方工业安全设备的策略管控，极大提升在响应处置过程中的工作效率。

■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。

■告警处置

通过白名单、关闭规则、告警级别管理、告警延迟处置和风险订阅管理等功能，为用户提供半自动化、自动化告警响应处置能力，提高用户对告警处置的响应处置效率以及告警降噪效率。

（5）运营管理

■安全工作台

为公司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。

■安全仪表管理

为用户提供可编辑的安全可视化功能，为用户展示度量安全信息和关联安全业务指标现状的工具。仪表盘根据用户的实际需求定义其展示内容，平台内置丰富仪表盘组件，提供十种以上的可视化图像，包括一维时序图、一维分布图、二维时序图、二维分布图、大字报等图标类型。

■安全报告管理

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。平台目前支持导出深度威胁分析报告，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，平台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。

■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，工单记录状态未处理/处理中/已解决/已关闭，便于监督工单是否及时处理以及闭环。提供包括工单查询、工单新增、工单处置、工单删除、工单跟着以及工单批量操作等功能。

■通报预警

为用户提供预警和通报功能，用户对平台产生的安全告警进行新增预警，提示平台用户该告警可能存在一定风险隐患。

■级联管理

基于组织架构为企业建立上下级级联体系，平台可通过级联体系实现上下级之间的管理监控体系。

上级平台可对下级平台的风险情况实现整体分析后进行对比，上级平台可单独查看某一下级组织的风险情况。同时基于级联架构，实现上下级之间的通报预警、工单管理、绩效考核等能力。

（6）安全态势感知

安全可视化能够对公司态势进行展示，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。从整体视角展示公司总体的安全情况，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。

2.1.3 下一步实施计划

增强式数据过滤，在现有安全数据中台基础上，迭代开发增强式数据过滤技术，升级数据过滤引擎，对告警日志数据字段逐个解析，将不符合接入规范要求

的数据打标签，并记录不符合原因，通过标签过滤方式过滤这些不符合要求的数据，以进一步增强可读性。

建设安全垂域大模型，建设安全垂域大模型，并与现有态势感知系统协同，并辅助网络安全运营团队，构建全面的脆弱性评估能力、提升受保护目标的安全韧性、提升安全事件研判与分析能力，全面实现安全运营新目标。

IT/OT 告警事件智能研判，通过安全垂域大模型，将安全大区告警信息进行智能解读，将单个告警聚合组的攻击者 IP、受害者 IP、告警类型、告警名称、告警时间等字段作为输入，通过模板的方式对上下文进行解读，实现告警时间智能研判，大大提高威胁事件的处理效率和准确率。

智能运营驾驶，运维人员可通过自然语言的方式进行安全指令下发、数据查阅等功能，能够更快地获取到本地安全运营的态势情况，并通过更加便捷、简单的方式进行安全指令下发，极大提升用户体验。

2.1.4 方案创新点和实施效果

1.项目先进性及创新点

（1）基于智能机器学习的威胁感知技术创新

本项目中涉及的安全监测数据量大，通过基于智能机器学习的威胁感知，可自动收集、分析和学习系统正常运行状态下的数据行为，在此基础上智能提取用户节点的行为特征，并自动生成容易理解的操作规则、白名单、配置规则等，实现自动化特征规则的提取和生成，对异常数据、操作行为、安全事件、安全隐患等进行告警及综合管理。

（2）管理信息大区与生产控制大区数据深度融合分析技术创新

基于大数据分析技术和人工智能算法，将工业安全技术指标与安全生产指标进行分析挖掘，实现对多维度的信息和多源数据整合、关联、智能分析和预测，海量安全告警分析基于攻击意图、攻击策略、攻击方法、攻击次数、攻击时间、处置状态等影响因子构建资产评级模型，有效识别失陷资产，快速定位威胁源头。

（3）基于电力行业的网络安全场景化分析技术创新

在数据融合的基础上，本项目通过构建一整套以电力行业网络安全监测标准的场景化分析模型，并结合当前的组织结构、网络结构、业务系统、网络协议、网络流量、攻击链等数据进行自定义威胁模型与关联，提供全网域、全场景、全时空的安全事件监测分析与还原能力，提高监测精度、响应运营效率。

（4）基于闭环安全管理机制的多级协同响应处置技术创新

态势感知系统可针对安全事件和风险隐患进行实时发现，并提供了多元数据安全分析研判工具，为安全分析人员提供详细的调查取证工具，为安全预警与信息通报提供了有效支撑。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，协同响应公司各级单位或部门相关负责人员，有效提升了应急响应与处置效率。

2.实施效果

通过建立态势感知系统，实现公司全域网络安全监测无死角，大大提高了企业安全监测水平，保护了公司重要资产，减少了因网络安全事故造成大的经济损失。主要实施效果如下:

（1）建立统一数据共享机制

建立了公司本部与各区域的数据安全共享机制，形成监测数据上报、风险信息及时通报机制，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。

（2）提升跨地域、跨部门多方协同管理能力

依托大数据技术建立公司全网域网络安全监测预警与态势感知能力，实现了公司三级长效协同工作机制，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。

（3）促进网络安全态势技术持续创新

全面提升了公司各区域网络安全监测水平，加强了关键信息基础设施安全防护能力。同时可结合行业需求，对安全技术和方案进行改进和大范围推广，通过开发新产品、新技术、新服务等方式

2.1.5 单位基本信息

安恒信息技术股份有限公司（简称：安恒信息）成立于2007年，自成立以来，安恒信息秉承“构建安全可信的数字世界”的企业使命，以“数字经济的安全基石”为企业定位，以“诚信正直、成就客户、责任至上、开放创新、以人为本、共同成长”为企业核心价值观，致力于成为全球领先的数字安全企业。

自2008年首次为北京奥运会提供网络安保服务开始，安恒信息先后为上海世博会、广州亚运会、历届世界互联网大会、G20杭州峰会、厦门金砖会议、世界游泳锦标赛、武汉军运会、成都大运会、杭州亚运会、世界人工智能大会等上百场大型国际赛事、活动提供网络安保服务，实现16年重保零事故的成绩。

一直以来，安恒信息坚持把营收的近30%投入到研发当中。截至2024年6月，公司共申请专利2932项，参与制订信息安全类国家标准41项。

未来，安恒信息将继续以助力网络强国和数字中国为己任，为数据要素价值释放、数字经济发展筑牢数字安全屏障，以AI能力赋能数字安全产品和服务，并进一步推动产业生态合作，与合作伙伴一道，携手构建安全可信的数字世界。

2.2 案例二：基于物联网僵木蠕安全大模型的车联网安全风险监测服务——新型工业化安全赋能

引言：在“车路云一体化”多网融合、多主体交互、多种复杂场景并存的背景下，来自车端、路侧、云端的威胁呈爆发式增长，安全风险进一步加大，影响用户隐私，影响车辆安全，影响企业运营，威胁国家安全。

基于物联网僵木蠕安全大模型的车联网安全风险监测方案推向市场以来，一方面获得了产业界的充分肯定，如获得了中国信通院“2024 年智能网联汽车网络和数据安全典型案例”；另一方面，也通过向车企提供车联网安全保障服务，获得用户得充分认可，如获得广汽乘用车、广州云百科技的肯定和感谢。

同时，基于物联网僵木蠕安全大模型的车联网安全风险监测服务推向市场后，也取得了很好的经济效益。目前与广汽埃安、广汽本田、广州云百科技等相关企业进行车联网安全相关合作的合同金额已达 2.4 亿元，累计开通链接数达到百万级。

2.2.1 方案概述

本案例将“端安全”（轻量化安全防护技术）、“网安全”（车联网专有安全大模型）、“云安全”（端到端的车联网数字孪生体）三个方向的创新技术相结合，与车联网的云、网、车三个层级有机融合，在“端”提供防护、检测、响应能力，在“网”提供网络攻击、车联网场景、协议检测能力，在“云”提供综合的安全分析、安全运营、策略管理下发能力，构建了“云-网-端”协同联动的安全防护体系，为车企、示范区提供了具备自适应闭环安全防护能力的建设与运营服务，为国家监管提供了涵盖从车辆到网络的全面的安全数据支撑。

1.方案背景

为了综合因对车联网产业发展伴生的网络安全问题，解决智能网联汽车生产企业的信息安全合规、提升产品竞争力，满足车联网行业监管的诉求，城市示范区对“车路云一体化”建设中对网络安全数据的监测运营的需求，以及基础电信运营企业对车联网流量数据分析，支撑国家车联网信息安全监测的要求，广东移

动牵头，充分利用轻量化的车载安全组件技术、物联网僵木蠕安全大模型检测技术以及数字孪生、机器学习技术建设了本项目的车联网安全风险监测服务。

2.方案简介

面对在我国智能网联汽车产业快速发展的同时，网络信息安全问题日益蔓生的严峻问题，积极支撑国家监管要求。本项目通过基于物联网僵木蠕安全大模型、智能网联汽车场景的数字孪生技术，车端轻量化的安全防护技术，构建了完整涵盖“端”、“网”、“云”的立体安全防护服务。

面向智能网联汽车生产企业，通过智能网联汽车整车级安全防护与监测服务，满足了其对车辆产品自身的安全合规需求，以及持续的安全运营监测需求。

面向城市车路云一体化的建设者、运营者，通过车联网流量异常检测分析服务、车联网综合安全运营监测服务，满足了其对车辆、网络、云端的一体化安全监测、运营的需求。

面向行业监管，为国家车联网安全监测与公共服务平台提供“智能网联汽车+车联网大网”两方面的安全事件数据，支撑行业健康有序发展。

3.方案目标

（1）总体目标

a.服务对象

- 智能网联汽车生产企业

满足企业安全合规刚需，持续安全运营的需求。

- “车路云一体化”城市示范区

满足云管端一体化安全监测、运营的需求，并满足对车联网流量异常分析、安全预警的需求。

- 行业监管机构

为国家车联网安全监测与公共服务平台提供“智能网联汽车+车联网大网”两方面的安全事件数据，支撑行业健康有序发展。

b.服务内容

在服务内容方面，本案例方案提供了:

- 智能网联汽车整车级安全防护与监测服务

解决车企智能网联汽车产品的安全合规的需求，以及对车辆的持续安全运营监测需求，提升其产品的核心竞争力。

- 车联网异常流量、加密流量分析检测服务

解决在车联网方面的僵木蠕网络攻击、恶意程序、数据违规流转等安全风险检测需求，提供对重点业务保障手段的需求，满足国家在车联网流量监测上对网络安全威胁分析，安全事件上报支撑的要求。

- 车联网综合安全运营监测服务

一是为车企提供持续的安全监测、态势感知、应急响应等安全运营服务，应对网络安全风险；二是解决城市进行“车路云一体化”应用试点建设对“云-网-端”一体化安全监测运营的需求，满足智能网联汽车上路试点对示范区的安全防护、监测与运营的能力要求。

- 国家车联网安全监测数据上报支撑服务

通过车联网流量检测和分析服务提供车联网流量层面的安全事件上报支撑，通过智能网联汽车整车级安全防护与检测、综合安全运营服务提供对车辆层面的安全事件上报支撑。完成了和国家车联网产品安全漏洞专业库(CAVD)对接，上报车联网漏洞数据；完成和国家车联网安全监测与公共服务平台的对接，上报网络安全事件数据，数据接口符合国标《车联网安全管理接口规范》要求。

c.创新性

总体来看，本案例将“端安全”（轻量化安全防护技术）、“网安全”（车联网专有安全大模型）、“云安全”（端到端的车联网数字孪生体）三个方向的创新技术相结合，与车联网的云、网、车三个层级有机融合，在“端”提供防护、检测、响应能力，在“网”提供网络攻击、车联网场景、协议检测能力，在“云”提供综合的安全分析、安全运营、策略管理下发能力，构建了“云-网-端”协同联动的安全防护体系，为车企、示范区提供了具备自适应闭环安全防护能力的建设与运营服务，为国家监管提供了涵盖从车辆到网络的全面的安全数据支撑。

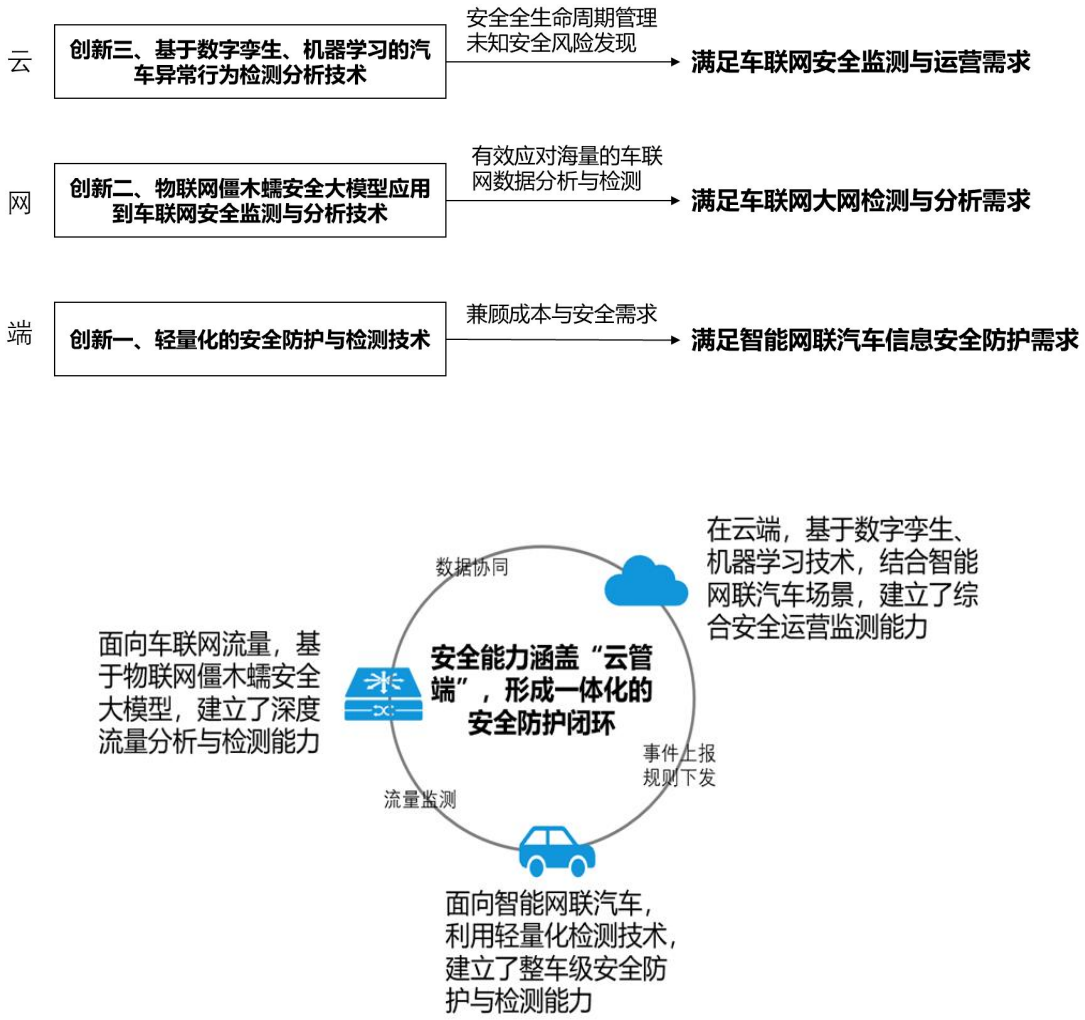

图 2-1 形成“云网端”协同安全防护和检测能力的创新

2.2.2 方案实施概况

面对在我国智能网联汽车产业快速发展的同时，网络信息安全问题日益蔓生的严峻问题，积极支撑国家监管要求。本项目通过基于物联网僵木蠕安全大模型、智能网联汽车场景的数字孪生技术，车端轻量化的安全防护技术，构建了完整涵盖“端”、“网”、“云”的立体安全防护服务。

1. 项目总体技术架构和主要内容

（1）方案综述

端侧实现了对智能网联汽车的安全防护与检测能力，网侧实现了对车联网流量的深度分析和检测能力，云端实现了对车联网综合的安全运营服务能力，形成覆盖“云-管-端”一体化的安全监测方案。

（2）服务整体框架

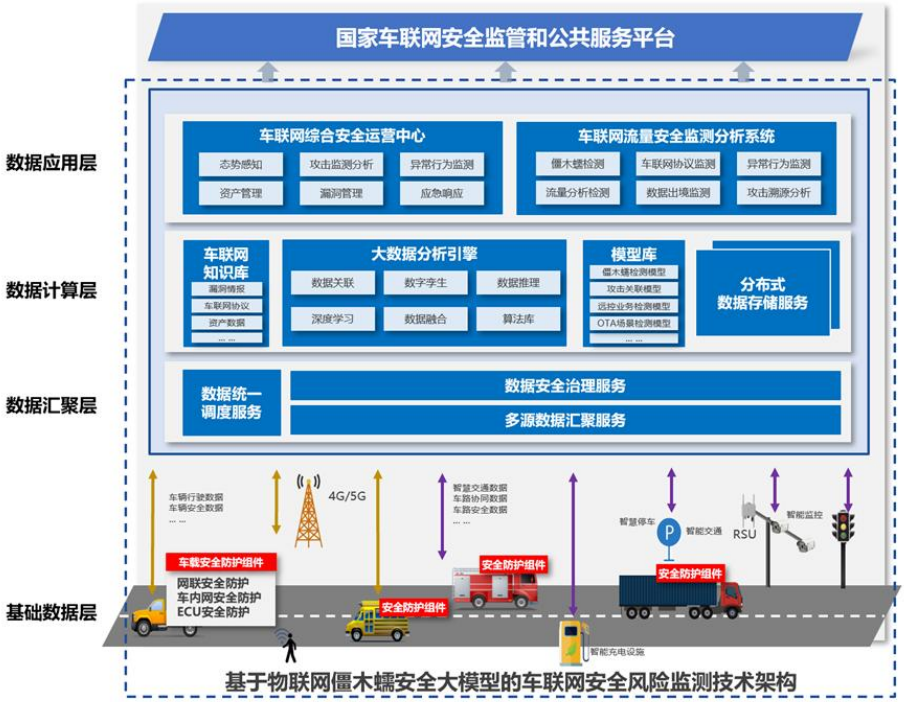

图 2-2 基于物联网僵木蠕安全大模型的车联网安全风险监测服务的技术架构

如上图所示，广东移动建立的基于物联网僵木蠕安全大模型的智能网联汽车安全风险监测服务的技术架构包括四个层级：基础数据层、数据汇聚层、数据计算层和数据应用层，以下分别展开描述：

■ 基础数据层

实现对智能网联汽车的安全检测、防护能力，对车联网数据的监测、采集能力。

依托当前已经建设的物联网 DPI 系统和物联网僵木蠕检测系统，采集全量的车联网上网日志以及网络攻击、网络入侵、网络受控、隐蔽隧道、敏感数据、恶意程序等网络安全事件。通过对流量的检测和采集，为上层的深度分析、安全事件发现提供基础的数据支撑。此外，本层通过自研的轻量化车载安全组件在车端的集成部署，为智能网联汽车提供了满足安全准入要求的检测与防护能力。

■ **数据汇聚层:**

实现对车联网多源异构数据的统一汇聚管理，统一调度处理的能力，以及对重要数据、个人隐私数据的安全治理能力。

数据汇入系统包括日志数据采集和全流量数据采集两部分,准实时完成数据的采集上传，并进一步完成数据解析操作。并同时支持资产数据、系统日志等数据的同步导入。

数据包括但不限于面向硬件设备、支撑层（软件信息、开发信息等）、系统层、网络层、应用数据层等信息数据。对接的数据源包括: 与车辆信息系统相关的元数据信息、资产信息，漏洞信息，日志信息，安全设备配置信息，策略信息，威胁情报信息，异常流量信息，已知事件库信息，未知行为检测信息等。

■ **数据计算层:**

为本案例的核心技术层，主要提供的功能包括:

车联网知识库，为车联网大数据分析、应用层的安全运营，提供了丰富的知识图谱。

车联网安全大模型、大数据分析引擎，基于数字孪生、机器学习、人工智能等先进技术，提供核心的智能网联汽车安全风险识别发现能力。

当前广东移动物联网专网安全监测平台实现了对网络中全量车联网流量的监测，并能够提取全量的车联网卡用户流量。本项目当前网络覆盖了包括广汽、比亚迪、小鹏、蔚来、大众、通用等知名车企在内的超过 50 个车型；共监测车联网卡用户日活超过 500 万。

针对智联网联汽车的场景特征，建立了多种安全场景分析模型，主要包括: 用于各种网络安全风险检测的僵木蠕检测模型;用于实时网络攻击检测的基于规则的攻击关联检测模型; 结合车联网专有协议，用于各种场景的未知安全风险的检测模型，如远控业务安全检测模型，OTA 场景安全检测模型，网约车安全风险检测模型，新能源汽车安全检测模型，物流运输车队安全检测模型等等。

基于 Hadoop 集群、数据湖等技术构建了可承载海量车联网数据的数据库，基于分布式文件系统，实现了动态扩容能力。为上层的智能网联汽车安全运营中心、车联网异常行为分析系统提供了可靠的基础的数据存储计算服务。

■ **数据应用层:**

基于数据计算层的分析结果，实现场景化的功能应用，包括面向车企、示范区安全监测运营需求的智能网联汽车安全运营中心，面向运营商、监管支撑的车联网异常行为分析系统。

（3）服务方案介绍

智能网联汽车安全防护与检测: 部署于车辆端的轻量化安全防护与检测组件的主要功能提供网联防护和监测能力、提供车内网络的防护和监测能力、提供 ECU 系统的防护和监测能力。

车联网流量安全检测与分析: 车联网流量安全监测分析系统，可提供如下的安全分析业务包括，网络攻击检测管理、车联网协议检测管理、异常行为监测管理、流量分析监测管理、数据出境监测、攻击溯源分析。

车联网综合安全监测运营: 智能网联汽车安全运营中心，可提供如下的安全运营业务:

- 态势感知: 全局的车辆、网络、IT 设备的运营状态态势分析、统计能力
- 攻击监测: 基于规则的网络攻击事件监测能力
- 异常行为监测: 基于数字孪生、机器学习技术的车辆运行安全、异常行为发现能力
- 资产管理: 提供对“车路云网图”各类资产统一纳管，安全风险分析能力
- 漏洞管理: 提供对车辆、云端系统漏洞的全生命周期（发现、评估、修复、验证）管理能力
- 应急响应: 提供可自定义的安全事件管理能力，自定义的工单管理功能

图 2-3 车联网综合安全运营中心截图

2. 具体应用场景和安全应用模式

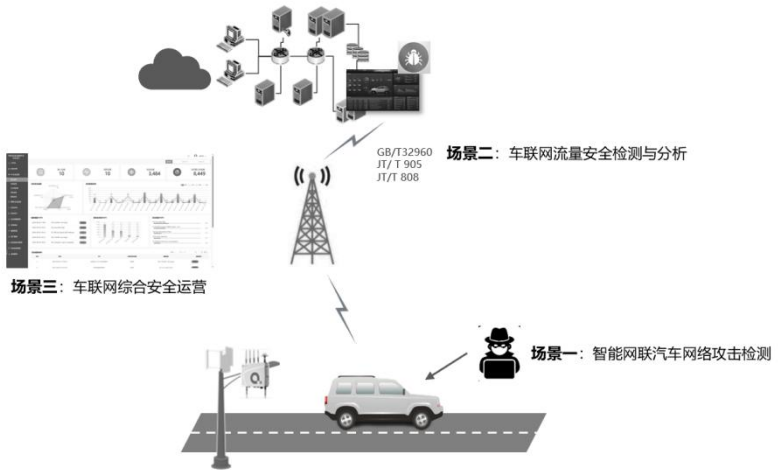

图 2-4 车联网场景图

本案例面向车联网的车端、网络、云端三个关键要素，提供了三个方面的关键服务场景：

➢ 面向智能网联汽车安全防护的场景：基于“轻量化的车端纵深防护技术”为智能网联汽车提供网联、车内、ECU 系统三层级的纵深检测、防护、事件采集能力，满足车企降本增效、安全合规的双重需求，已助力多家车企多款车型通过国际 R155、国内 L3/L4 准入安全合规认证，并与云端安全运营平台形成联动，提供了持续的安全监测、分析、响应处置等运营服务

➢ 面向车联网流量安全分析与检测的场景：基于“车联网安全大模型”打造的“自适应闭环检测”能力，为提联网提供了全流量的安全检测、分析、预警能力，满足车企、城市示范区、电信运营商的安全运营监测需求，国家对车联网行业网络与数据安全的监管数据对接要求

➢ 面向车联网安全运营监测的场景：基于“端到端的车联网数字孪生体”结合机器学习技术，面向车联网各类资产打造了网络安全+运行安全的安全运

场景一：智能网联汽车安全检测与防护

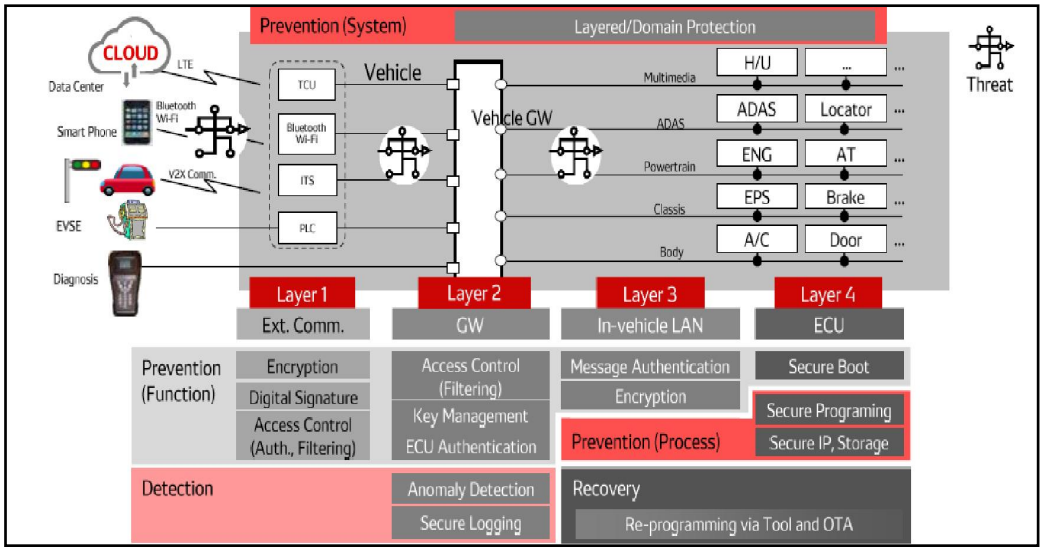

图 2-5 智能网联汽车面临有外及内的安全威胁场景

（1）场景描述

智能网联汽车在对外网联、车内网络、零部件系统面临的网络攻击、总线重放攻击、主机入侵、个人隐私泄漏等全方面的网络信息安全风险，以及远程控车、OTA、数字钥匙等具体业务场景下的安全风险。需要针对网联、车内网、ECU 系统的特征和安全目标，建立合理的安全防护能力。

本案例，基于“轻量化的车端纵深防护技术”的创新思路为智能网联汽车提供网联、车内、ECU 系统三层级的纵深检测、防护、事件采集能力，满足车企降本增效、安全合规的双重需求，已助力多家车企多款车型通过国际 R155、国内 L3/L4 准入安全合规认证，并与云端安全运营平台形成联动，提供了持续的安全监测、分析、响应处置等运营服务

（2）关键技术

依据国际 R155 法规、《GB44495 汽车整车信息安全技术要求》中对”外部连接-通信通道-数据代码-软件升级“的安全要求，由车辆从外至内的网络空间维度出发，通过不同安全技术的互补 、从外到内分层次部署安全防线，满足车辆信息安全防护的**纵深性、均衡性、完整性**的要求。

➢ 车辆网联层：依托车载网联入侵检测、防火墙、身份认证技术，实现对网联网络攻击检测、防御能力，传输数据的加密保护能力，车云连接的身份认证能力

➢ 车内网络层：基于总线入侵检测、SecOC、域隔离技术，实现车内网络通

信数据保护能力，防重放攻击能力

➢ ECU 系统层：通过安全启动、安全存储、应用权限管控技术，实现零部件系统的运行状态检测能力、关键数据\隐私数据的异常检测能力

（3）成果成效

通过在智能网联汽车车端分布式部署轻量化的安全防护与监测组件，实现对车辆网络安全、数据安全风险的有效监测与防护，并通过车端进行安全检测，安全日志上报云端安全运营平台，云端接收安全日志进行安全风险的分析、预警，生成安全防护策略下发车端的“车-云”联动的方式，实现安全事件的实时上报预警，安全规则的实时下发生效的能力。支撑车企可同时满足海外 R155、中国 GB44495 标准、智能网联汽车安全准入的合规需求。

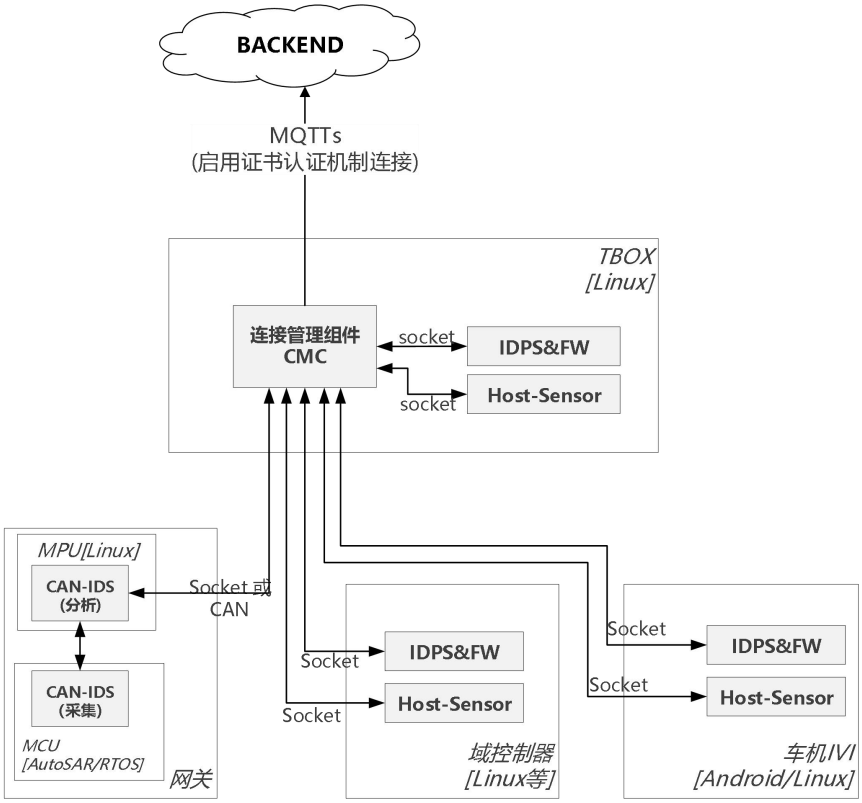

图 2-6 车端安全防护与检测组件的部署架

安全防护与监测组件已在多家车企（广汽、比亚迪、小鹏、蔚来、金龙、大众…）的智能网联汽车上进行了部署应用，支撑车企通过了严苛的国际 R155 VTA 安全认证，检测并防护了上千条车端网络攻击事件。

通过上述业界领先的车规级车端轻量化安全防护技术，车端计算资源占用较传统手段节约 60%，安全检测时延＜200ms，防护效果满足国际 R155 汽车信息安

全法规、中国 GB44495 整车安全强制性标准。

场景二：车联网流量安全分析与检测

（1）场景描述

图 2-7 车联网面临的网络安全威胁场景

由“车、路、云、网、图”组成的车联网车路云一体化系统，安全隐患与威胁到处存在，是运营方必须面对的核心问题。面向车联网井喷式的数据流量，网络指标已不能反映业务质量，车联网业务的保障手段出现不足，部分车联网通道安全性较低，面临着僵木蠕网络攻击、数据违规出境等安全风险，缺乏灵活的流量运营分析手段的现实问题。

本案例，基于“车联网安全大模型”打造的“自适应闭环检测”能力的创新思路，为提联网提供了全流量的安全检测、分析、预警能力，满足车企、城市示范区、电信运营商的安全运营监测需求，国家对车联网行业网络与数据安全的监管数据对接要求

（2）关键技术

基于物联网僵木蠕安全大模型，并结合车联网的业务特征，车联网专有协议，通过与海量车联网数据的识别训练，建立了车联网僵木蠕安全大模型、车联网占有协议检测模型、车联网异常数据/加密流量的检测技术。

➢ 僵木蠕网络攻击、恶意程序安全大模型

- 车联网专有协议分析检测
- 车联网异常数据/加密流量识别分析检测

（3）成果成效

通过借用物联网成熟可靠的僵木蠕安全大模型检测技术，结合对车联网的数据特征进行持续的识别训练，实现了对车联网安全风险的有效识别，建立了车联网质量监测模型，开展车联网业务质量预警。具备核心业务实时预警，投诉问题多域溯源的能力。

依托基于物联网僵木蠕安全大模型的车联网安全风险监测平台，广东移动已成功处置 10 亿/天规模的安全事件 3 次，通用网络攻击 3000 多次，通报出境交互 6 次，有效保护了用户隐私、车企业务和国家安全。

经过将物联网僵木蠕安全大模型技术应用到车联网安全检测上，可支持车联网业务场景＞6 大类，流量采集完整率和准确率 100%，车联网协议识别准确率 ＞95%，特征库规则＞3 万条，隐蔽通道漏判总量＜10%。

场景三：车联网综合安全运营监测

（1）场景描述

图 2-8 汽车综合安全运营场景

无论车企还是城市，面对“车、路、云、网”都需要建立“安全作战地图”，提供持续的安全风险监测、预警能力，具备对网络安全风险的统一管理能力，安全事件、漏洞的全生命周期管控能力，以及应对未知的网络安全风险的能力。

本案例，基于“端到端的车联网数字孪生体”结合机器学习技术的创新思路，面向车联网各类资产打造了网络安全+运行安全监测、预警和响应的安全运营服务。

（2）关键技术

利用数字孪生、机器学习技术，建立智能网联汽车的数字孪生模型，结合车辆运行数据、TSP 数据、车主 APP 数据、车联网流量检测数据等，实现对车辆的网络安全风险检测与分析功能，并针对安全事件处置管理的实际需求，基于 SOAR 自动化编排理念实现了自动化的应急响应管理功能。

- 针对智能网联汽车的数字孪生、机器学习技术
- 自动化的应急响应（SOAR）技术
- 态势感知、安全风险分析监测技术

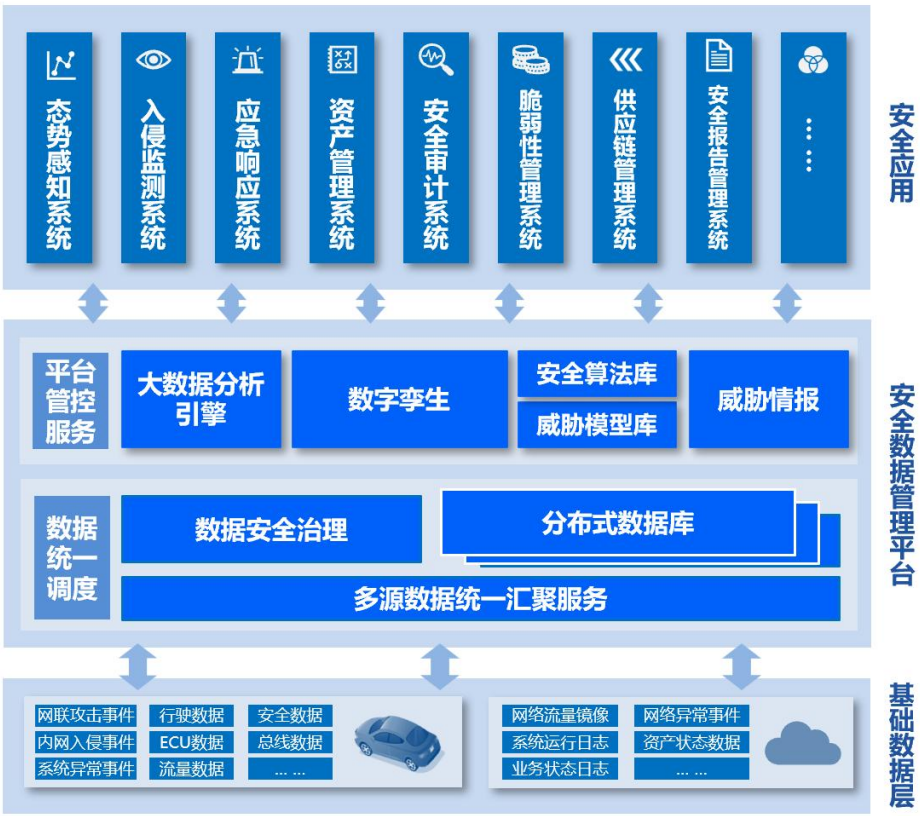

图 2-9 车联网综合安全运营的技术架构

（3）成果成效

通过建立的智能网联汽车的数字孪生模型，结合实际的车辆运行数据、车辆网络安全告警数据、车联网流量数据、车企 TSP 平台数据，可有效识别发现未知的网络安全事件（例如车辆在高速行驶状态下车窗突然开启，则可能是一次网络

攻击问题）。

目前通过建立车辆控制域，车载娱乐域质量监控闭环体系，已预警或溯源疑难问题 50 多起，建立核心业务保障方案 20 多套。

通过建立智能网联汽车的数字孪生模型，提供了业界领先的安全运营监测能力，较传统 SOC 提供预测潜在威胁的能力，威胁场景覆盖＞20 种，分析算法＞10 种，自动化应急响应处置流程＞50 个。

3. 安全及可靠性

本案例充分利用物联网已有的入侵检测、僵木蠕安全大模型、数字孪生等技术，与车联网行业具体场景（车辆 OTA 升级、远程控车、远程诊断、网约车运营、物流车队管理等等）、车联网专有协议、流量特征结合，构建了基础数据支撑、安全检测能力、应用运营服务三个层级的业内领先的车联网安全技术。

（1）基础层面，形成首个车联网行业车联网安全资产库：

建设了覆盖度广、内容全面的车联网安全资产库，涵盖知识、模型、技术三个维度，为车联网安全检测、防护、运营提供了完备的数据和技术支撑。

➢ 车联网知识库方面形成的能力：

1）漏洞及威胁情报：完成和 CNVD、CNNVD、CAVD、CVE 的漏洞平台对接，车联网漏洞数据＞2 万条；

2）资产数据：完成和 50 余车企的车辆、零部件资产对接，车联网车辆资产数据＞50 个，零部件资产数据＞1000 个，IT/网络设施资产数据上千个。

3）其他数据：可实时对接地理信息、天气、路况等数据。

➢ 安全模型库方面：

1）智能网联汽车威胁场景模型，已涵盖：远程控车、OTA 升级、远程诊断、数字钥匙、智能座舱、网约车、物流车队＞20 个场景。

2）车联网威胁场景模型，覆盖：僵木蠕、数据出境、隐蔽隧道、加密数据等检测方向＞6 大类

3）基于数字孪生技术，建立了针对智能网联汽车的场景，覆盖车型 100 余款。

➢ 安全监测能力方面：

1）具备面向智能网联汽车的车联网、车内网、零部件三个层级，10 余种分类的车端监测能力。

2）具备面向车联网网络侧的僵木蠕检测、违规数据检测、加密数据检测、车联网协议检测、隐蔽隧道检测等＞4 大类型分类的监测能力，特征库＞3 万

3）安全运营方面，具备安全监测分析算法＞10 种，自动化响应处置流程＞100 个，完整覆盖对云管端的安全运营管理能力。

通过上述构建的业内领先的车联网安全资产，对车联网行业上安全监测、检测、预警、应急处置提供了完备的技术和数据支撑。

（2）能力层面，打造了业内首个车联网专用安全大模型：

以通义千问安全大模型基座为基础，依托车联网安全知识库打造了车联网安全大模型，具备每日 PB 级的数据处理能力，流量采集完整率和准确率达 100%，车联网风险识别准确率 ＞95%，覆盖车联网业务场景＞12 大类，形成安全资产、安全检测流程的双闭环能力。

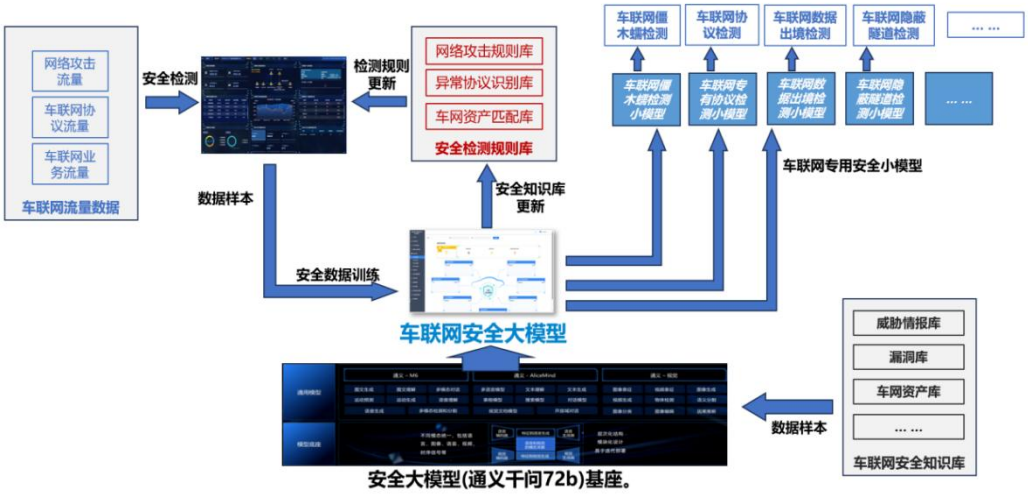

图 2-10 车联网安全大模型，形成安全资产、安全流程双闭环能力

（3）服务层面，提供了从端到云完整的“检测、监测、预警、防御、响应”自适应安全服务闭环：

面向智能网联汽车生产企业、“车路云一体化”城市示范区、基础电信运营商以及行业监管机构提供了从端到云完整的“检测、监测、预警、防御、响应”自适应安全服务闭环。

一是自主研发了车端轻量化的纵深防护产品，采用先进的 SOA 架构实现，对

车端资源占用消耗较传统方案降低 60%，再不增加车企额外的硬件成本前提下，完整提供了端侧“网联->内网->系统”多层级的防护能力，同时满足国内、国际 L3/L4 准入对信息安全的防护需求。

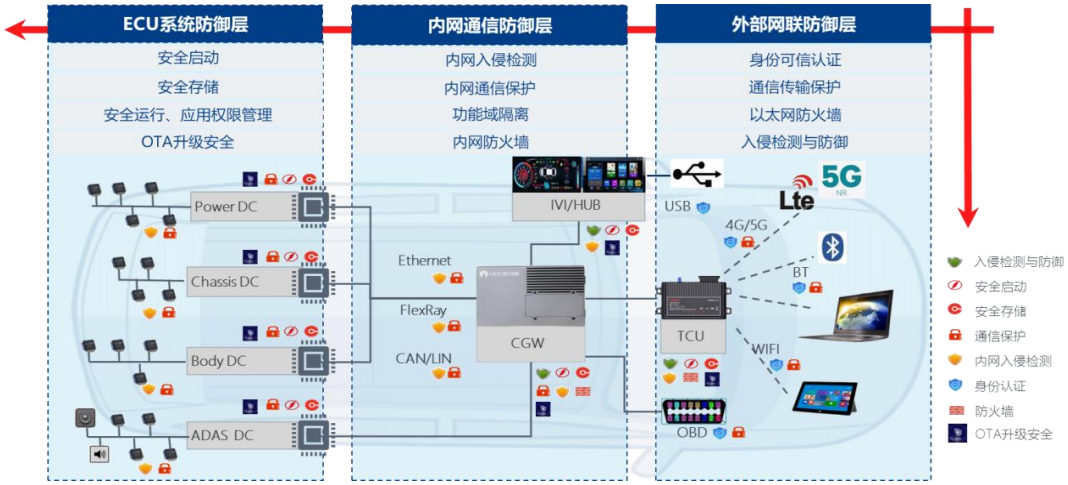

图 2-11 车端轻量化纵深防护矩阵

二是构建了“云-网-端”一体化、协同联动的安全监测服务体系，形成车联网自适应安全闭环管理支撑服务，目前可监测车辆日活数据超过 500 万辆，威胁场景覆盖＞20 种，车联网安全分析算法＞10 种，响应处置流程＞100 种。

图 2-12 基于数字孪生、机器学习技术的车联网安全运营服务

2.2.3 下一步实施计划

1. 技术迭代优化

（一）安全模型持续升级

基于车联网安全大模型，不断扩充其训练数据集。持续收集车联网各类安全事件数据，包括但不限于新型网络攻击手段、车联网协议变种引发的安全问题等，每月新增数据量不低于 100 万条，以提升模型对复杂、多变安全风险的识别能力。

每季度对车联网安全大模型进行一次全面优化升级。引入最新的人工智能算法，如基于 Transformer 架构的改进算法，提升模型对海量车联网数据的处理效率和分析准确性，将车联网风险识别准确率在现有基础上再提升 5%。

针对车联网业务场景不断细化小模型。结合网约车、物流运输等特定场景的业务数据和安全需求，每半年新增至少 2 个专用小模型，实现对不同场景下安全风险的精准检测。

（二）数据处理能力提升

对分布式数据存储系统进行扩容和性能优化。在接下来的一年内，增加 20%的存储节点，提升系统的存储容量和读写速度，确保能够应对车联网数据量的快速增长，保障数据存储的稳定性和高效性。

优化数据汇聚和计算流程。采用更先进的数据调度算法，减少数据处理时延，将数据从采集到分析完成的时间缩短 30%。同时，引入数据预处理技术，在数据采集阶段对数据进行清洗和初步分析，减轻后续计算层的压力。

加强对加密数据和异常数据的分析能力。投入专项研发资源，研究针对加密流量的破解和分析技术，以及对异常数据特征的深度挖掘技术，每季度更新一次相关的检测规则库，提高对隐蔽安全威胁的发现能力。

（三）车端技术改进

持续优化车端轻量化安全防护组件。进一步降低组件对车端计算资源的占用，在现有基础上再减少 10% 的 CPU 和内存占用，同时提升安全检测的速度和准确性，将安全检测时延降低至 80ms 以内。

加强车端与云端的联动响应机制。通过优化通信协议和数据交互流程，实现车端安全事件的快速上报和云端防护策略的及时下发，将从车端发现安全事件到云端下发防护策略的时间缩短至 1 分钟以内。

结合车联网新业务需求，如智能驾驶辅助系统的升级、车路协同业务的拓展等，对车端安全防护技术进行针对性改进，每半年推出一次适配新业务的车端安全防护升级版本。

2. 市场落地推广

（一）拓展客户群体

针对车企市场，组建专业的销售团队，深入调研国内前 20 强车企的安全需求，制定个性化的车联网安全解决方案。在未来一年内，与至少 5 家尚未合作的车企建立合作关系，将车联网安全风险监测服务推广至其智能网联汽车产品中。

积极开拓城市示范区市场。与国内 多家正在推进 “车路云一体化” 建设的城市示范区进行对接，展示项目在车联网综合安全运营监测方面的能力和成果，争取在半年内与 3 个城市示范区达成合作意向，为其提供安全监测和运营服务。

面向基础电信运营商，开展技术交流和合作推广活动。组织行业研讨会，分享广东移动在车联网安全领域的技术经验和实践成果，吸引其他运营商采用本项目的车联网流量安全检测与分析服务，在一年内与至少 3 家省级电信运营商建立合作。

（二）提升品牌影响力

参加国内外知名的车联网行业展会和安全技术峰会，如世界智能网联汽车大会、全球网络安全大会等，设立专门的展位展示项目的技术成果和应用案例，每年参加不少于 5 次此类活动。

与行业内权威媒体建立合作关系，发布项目的最新进展、技术创新和应用成果等新闻稿件，每月发布新闻稿件不少于 2 篇。同时，利用社交媒体平台，如微信公众号、微博等，定期推送车联网安全知识和项目动态，吸引行业关注，提升品牌知名度。

积极参与车联网安全相关标准的制定和修订工作。联合行业内其他企业和机构，推动车联网安全行业标准的完善，增强项目在行业内的话语权和影响力，在未来两年内主导或参与制定至少 3 项车联网安全相关标准。

（三）加强客户服务与合作

建立完善的客户服务体系。为客户提供 7×24 小时的技术支持和咨询服务，设立专门的客户服务热线和在线客服平台，确保客户在使用车联网安全风险监测服务过程中遇到的问题能够得到及时解决，客户满意度达到 95% 以上。

与客户建立长期合作机制。定期对客户进行回访，收集客户的反馈意见和建议，根据客户需求对服务进行优化和改进。每季度组织一次客户座谈会，邀请重点客户参与，共同探讨车联网安全领域的发展趋势和合作方向。

开展客户培训活动。针对不同类型的客户，如车企、城市示范区运营方、电信运营商等，制定个性化的培训方案，为客户提供车联网安全技术培训和服务使用培训，提升客户对车联网安全风险监测服务的认知和应用能力，每年开展培训活动不少于 5 次。

2.2.4 方案创新点和实施效果

1. 项目先进性及创新点

（1）构建了完整覆盖“云、网、端”的自适应安全闭环

总体来看，本案例将“端安全”（轻量化安全防护技术）、“网安全”（车联网专有安全大模型）、“云安全”（端到端的车联网数字孪生体）三个方向的创新技术相结合，与车联网的云、网、车三个层级有机融合，在“端”提供防护、检测、响应能力，在“网”提供网络攻击、车联网场景、协议检测能力，在“云”提供综合的安全分析、安全运营、策略管理下发能力，构建了“云-网-端”协同联动的安全防护体系，为车企、示范区提供了具备自适应闭环安全防护能力的建设与运营服务，为国家监管提供了涵盖从车辆到网络的全面的安全数据支撑。

（2）“端”安全创新：面向智能网联汽车的轻量化安全防护与检测技术

建立的业界领先的车规级车端轻量化纵深安全防护技术，车端计算资源占用较传统手段节约 60%，安全检测时延＜100ms，攻击检出率＞99%，误检率≈0。防护效果满足国际 R155 汽车信息安全法规、中国 GB44495 整车安全强制性标准。

服务场景：车企在不增加智能网联汽车硬件改造成本的情况下，满足其网络信息安全合规准入的要求。

创新性亮点：基于 ICT 行业传统的入侵检测技术，通过对其检测规则、内部

逻辑的优化裁剪、适配车端计算资源不足的现状，做到了资源占用轻量化（CPU占用率从20%降低到5%，内存占用从50MB降低到15MB）的优势，满足在车端零部件资源匮乏的情况下仍可部署的要求。

通过本技术的落地实施，可以在满足车企的智能网联汽车产品在最大限度不增加硬件成本投入的情况下符合安全准入合规的诉求。提供完整满足R155、国家GB44495强制性安全标准要求的车辆网联信息安全防护、检测的需求。

（3）“网”安全创新：基于物联网僵木蠕安全大模型的车联网安全监测分析技术

构建了业内首个车联网安全大模型，可提供日PB级的车联网流量实时检测能力，记录数据以超过5千亿条，流量采集完整率和准确率达100%，车联网协议识别准确率 ＞95%，累计特征库规则＞3万条，覆盖车联网业务场景12大类+，隐蔽通道漏判总量＜10%。

服务场景：针对车联网全流量的深度分析和监测，车联网专有协议的分析和监测，以及数据出境和隐蔽隧道数据的风险监测的场景。

创新性亮点：将基于物联网僵木蠕安全大模型的数据分析检测技术经过适配升级，应用到车联网流量数据的分析和检测场景上，针对车联网业务数据、协议特征进行识别训练，检测发现和车联网相关的网络安全风险。

（4） 云”安全创新：基于数字孪生、机器学习的异常行为检测分析技术

建立了端到端的车联网数字孪生体，与车联网流量、车辆运行、TSP等数据融合，提供业界领先的安全运营监测能力。构建了“车-云”联动防护体系，有效应对未知安全风险，监测车辆日活数据超过500万，汽车威胁场景覆盖＞20种，车联网分析算法＞10种，自动化应急响应处置流程＞100种。

服务场景：为车企、城市示范区运营商提供应对复杂、难以预知的高等级网络安全风险的安全监测、分析和应急响应等运营服务。

创新性亮点：将数字孪生、机器学习技术应用到具体的智能网联汽车业务，为智能网联汽车建立车辆的数字孪生模型，结合车辆的历史数据、实时上报的安全数据、车联网流量数据，TSP平台数据，综合分析后，可提供对潜在的未知网络安全风险的告警检测能力，并通过和车端安全防护与检测组件的联动，形成有

效的安全防护闭环。

2. 实施效果

基于物联网僵木蠕安全大模型的车联网安全风险监测方案推向市场以来，一方面获得了产业界的充分肯定，另一方面也取得了很好的经济效益，相关合同金额已达 2.4 亿元，车联网安全服务获得用户充分认可，具有良好的经济效益和社会效益。

首先，依托本项目构建和积累的车联网知识库、安全模型库、以及建设的安全监测能力，形成了车联网行业有深度、广度的车联网安全资产。

- **车联网知识库方面：**

（1）漏洞及威胁情报：完成和 CNVD、CNNVD、CAVD、CVE 的漏洞平台对接，车联网**漏洞数据＞2 万条**；

（2）资产数据：完成和 50 余车企的车辆、零部件资产对接，**车联网车辆资产数据＞100 个，零部件资产数据＞1000 个**，IT/网络设施资产数据上千个。

（3）其他数据：可实时对接地理信息、天气、路况等数据。

- **安全模型库方面：**

（1）智能网联汽车威胁场景模型，已涵盖：远程控车、OTA 升级、远程诊断、数字钥匙、智能座舱、网约车、物流车队＞20 个场景。

（2）车联网威胁场景模型，覆盖：僵木蠕、数据出境、隐蔽隧道、加密数据等检测方向＞6 大类

（3）基于数字孪生技术，建立了针对智能网联汽车的场景，覆盖车型 100 余款。

- **安全监测能力方面：**

（1）具备面向智能网联汽车的车联网、车内网、零部件三个层级，10 余种分类的车端监测能力。

（2）具备面向车联网网络侧的僵木蠕检测、违规数据检测、加密数据检测、车联网协议检测、隐蔽隧道检测等＞4 大类型分类的监测能力，特征库＞3 万

（3）安全运营方面，具备安全监测分析算法＞10 种，自动化响应处置流程＞100 个，完整覆盖对云管端的安全运营管理能力。

综上，通过上述构建的业内领先的车联网安全资产，对车联网行业上安全监测、检测、预警、应急处置提供了完备的技术和数据支撑。

基于物联网僵木蠕安全大模型的车联网安全风险监测服务已经在广东移动上线，并向广汽、比亚迪等车企赋能输出。该解决方案包括一套应用于车端/路侧设施的轻量化安全防护 SDK、一套部署于车企/示范区的汽车安全运营系统、以及一套部署于运营商网络的车联网安全监测平台，构建车联网三级防护体系。可以对车联网数据进行全覆盖采集，管道侧数据每日千亿级。由于平台采用了业界领先的安全大模型 SecLLM+ 机器学习/深度学习/知识图谱协同驱动的方式，结合 AISecOps 技术对海量数据进行分析和处置，MTTR 从原来的 2 小时减为 30 分钟，每天可处理各类数据超万亿条。可识别车辆已超过 500 万辆/天，覆盖了包括广汽、比亚迪、小鹏、蔚来、大众、通用等知名车企在内的超过 50 个车企。

同时，依托监测平台的车联网安全情报库及车联网核心业务安全分析引擎，数据处理时延从 10 分钟缩短至 1 分钟，模型时延从 1 小时缩短至 15 分钟，并实现了对车辆状态上报、车辆远程启动、OTA 升级、远程救援等核心业务安全情况的深度分析及监测。同时，还通过采用 5G 网络的 MEC+切片能力，实现对隐私数据进行单独隔离，保障数据传输安全。目前，依托基于物联网僵木蠕安全大模型的车联网安全风险监测平台，广东移动已成功处置 10 亿/天规模的安全事件 3 次，通用网络攻击 3000 多次，通报出境交互 6 次，有效保护了用户隐私、企业信息和国家安全。

此外，在面向车联网的网络安全监管支撑上，已经依据《车联网安全管理接口规范》完成接口开发，后续可支撑开展数据报送工作。和国家车联网产品安全漏洞专业库（CAVD）的对接，进行了部分车联网关联漏洞的提交。

图 2-13 安全事件通报及处置闭环管理实际案例

2.2.5 单位基本信息

云百科技主要以物联网技术为载体，依托自身行业耕耘和研发能力，集物联网技术服务，云平台管理和搭建，工业数字化以及智能软硬件定制开发为一体，以 ToB 提供完整解决方案为核心竞争力的的物联网科技企业。云百智能物联车连接数全国第一、5G 智能网联车规模全国领先，为国内新能源汽车智能网联车细分市场龙头。 在车联网平台领域，与中国移动合作，展开 5G+智慧交通、车联网安全态势感知等多个领域上的合作，建设中国移动物联 5G 智能网联管理平台，共同推进车联网技术的发展， 提供标准化车联网接入服务，在汽车 TSP 产业链居于核心地位，上接汽车、车载设备制造商、网络运营商，下接内容提供商，集合了位置服务、Gis 服务和通信服务等技术，为车企提供强大的车联网接入服务。

北京浩瀚深度信息技术股份有限公司致力于成为国内互联网流量和数据智能化的领航者，通过持续探索新技术、新业态、新模式，多年来为中国互联网提供高性能、高精度、高安全、高可靠性的整体解决方案，实现了网络可视、智能管控、数据治理、AI 应用、安全防护和数据价值，是一家集软硬件产品研发、生产、销售和服务于一体的高科技企业。为各行各业提供数据采集、大数据治理、人工智能应用等一体化解决方案。聚焦车联网安全方向，浩瀚具备丰富的车联网安全防护体系建设经验，自主研发了覆盖车端安全防护、车联网安全通信以及面向车路云一体化的安全运营产品，可为车企提供完整满足国际、国内一体化的安全合规建设服务，为城市提供车路云一体化的安全防护建设、持续的安全运营服

务。此外，浩瀚深度积极参与了车联网相关安全标准的制定，具备丰富的监管支撑经验。

中国移动通信集团广东有限公司是国内最早在海外上市的省级电信运营企业之一，也是国内最大的省级通信运营商。近年来，公司保持持续稳健发展，客户数、收入、净利润占中国移动比例约为 1/9、1/8、1/6。在客户规模、收入规模、网络能力和服务水平等方面、均保持了行业绝对领先地位。广东移动采取 700M+2.6G+4.9G 高/低频协同组网策略，累计建成 5G 基站 9.7 万个（2.3 万个 700M），约占全集团八分之一，占全省比例超 50%，5G 网络覆盖率达 96.2%，实现全省县区以上连续覆盖。在打造 5G 精品专网的同时，广东移动设立大湾区创新研究院，紧密结合网络、云、大数据、人工智能、安全、边缘计算、终端、区块链（ABCDNETS）等多种技术，推动行业平台、产品、能力等研究全面体系化，全面提升广东移动在垂直行业的信息化集成、行业产品能力。在网络安全方面，广东移动积极推动实现技术先进、生态发达的高质量发展目标，入选首批工业和信息化部 5G 应用安全创新推广中心，建设物联网僵木蠕，互联网僵木蠕等多个安全监测系统，多个项目入选工业和信息化部网络安全试点示范项目。

斑马网络技术有限公司，立志于用数字化服务汽车全产业链，驱动用户出行体验的创新，成为汽车产业的数字化技术底座和车生活生态平台。作为车内场景交互的平台方，斑马直接打通用户与服务、用户与内容运营提供方，并致力于用户体验的不断优化。斑马面向汽车和交通行业提供智能汽车操作系统、智能汽车解决方案、数字交通解决方案，打造汽车+互联网全球创新的智能汽车解决方案平台，充分协同阿里巴巴集团在语音、视觉、芯片、IoT、云计算、地图、支付、电商等领域技术和生态优势，和车企一起重新定义汽车，为用户打造智慧出行空间，提供智慧驾乘服务和丰富车生活。基于自研 AliOS 打造斑马智行智能汽车解决方案，目前已经合作上汽、一汽、南北大众等车企 10 余个汽车品牌、40 多款车型、100 多万辆智能汽车上。

2.3 案例三：工业互联网 5G 泛终端可信接入实践——筑牢终端管控基石，引领业务数智化转型

引言：5G 的发展促进了实体经济和数字经济深度融合，助推中国新型工业化。随着各行各业数字化转型需求，5G 应用场景竞相绽放。5G 场景离不开 5G 终端的赋能，千行百业涉及的 5G 终端形形色色，不同标准、规格、类型的终端接入给企业带来了不可预知的网络安全风险。

安徽古井集团是中国老八大名酒企业之一，中国制造业 500 强企业，中国第一家同时发行 A、B 两股的白酒类上市公司。近年来，古井集团持续推进战略 5.0，力争建设成为先进制造业与现代服务业深度融合、一体发展的数字化公司。为加快数字化转型发展，古井集团大力挖掘 5G+终端应用场景，并提出打造定制化 5G 专网、集成终端安全管控系统的项目需求。

安徽移动联合启明星辰等二十余家 5G 应用安全产业链企业，为古井集团量身打造“5G+终端安全”全连接工厂。本项目通过定制“网络+终端”一体化应用场景，赋能古井新智能园园区白酒酿造生产全流程。

2.3.1 方案概述

1.方案背景

5G 时代使得更多的工业场景实现了“少人化”和“无人化”，这对信息传输和安全提出了更高的要求，大量智能装备、高清视频、AI、VR 等新技术新装备的运用使得应用现场需要一套功能丰富、高性能、高可靠的无线通信网络。

本项目根据安徽古井集团亳州智慧园区 5G 专网和网络安全建设需求，构造一套适应于生产应用的高可靠性、高安全性的 5G 工业应用专网和泛终端安全接入管控系统，助力古井在智慧制造的领域占据先机，为产业转型、质量提升提供有力支撑。通过网络切片及边缘计算技术，在古井集团部署边缘 MEC 及本地应急 5GC 网络，为企业提供专属覆盖、网络定制、数据隔离、质量保证的基础连接网络，实现适应不同应用需求的大带宽、低时延、安全可靠的数据传输，满足企业生产、办公、管理等应用的通信服务需求。通过部署 5G 泛终端安全接入管控系

统,使古井集团拥有简单而必要的安全自运营能力,满足安全接入策略灵活配置、自主运营等需求，为企业的行业应用及业务创新提供了一体化安全管控平台。

2.方案简介

本项目聚焦安徽古井集团新智能园，通过在园区部署专用 UPF、MEC、传输网络及 5G 工业应用专网企业管理平台，为集团打造专属覆盖、网络定制、数据隔离、质量保证的基础连接网络。同时，部署 5G 泛终端安全接入管控系统，实现对各类终端的可信接入认证、访问控制、风险识别与处置等功能，保障企业网络安全和数据安全。

3.方案目标

全面覆盖智能园区酿造管理中心、成品灌装中心、物流中心等关键区域，确保 5G 信号连续稳定，满足约 8000 台生产设备（含视频监控）的正常连接需求，不限流量，为生产运营提供可靠网络支持。

解决非法终端接入、数据泄露、访问权限混乱等典型安全问题，构建完善的 5G 工业应用专网和泛终端安全接入管控系统，实现终端身份统一管理、多重访问控制、风险识别和处置、行为审计和溯源，满足企业安全合规管理要求。

2.3.2 方案实施概况

本项目围绕安徽古井新智能园 5G 专网及泛终端可信接入展开,深度融合 5G、工业互联网与安全技术,致力于解决企业在智能化转型中的网络连接和安全难题,实现生产效率提升与业务创新。

1. 方案总体架构和主要内容

（1）方案总体架构

采用 5G+MEC 架构打造 5G 专网，通过网络切片及边缘计算技术，在集团部署边缘 MEC 及本地应急 5GC 网络，为企业提供定制化基础连接网络，满足不同业务场景的大带宽、低时延、安全可靠数据传输需求。

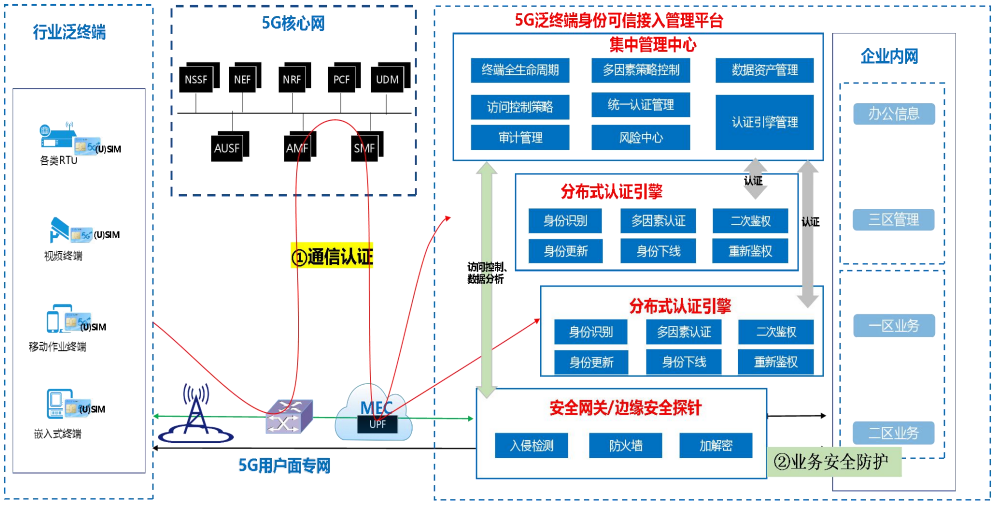

图 3-1 方案总体框架

构建以企业为主导的异构终端多元认证和身份管理体系，增加企业自主控制的二次认证、多因素认证、细粒度权限控制等功能，结合零信任概念，提供持续身份认证和动态访问控制能力。

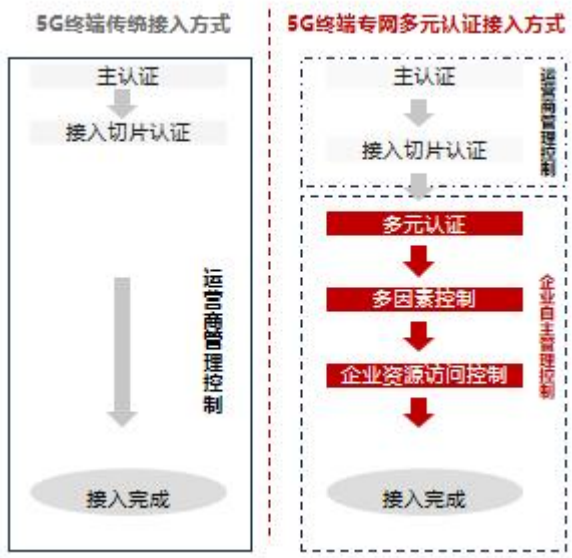

图 3-2 传统认证与多元认证方式

系统架构遵循模块化和可扩展性、可维护性和可测试性、先进性、“三同步”原则，以及与外部系统的集成能力等理念，采用“1+N”技术框架（1 个集中管理中心和 N 个能力组件），实现终端生命周期管理、访问控制、认证策略、风险管理、溯源等功能。

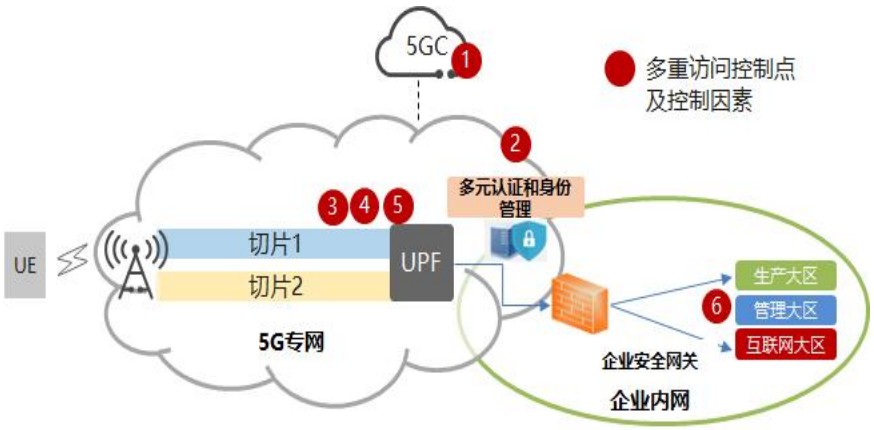

图 3-3 方案组网架构

（2）方案技术方案

● **核心网 5G+MEC**：本项目核心网采用 5GC 控制面复用中国移动大网 ToB 核心网网络，部署 2 套边缘 UPF 下沉至园区内的方案，支持 5G 终端接入数量 20000 个，吞吐量 10Gbps，2 套设备互为容灾，保障业务可靠性。

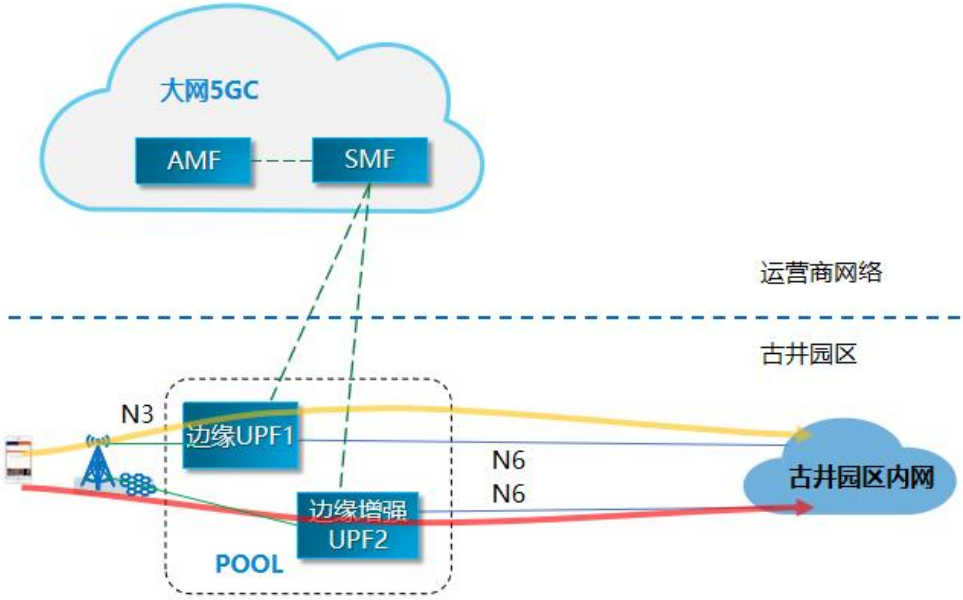

图 3-4 核心网 5G+MEC 方案

在园区内部署的边缘 UPF 设备，包括 1 套边缘 UPF 及 1 套边缘 MEC，其中新建的 1 套边缘 MEC 为 UPF 和 MEP 平台合一部署，满足园区边缘计算能力的需求。园区边缘 UPF 外围接口（N3/N4/OM）通过 SPN 设备开通部署；核心网为客户侧 5G 终端配置专用 DNN，实现远程控制及无人值守业务在 5G 网络的专用隔离；客户业务数据通过园区边缘 UPF 承载，实现数据不出园区，进一步降低数据转发时延。

为古井集团分配独立的切片 ID，大网 AMF 与应急 5GC 均配置支持古井集团专用切片 ID，应急 5GC 仅与园区内的基站互通，应急 5GC 中的 AMF 均向园区内的专属基站注册支持古井集团专用切片 ID，且优先级（Capacity）为 0，园区基站默认将终端注册信令转发给大网 AMF（Capacity 非 0），当大网 AMF 均不可达时，选择 Capacity 为 0 的 AMF。应急 AMF 选择应急 SMF，应急 SMF 为终端创建 PDU 会话，保障古井集团园区业务继续使用。

古井集团园区建设 5G 专网工业环网，配置基站汇聚交换机，用于园区内基站的媒体面数据本地分流。

● **无线网络**：本次古井集团 5G 工业应用专网项目，5G 基站 BBU 设备安装在厂区内的 BBU 集中机房，无线侧根据古井集团厂区内业务带宽的实际需求，以及上行业务的分布情况，采用 2.6GHz+4.9GHz 双频组网模式，部分区域部署 4.9GHz 基站，建设方式方面有宏站、微站、分布式皮站等多种方式，覆盖厂区内各种业务场景。

本次项目主要对古井智能园区酿造管理中心制曲车间，1-6#酿造车间；技术质量 2#制曲实验车间，7#酿造实验车间以及原粮投料运输连廊；成品灌装中心 4 个灌包装车间，物流中心 4 个立体仓库等区域进行 5G 室分系统建设，总计 RRU 室分 153 台。

本次古井集团 5G 工业应用专网项目，无线网基站规划根据古井集团厂区内覆盖场景的不同和业务需求，提供宏基站、微站和皮站等多种建设方式，制定详细覆盖方案，在满足覆盖的前提下，做到节省投资，网络结构的最优化。

● **可信接入功能建设方案**：5G 泛终端身份可信接入系统，包含终端全生命周期管理、认证引擎管理、资产管理、设备与策略管理、审计管理、风险管理等几大重要模块，实现 5G 专网中异构终端的可信多重身份认证、精细化访问控制、安全审计等安全技术的运用，避免 5G 专网中未经授权设备的非法访问，提高网络安全性和可控性。

图 3-5 泛终端身份可信接入系统

2. 网络、平台或安全互联架构

（1）5G 切片网络架构

采用 FlexE 硬隔离+VPN+SRv6 软隔离双重机制构建分层网络架构，划分生产、管理、互联网三大切片：

● 生产切片：独享 25Gbps 带宽，支持行车控制（100Mbps/25ms/3%丢包率）、AGV 调度（5Mbps/100ms/3%丢包率）等时延敏感业务。

● 管理切片：10Gbps 带宽，承载 ERP、MES 等企业管理系统。

● 互联网切片：5Gbps 带宽，通过防火墙实现最小化访问控制。

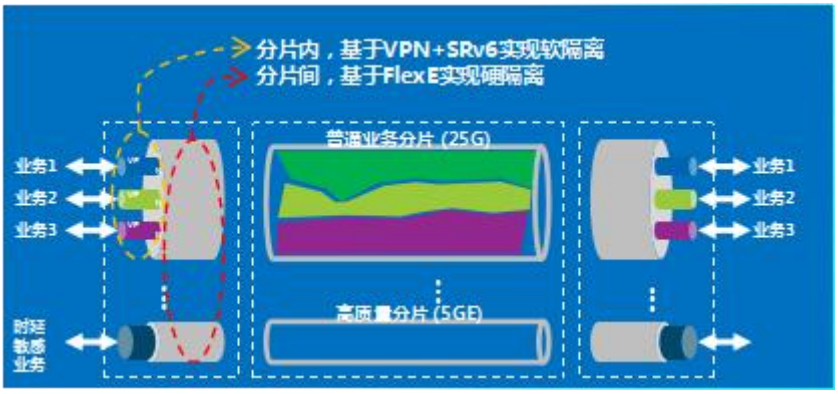

图 3-6 5G 切片

● 技术实现：

分片间隔离：基于 FlexE2.0 技术实现物理层隔离，支持 100Gbps 带宽分片。

分片内隔离：采用 VPN+SRv6 技术实现逻辑隔离，支持 20000 终端并发接入。

本地分流：边缘 UPF 配置专用 DNN（古井专网），实现生产数据 100%不出园区。

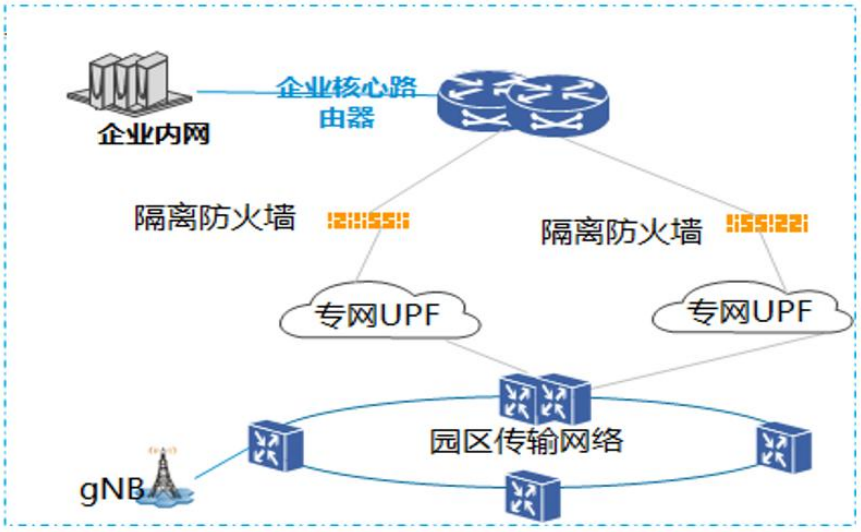

图 3-7 专用 UPF 独享数据通道

（2）终端接入认证架构

基于 3GPP 二次认证标准，构建运营商主认证+企业二次认证双链路体系。

● 主认证流程：

终端通过 SIM/IMSI 完成运营商 5G 核心网认证，认证成功率≥99.5%，支持双向鉴权防止伪基站攻击。

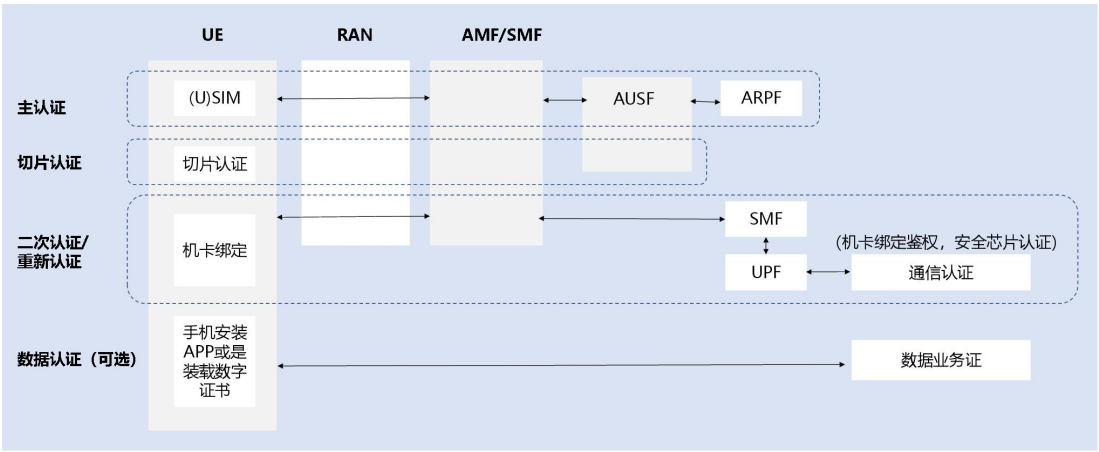

图 3-8 5G 泛终端可信接入认证流程

● 二次认证流程：

终端访问企业内网时，触发 IAM 平台“无感知”认证。

多因子验证：SIM 卡+设备指纹（IMEI/MAC）+动态令牌

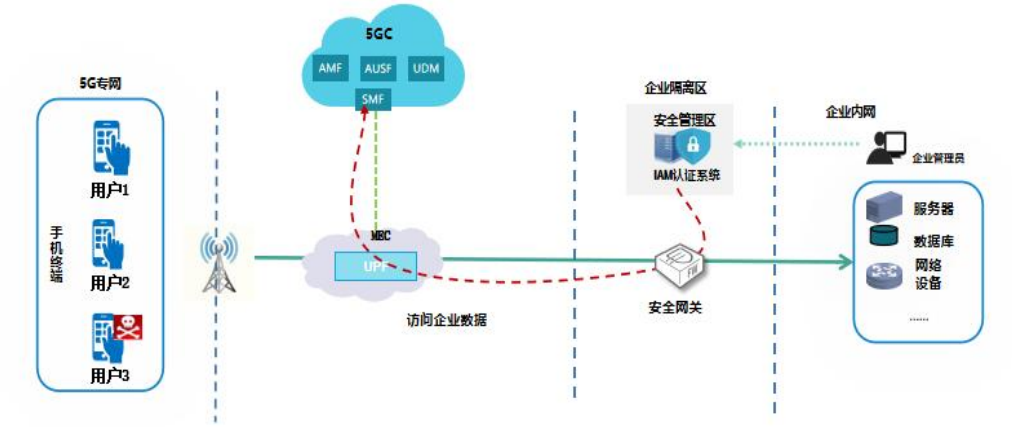

图 3-9 终端风险识别流程

动态策略：结合 GIS 围栏、时间窗（如夜间禁止高危操作）、终端健康状态（病毒检测结果）动态调整权限。

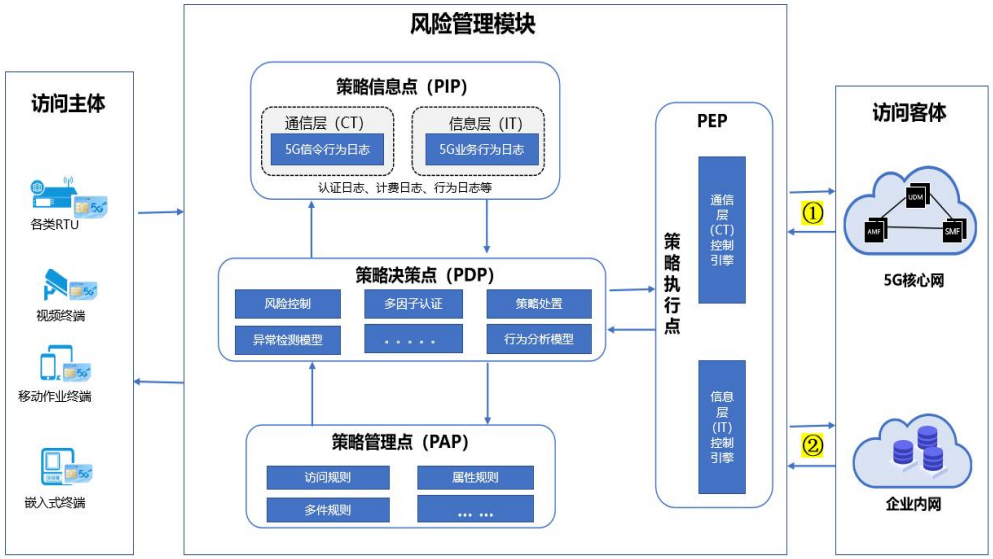

图 3-10 终端接入认证管控系统风险管理

3. 具体应用场景和安全应用模式

1）5G+AGV 无人制曲

● 部署方案：

为 200 台 AGV 配置专用 DNN（古井专网），通过边缘 UPF 实现本地分流，保障 100ms 控制时延。

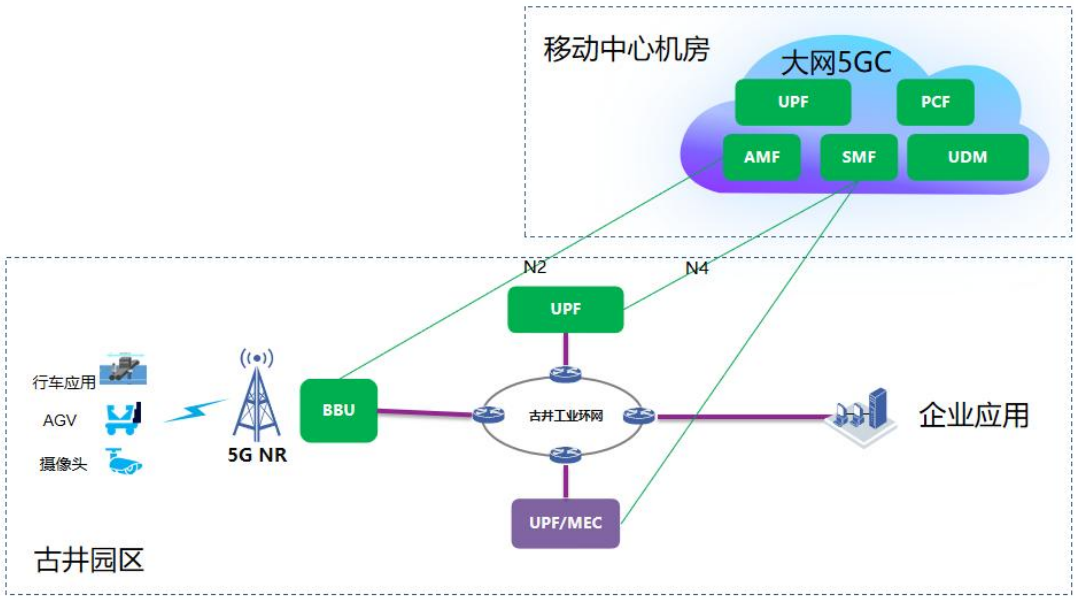

图 3-11 整体方案网络架构

网络配置：AGV 终端采用 5GPLC 通信，支持 2.6GHz+4.9GHz 双频接入。

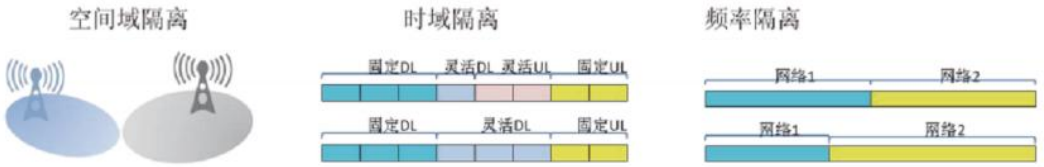

图 3-12 无线隔离

数据交互：AGV 实时上传位置、载重数据至 MEC 平台，支持路径优化算法。

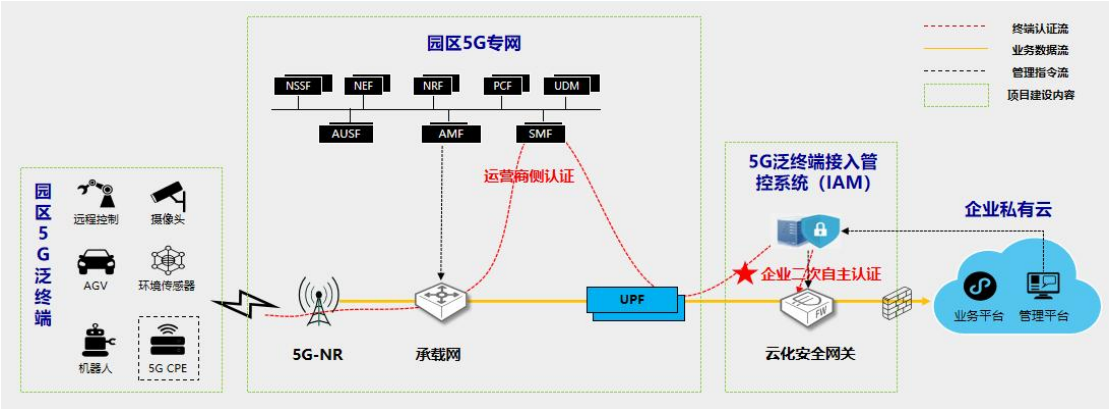

图 3-13 园区 5G 泛终端

● **数据价值挖掘：**

基于 AI 算法分析 AGV 运行轨迹，优化制曲车间物流路径，减少无效行驶里程 20%。结合 MES 系统数据，动态调整 AGV 调度策略，订单完成效率提升 30%。

● **安全应用模式：**

动态权限控制：结合 GIS 围栏，限定 AGV 在酿造车间 1-6#区域活动，越界自动触发断网。

异常行为阻断：部署边缘安全探针，实时监测 AGV 终端 Root 状态、异常流量，发现病毒感染立即通过 CoA 指令断网。

操作审计：AGV 操作日志通过区块链存证，支持生产流程回溯。

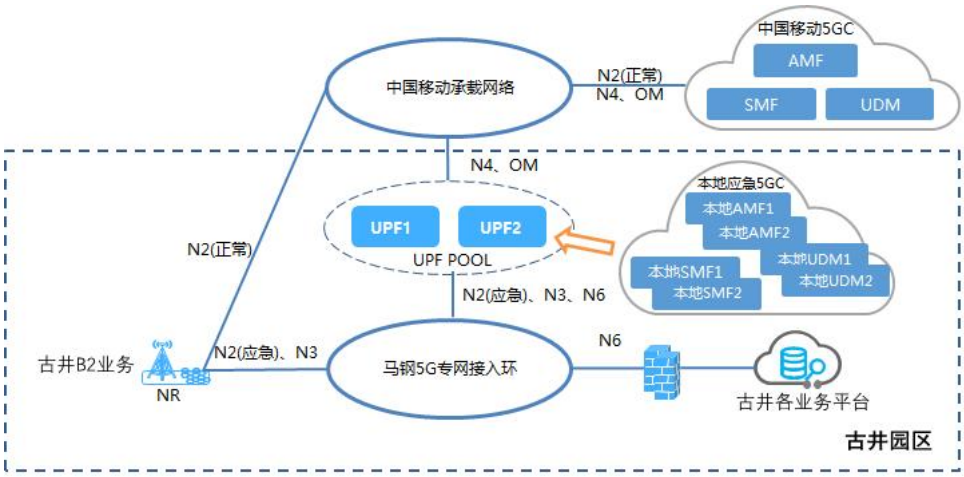

图 3-14 UPF 外部接口需求

● **实施效果：**

AGV 路径规划效率提升 40%，单台能耗降低 15%。非法越界事件下降 98%，未发生因终端感染导致的生产事故。

2）5G+智能仓储

部署方案：

4 个立体仓库部署 5G 机械臂（支持 200Mbps 带宽）和 5GPLC，通过 MEC 实现仓储数据实时分析。

网络配置：采用 5GLAN 技术实现设备间低时延通信，支持 2000 终端并发接入。

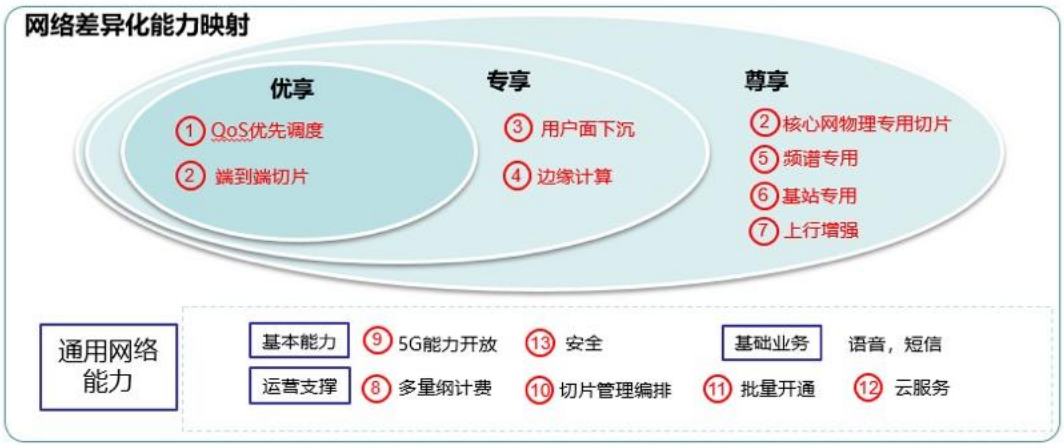

图 3-15 中国移动 5G 专网差异化服务网络

数据应用：AI 算法分析货物堆放密度，动态调整机械臂作业策略。

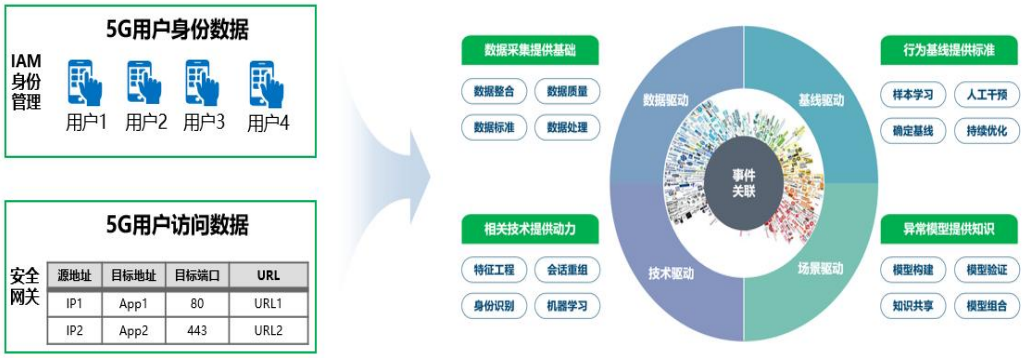

图 3-16 终端行为审计和溯源

● **数据价值挖掘：**

集成 WMS 系统数据，实现库存智能预警，滞销品周转周期缩短 45%。通过数字孪生技术模拟仓储布局，拣货路径优化减少人力成本 25%。

● **安全应用模式：**

访问控制：基于 RBAC 模型，为不同岗位人员分配差异化权限（如仓管员仅可操作指定区域机械臂）。

数据加密：仓储操作指令通过国密 SM4 算法加密，密钥生命周期≤24 小时。

异常检测：部署全流量管理系统，实时识别恶意扫描、敏感数据外传等行为。

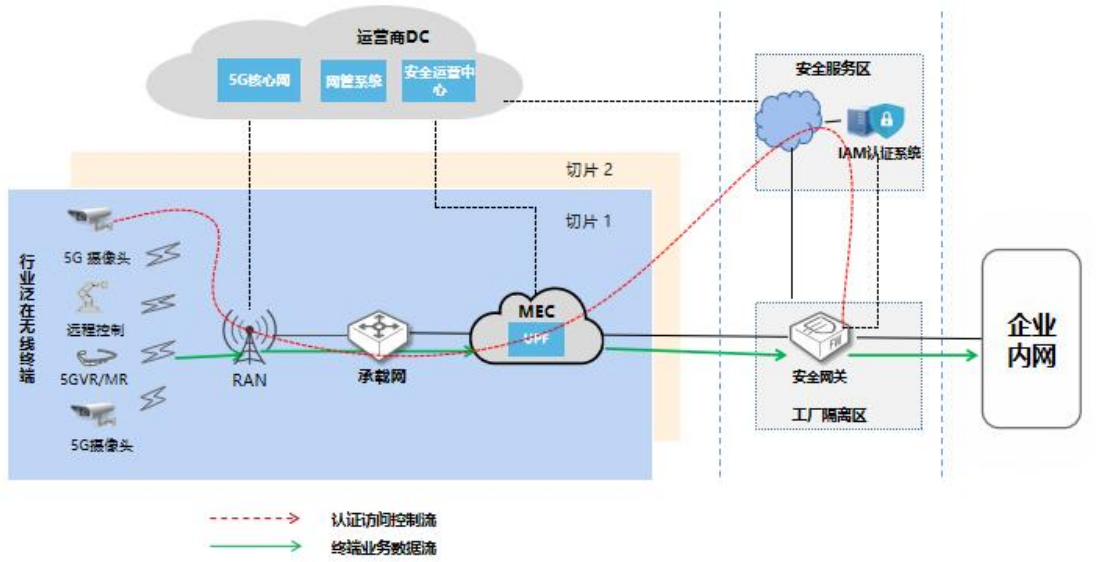

图 3-17 5G 专网+终端接入认证管控系统组网

● **实施效果:**

仓储盘点时间从 4 小时缩短至 1.6 小时，库存准确率提升至 99.99%。敏感数据泄露事件归零，网络攻击拦截率达 100%。

3）酿造车间行车控制

● **部署方案:**

12 台行车配置 5GDTU，通过 UPF 实现 100Mbps/25ms 低时延连接。网络配置采取专用生产切片保障带宽，支持双链路冗余。

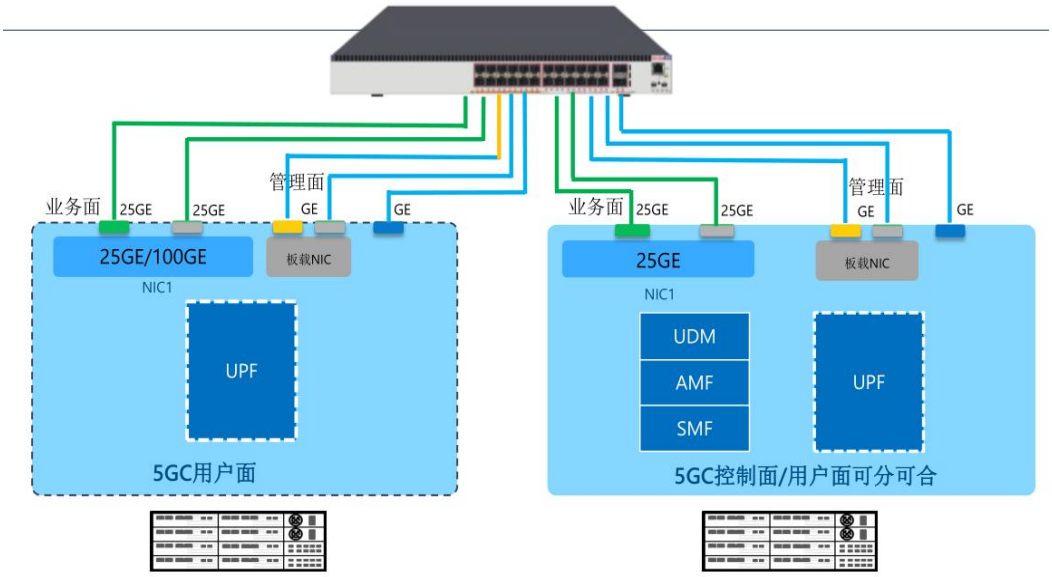

图 3-18 UPF 内部组网

● **数据价值挖掘:**

实时采集行车运行参数（如速度、载重），通过机器学习预测机械故障，维护成本降低 22%。结合生产订单数据，动态调整行车作业优先级，生产计划达成率提升 18%。

● **安全应用模式:**

双向认证: 行车终端与 MEC 平台通过双向证书认证，防止伪冒设备接入。

时延监控: 部署网络质量监测系统，时延超过 25ms 时自动切换备用链路。

● **实施效果:**

行车控制故障率下降 75%，生产事故响应时间从 30 分钟缩短至 5 分钟。

4. 安全及可靠性

本项目构建了涵盖“终端-网络-平台”的立体化安全防护体系，融合多重创新技术，达成了工业级安全可靠性标准，具体如下:

1）身份认证安全

● **多因子认证机制**

采用“SIM 卡+设备指纹（IMEI/MAC）+动态令牌”三重认证，认证成功率≥99.5%。

双向认证: 终端与网络相互验证身份合法性，有效防范伪基站攻击。

动态策略: 结合 GIS 围栏、时间窗（如工作日 9:00-18:00 开放高危操作权限）和终端健康状态（病毒检测结果）实施动态授权。

● **终端可信根技术**

部署启明星辰可信终端模块，实现终端硬件级身份绑定，防止篡改。支持安全启动（SecureBoot），确保终端固件完整性。

2）数据安全

● **切片隔离与加密**

生产、管理、互联网切片通过 FlexE 硬隔离+VPN+SRv6 软隔离，保障业务独立性。敏感数据传输采用国密 SM4 算法加密，密钥生命周期≤24 小时。

● **全流量审计与分析**

部署全流量管理系统，实时监测 HTTPS 加密流量。支持恶意文件检测、

Webshell 识别，威胁拦截率达 99.9%。

3）网络可靠性

● 冗余架构设计

核心网：双边缘 UPF 热备，单套支持 10Gbps 吞吐量、20000 会话，故障切换时间<50ms。

无线网：2.6GHz+4.9GHz 双频组网，宏站+室分混合部署，边缘速率≥100Mbps。

● 容灾备份机制

采用独立存储、计算、网络资源，支持虚机热迁移、存储热迁移。

数据备份策略：生产数据每日增量备份，关键数据异地容灾。

4）合规审计

● 全生命周期审计

终端访问行为日志通过区块链存证，支持：

操作记录不可篡改，保存期限≥6 个月（公安部等保要求）。

AI 异常行为分析，误报率<0.1%。

● 等保合规性

通过公安部“天榕统一身份认证系统 V6.0”三级等保认证，满足：

身份鉴别失败处理（A 级）。

审计跟踪（B 级）等要求。

5. 其他亮点

1）行业专网差异化能力定制

● 尊享服务模式：

提供“专属基站+核心网物理隔离”的 5G 专网尊享服务，支持：

无线频谱专用（4.9G 频段），避免与公网干扰，上行峰值速率达 2.5Gbps。

核心网独立部署，实现 20000 终端并发接入，满足白酒生产全场景需求。

● 按需扩展架构：

采用虚拟化架构，支持硬件资源动态扩容，单节点故障不影响业务连续

2）5G+工业互联网融合创新

● 全要素可信连接：

实现终端身份、位置、行为三维验证，非法接入率下降 98%。结合 GIS 围栏技术，限定终端在厂区 300 米范围内访问生产系统。

● **数字孪生应用:**

基于 MEC 平台构建仓储数字孪生系统，支持:

实时模拟仓储作业，优化机械臂调度效率 25%。

虚拟环境中测试新业务流程，降低试错成本 40%。

3）自主可控安全体系

● **微服务化认证架构:**

采用微服务拆分技术，将认证、授权、审计解耦，支持:

独立扩展认证协议（如新增生物识别），无需重构系统。

单节点故障不影响整体认证，系统可用性达 99.999%。

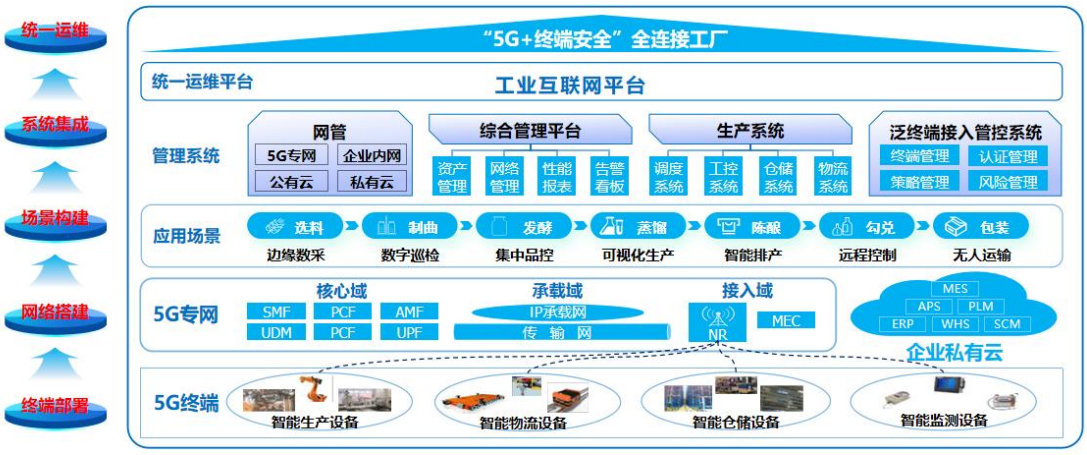

图 3-19 方案总体框架

● **国产化安全组件:**

部署启明星辰国产化防火墙、入侵防御系统（NIPS-1000-B1400），实现恶意流量拦截率 100%，误报率<0.1%。

2.3.3 下一步实施计划

1. 5G+AI 酒体质量检测系统部署

1）目标

➢ 2025 年完成 5G 视觉检测系统试点，实现酒体杂质检测自动化，提升质量

一致性。

2）实施步骤

➢ 部署 5G 高清摄像头（支持 200Mbps 带宽）于灌装生产线，实时采集酒体图像。

➢ 利用 MEC 平台运行 YOLOv5 目标检测模型，识别杂质。

➢ 集成至 MES 系统，自动剔除不合格产品，生成质量分析报告。

3）预期成果

➢ 检测效率提升 50%，误检率降至 0.01%。

➢ 减少人工检测成本 30%，酒体合格率提升至 99.99%。

2. 5G+AI 酒体质量检测系统部署

1）目标

➢ 2025 年引入 AI 安全检测模型，开展季度攻防演练，提升系统抗攻击能力。

2）实施步骤

➢ 部署启明星辰 AI 安全检测平台，实时分析流量异常。

➢ 每季度联合公安部第三研究所开展红蓝对抗演练，模拟 APT 攻击、0day 漏洞利用等场景。

➢ 根据演练结果优化安全策略，更新威胁情报库。

3）预期成果

➢ 威胁检测准确率提升至 99.99%，响应时间缩短至 10 秒内。

➢ 通过公安部“增强级”等保认证，成为白酒行业安全标杆。

2.3.4 方案创新点和实施效果

1. 方案先进性及创新点

1）5G 原生安全架构创新

● **3GPP 二次认证技术:**

基于国际标准协议，在 SA 组网模式下实现“无感知”企业自主管控，解决传统专网无法自主控制终端接入的问题。

● **双向认证+多因子验证:**

终端与网络相互验证身份，结合 SIM 卡、设备指纹、动态令牌三重认证，非法接入率下降 98%。

2）动态风险控制模型

● **CT/IT 双维度行为分析:**

整合 5G 信令日志与业务行为数据，构建自适应访问控制模型，实时阻断异常终端。

● **零信任架构应用:**

采用“永不信任，持续验证”机制，每次访问均需重新认证，威胁拦截率达 100%。

3）全要素可信连接

● **三维验证体系:**

终端身份、位置、行为三维验证，结合 GIS 围栏技术，实现厂区 300 米范围内精准授权。

● **区块链存证技术:**

操作日志通过区块链存证，确保数据不可篡改，满足等保合规要求。

4）行业专网定制化能力

● **FlexE+SRv6 切片技术**

实现物理层+逻辑层双重隔离，支持 20000 终端并发接入，带宽利用率提升 40%。

● **4.9G 频段独享方案**

结合超级上行技术，上行峰值速率达 2.5Gbps，满足大上行业务需求。

2. 实施效果

1） 生产效率提升

● **5G+AGV 无人制曲**

➢ AGV 路径规划效率提升 40%，单台能耗降低 15%。

➢ 生产订单完成周期从 48 小时缩短至 32 小时。

● **5G+智能仓储**

➢ 仓储盘点时间从 4 小时缩短至 1.6 小时，库存准确率提升至 99.99%。

➢ 拣货路径优化减少人力成本 25%。

2） 安全防护增强

● 终端安全

➢ 非法接入率从 2.3%降至 0%，终端感染病毒事件归零。

➢ 敏感数据泄露事件归零，网络攻击拦截率达 100%。

● 网络安全

➢ 切片间隔离度≥99.99%，满足工业级安全要求。

➢ 双 UPF 容灾切换时间<50ms，保障业务连续性。

3）成本优化与创新

● 运维成本:

➢ 单终端运维成本从 800 元/年降至 400 元/年，年节省成本 400 万元。

➢ 网络时延敏感业务故障率下降 75%，生产事故响应时间缩短至 5 分钟。

● 创新价值:

➢ 数字孪生技术优化仓储布局，减少试错成本 40%。

➢ 主导编制行业标准，带动产业链产值增长 20%。

2.3.5 单位基本信息

安徽古井集团有限责任公司是中国老八大名酒企业，中国制造业 500 强企业，是以中国第一家同时发行 A、B 两只股票的白酒类上市公司安徽古井贡酒股份有限公司为核心的国家大型一档企业。

古井集团持续推进战略 5.0，力争建设成为先进制造业与现代服务业深度融合、一体发展的数字化企业。引入物联网、大数据和 AI 技术，将传统酿造工艺与现代智能设备结合，构建以“1 个战略+2 个底座+6 大能力+N 个平台应用”为核心的工业互联网体系，打造的“固态白酒智能化酿造 5G 工厂”被列入《2024 年 5G 工厂名录》。

古井集团以“做中国最受欢迎、最受尊重的白酒企业”为愿景，秉持“质量为天”的生产理念，致力于传承与创新中国白酒文化。古井积极履行社会责任，

助力中小企业数字化转型，注重绿色发展与社区共建，践行“贡献美酒、造福社会”的核心价值观

2.4 案例四：基于 5G 专网的可信数据空间安全解决方案——跨网络的“一站式”安全可信体系

引言：本方案根据当前面临的网络安全复杂形势和某新能源企业发展战略，设计安全解决方案，提高工业企业在网络安全监测管理、态势感知、应急响应等方面的安全能力，增强工业网络的全面安全监控和防护水平，建立有效的安全事件响应和处理机制，通过分析多源数据，提升安全分析和决策的智能水平。中国联通研究院建设的安全管理方案围绕网络可信、终端可信、数据可信的核心展开，旨在构建一个全面、智能、可信的工业网络安全可信体系，确保工业环境在面对日益复杂的网络威胁时能够保持稳定和安全，确保工业网络安全的全面性，为 5G 工厂的安全建设提供指导和示范。

2.4.1 方案概述

1.方案背景

工业企业通过打造 5G 专网，以实现工厂设备的全面无缝连接，并通过 5G 网络的高速率和低延迟特性，提升 PLC 数据采集效率，优化运维管理。工厂通过部署 AGV 自动化搬运系统和 AI 质检技术，以及利用 5G 网络实现仓储管理系统的智能化，从而优化库存管理和物流调度。工厂转型推动了产业从自动化向数字化、智能化的升级，也显著提高了生产效率和产品质量。面对传统 IT 网络和工业控制 OT 网络逐渐融合、互通互联，工业企业网络攻击面随之扩大风险不断上升。

为贯彻落实《中华人民共和国网络安全法》、《工业控制系统网络安全防护指南》、《信息安全技术网络安全服务能力要求》、《关键基础设施安全保护条例》等法规要求，应对工业网络的安全挑战主要包括以下几种，首先，设备终端众多且种类繁杂，工业互联网终端设备计算能力和安全防护措施较弱；其次，5G 网络的服务化架构使网络功能以通用接口对外呈现，可以实现灵活的网络部署和管理，但通用接口在身份认证、访问控制、通信加密等方面面临潜在的风险；最后，数据安全风险多样化，数据安全管理责任界定不明，网络边缘数据隔离与保

护的挑战明显。针对这些问题，中国联通研究院提出了一套针对性的工业网络安全解决方案，旨在加强工厂的网络安全防护。

2.方案简介

根据当前面临的网络安全复杂形势发展战略需求，基于定制 5G 专网，构建基于 5G 专网的可信数据空间安全解决方案，实现终端安全、内网安全、数据跨域交互安全等安全应用场景。

工业网络安全方案围绕终端安全、组网安全、数据安全核心展开，本方案旨在构建一个全面、智能、自适应的工业网络安全体系，确保工业环境在面对日益复杂的网络威胁时能够保持稳定和安全，确保工业网络安全的全面性。

3.方案目标

（1）建设工业互联网终端可信安全能力

在工业环境中，终端设备数量庞大且种类繁多，企业终端设备管理面临挑战，资产管理混乱和资产信息不明确导致未授权访问和非法连接等终端安全管理问题频发。目前，公司缺乏有效的终端接入管理机制，无法识别终端身份，且网络接入的终端数量与实际业务需求的终端数量不一致。为了全面掌握公司接入终端的详细信息，防止未授权设备接入网络，依托 5G 专网部署终端访问控制措施，有效减少恶意软件的传播和数据泄露风险，确保生产流程的连续性和安全性，保护关键资产，优化资产管理流程，提升整体运营效率。

（2）建设工业互联网组网可信安全能力

在智能制造和企业数字化转型的推进下，工业企业 OT 网络与 IT 网络正在逐步实现融合和互通，设备间的信息交换变得更加频繁。目前，公司工厂的现场网络结构复杂，涉及有线网络、5G 网络以及混合专网混用，各网络的防护策略不一致，缺乏对网络流量的深入威胁分析，难以及时发现和应对潜在的安全风险。为了提升企业的网络安全防护能力，并确保业务数据的安全，不外泄至园区外，通过构建融合 5G 网络和生产网络的微隔离和访问控制体系，实现业务间的逻辑隔离，增强网络边界的防护能力。推动 5G 定制网络中关键技术的安全可控发展，为公司网络安全和业务连续性提供强有力的保障。

（3）建设工业互联网数据可信安全能力

在多个参与方的工业数据交互场景中，数据的所有权、处理和使用权利界定模糊，对数据使用的管控措施不足，潜在引发数据滥用和安全问题。为解决数据权属不清的问题，通过部署 5G 专网、建设工厂内部跨网数据安全交互和云化工业数据安全交换，实现数据在园区内部封闭流转、精细化区域管控和数据隔离安全交换，有效提升工业数据交互的安全性和管控效率。

2.4.2 方案实施概况

通过部署 5G 专网，实现设备全面互联，促进其生产线从自动化向数字化和智能化的升级。针对企业痛点，落实网络安全、访问控制和数据安全的安全需求，依托核心技术和 5G 专网安全能力，构建可信数据空间安全体系，确保工业控制网络的安全性，提高对安全事件的监控能力，实现网络的持续稳定运行，增强态势感知，并优化安全运营的管控效率，全面把控工厂生产安全。

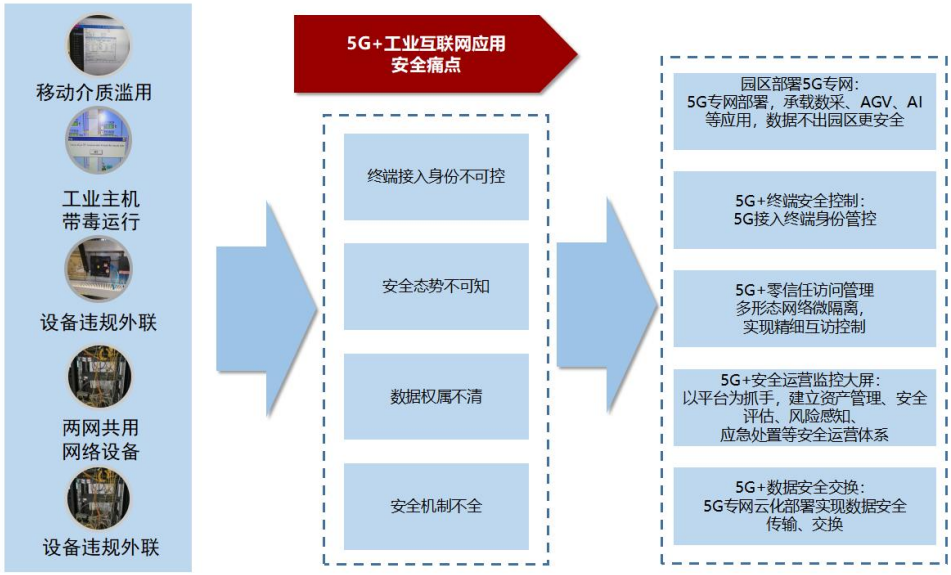

图 4-1 工业网络安全需求图示

1.方案总体架构和主要内容

（1）方案总体架构

项目将从终端接入可信安全、网络可信安全、数据可信安全维度，依托 5G 和可信技术能力，围绕企业对工控网络安全、设备安全及数据安全需求，通过终端可信安全接入、网络可信安全和数据可信安全等技术手段，构建覆盖全链条的动态化安全防护体系。

图 4-2 项目总体架构

2. 网络、平台或安全互联架构

（1）终端可信安全

1、5G DTU 接入认证及绑定

为了确保特定终端能够安全接入指定网络，在 5G 专网接入侧，提供首次登网时的机卡绑定验证，以及终端登网签权认证，确保只有授权的终端能够接入网络。终端锁小区和锁频点功能，进一步限制非法终端的接入。为了验证接入终端的可信度，通过物联网卡叠加 GBA 安全通信服务，利用 5G 专网向网关签发 CA 数字证书，生成“一事一密”的专用会话密钥，以供上层业务加密通信使用。

图 4-3 5G 终端首次登网机卡绑定

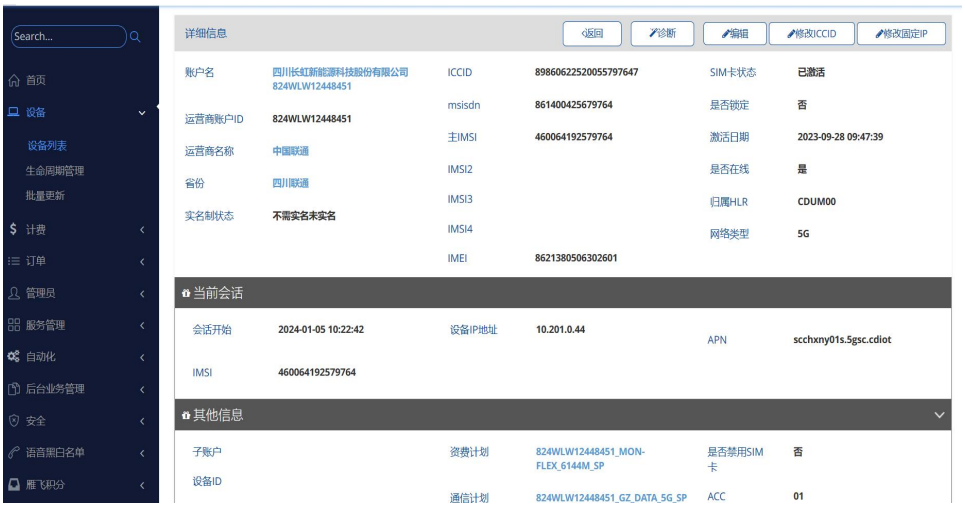

图 4-4 5G 终端登网签权认证

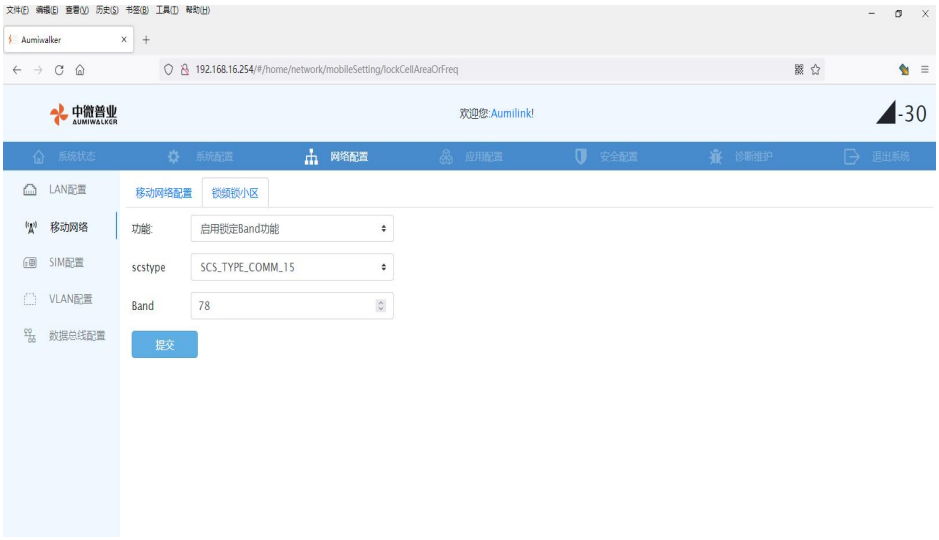

图 4-5 5G 终端锁定登网小区

我们所采用的创新型终端网络接入认证强化机制，是一种多维度、多层次的认证体系。首先，会综合运用多种身份验证因素，除了常规的用户名和密码外，还引入数字证书以及设备唯一标识等信息进行联合认证。比如，一台工业物联网终端设备在接入 5G 专网时，不仅要输入正确的预设密码，还需要出示与之匹配的数字证书，该数字证书中包含了设备的生产厂商、型号、序列号等关键信息，经过网络侧的严格验证，确保设备来源合法、身份真实。

同时，针对不同安全等级的终端设备，会设置差异化的接入认证流程。对于涉及高敏感数据的终端，在接入时会增加额外的动态口令验证环节。动态口令会通过专门的安全通道实时发送到终端设备管理员的移动端上，只有输入正确的动态口令，终端才能成功接入网络，大大提升了高风险终端接入的安全性。

而且，在认证过程中，会实时监测终端设备的网络环境。如果检测到终端是从未知的、存在安全风险的网络区域发起接入请求，系统会自动提高认证的严格程度，要求终端提供更多的辅助证明信息，如设备近期的安全检测报告等。

2、动态可信数字身份平台

5G 核心网通过动态可信数字身份平台增强终端接入安全，运用融合 5G 的终端接入动态可信数字身份平台，实现身份管理、模板管理、密钥管理、验证授权、存证确权和 SDK 能力，实现对设备 VC 信息的统一验证和管控。仅允许符合特定条件的行业终端接入，条件包括终端标识（如 IMSI/SUPI）、终端位置（如 CGI、TAI）、IMEI 黑名单、流量限制以及机卡绑定等，提供 CMP 平台进行自我管理，以提高网络接入的灵活性和安全性。

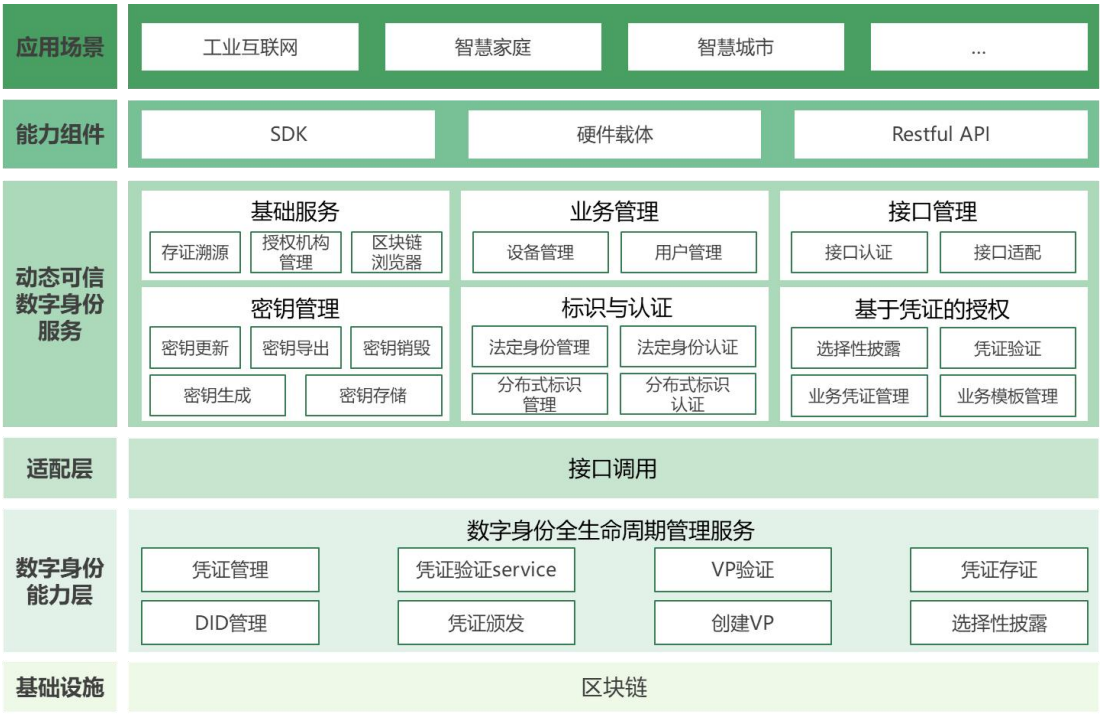

图 4-6 动态可信数字身份平台

- 身份管理：提供设备身份标识创建、凭证 VC 更新和撤销等功能；
- 模板管理：提供设备 VC 信息模板建造能力，可对同类设备建统一模板；
- 密钥管理：支持身份的公私钥生成，更新，销毁，导出等功能；
- 验证授权：提供人和物、物和物彼此之间身份的验证和授权功能；
- 存证确权：支持上传文件，并在链上存证，具备数字身份和哈希数据；
- SDK 能力：封装标识创建、身份认证、身份授权等多项功能 SDK 服务。

随着网络环境的瞬息万变，仅仅依靠静态的网络安全防护措施对于终端设备来说远远不够，我们在终端网络安全态势感知与自适应调整方面进行了创新性实践，为终端可信保障中的网络可信增添了有力的支撑。

我们的终端网络安全态势感知系统犹如一张无形的 “安全网”，它通过在终端设备上部署轻量级的传感器以及在网络侧设置集中式的分析平台，实时收集终端设备的各种网络相关信息，包括设备的连接状态、网络接口的使用情况、正在传输的数据特征以及周边网络环境的变化等海量数据点。

利用机器学习和人工智能算法，对这些收集到的信息进行深度挖掘和分析，构建出终端设备的网络安全态势画像。例如，对于一个物流仓库中的 5G 终端设备群，系统可以清晰地描绘出每个叉车控制终端、货物扫码终端等的网络安全状况，是处于安全稳定状态，还是存在潜在的安全风险，如受到周边不明信号干扰、有可疑的网络扫描行为等情况都能精准呈现。

一旦发现安全态势出现异常变化，比如检测到某个终端设备周围的网络攻击频次增加，或者该终端设备的网络通信行为偏离了正常的行为基线，自适应调整机制就会立即启动。系统会自动调整终端设备的网络配置参数，如更换通信信道、加密强度提升等，同时更新网络访问控制策略，限制可疑的网络连接，加强对关键数据传输的保护。

通过终端设备自身安全、终端控制安全、终端通信安全、确保接入到网络中的设备具有唯一标识、违规接入进行管控，实现工业互联网终端设备资产梳理和统一管理。

（2）组网可信安全

零信任访问管理系统和策略执行组件进一步提升了 5G+工业互联网的安全性，通过统一管理平台实现策略和组件的集中管理，根据不同应用场景配置定制化的策略授权模型。基于用户的实时操作行为和历史数据动态评估可信度，实时阻断风险行为。策略执行组件能够监测终端操作行为，拦截和管控非法软件，实现网络微隔离，有效防止非法外联和越权访问，确保整个工业互联网环境的安全和稳定运行。

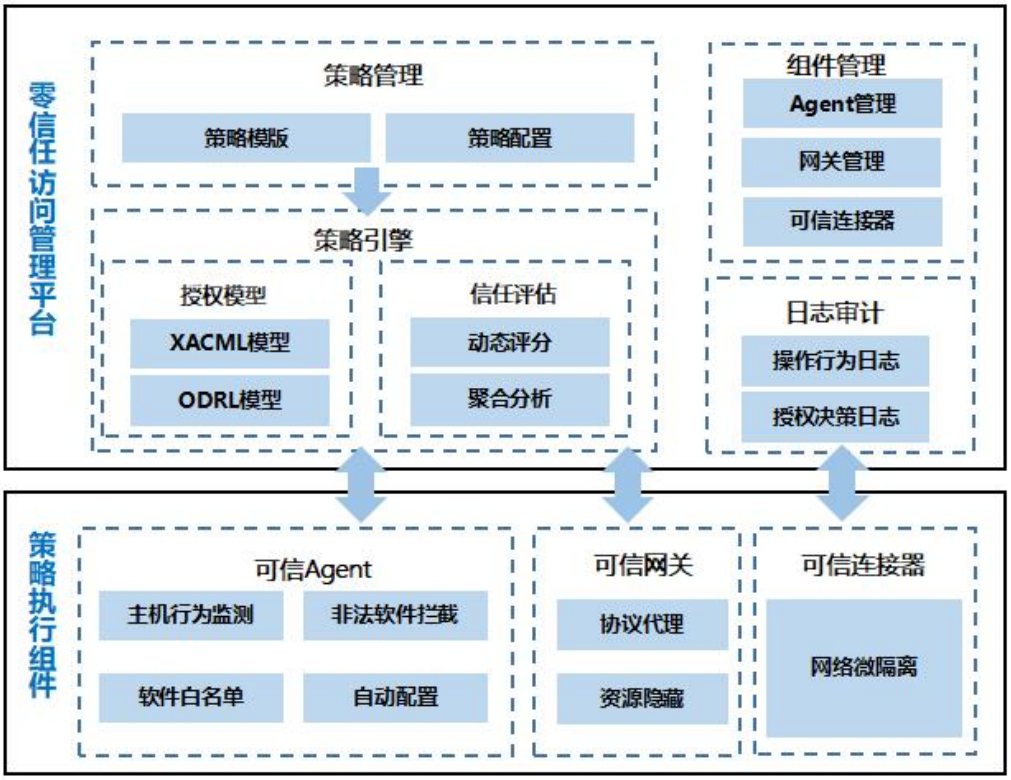

图 4-7 零信任访问管理系统

- 实现策略、组件统一管理
- 依据不同应用场景，可配置不同的策略授权模型，更加贴合业务需求
- 基于用户实时操作行为及历史数据，动态评估可信度，实时阻断风险行为

2、策略执行组件

- 实现从用户终端到网络的全面安全管控
- 实现终端操作行为监测，非法软件（病毒、违规软件）的拦截与管控，以及文件操作行为记录
- 实现网络微隔离，防止非法外联及越权访问

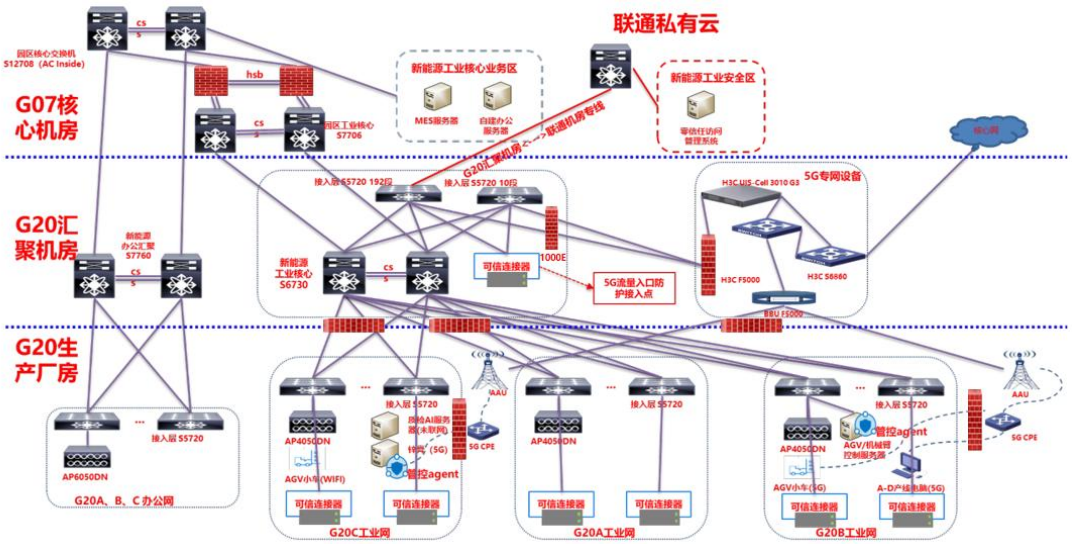

图 4-8 工业零信任访问管理系统部署示意

工业企业中，对于接入的设备也是如此，每一台物联网设备、办公电脑等，在持续的网络交互过程中，都会不断被监测其行为是否符合正常的操作模式。正常情况下它会按照固定的时间间隔向服务器上传采集的数据，若突然出现异常的数据传输频率或者试图访问其他无关的网络资源，零信任架构下的安全系统会立即察觉并阻断其访问，同时进行深度的安全检测，防止其已被恶意控制而成为攻击内部网络的跳板。

通过这样全方位、持续性的验证和监控机制，零信任安全架构在实际应用中能够将网络内部攻击以及横向移动攻击的风险降低，真正让 5G 专网构建起了一种处处设防、时时警惕的安全网络环境，有效应对了日益复杂的网络威胁，保障了网络的可信性和业务的正常运转。

（3）数据可信安全

工厂通过部署先进的工业数据安全交换系统，确保数据安全。系统对接数据源，自动扫描并采集未知数据资产，管理采集的元数据，并在数据采集、处理和使用过程中下发策略和存证，生成和管理数据目录。系统利用沙盒隔离环境对数据进行预处理和管控，确保数据应用过程的安全。

（1）数据目录管理

- 对接数据源，实现数据目录的生成与管理
- 实现目录信息与目录操作可信存证

（2）数据策略管理

- 实现数据采集、数据处理、数据使用等策略的配置、下发与存证
- 支持用户在线协商数据策略，实现协商过程存证

（3）存证溯源

- 基于区块链智能合约实现数据流通全过程存证溯源

（4）身份管理

- 结合动态可信数字身份技术，实现用户和数据流通设备的身份统一管理

（5）数据应用管控

- 通过沙盒隔离环境实现数据预处理、数据应用过程中的管控

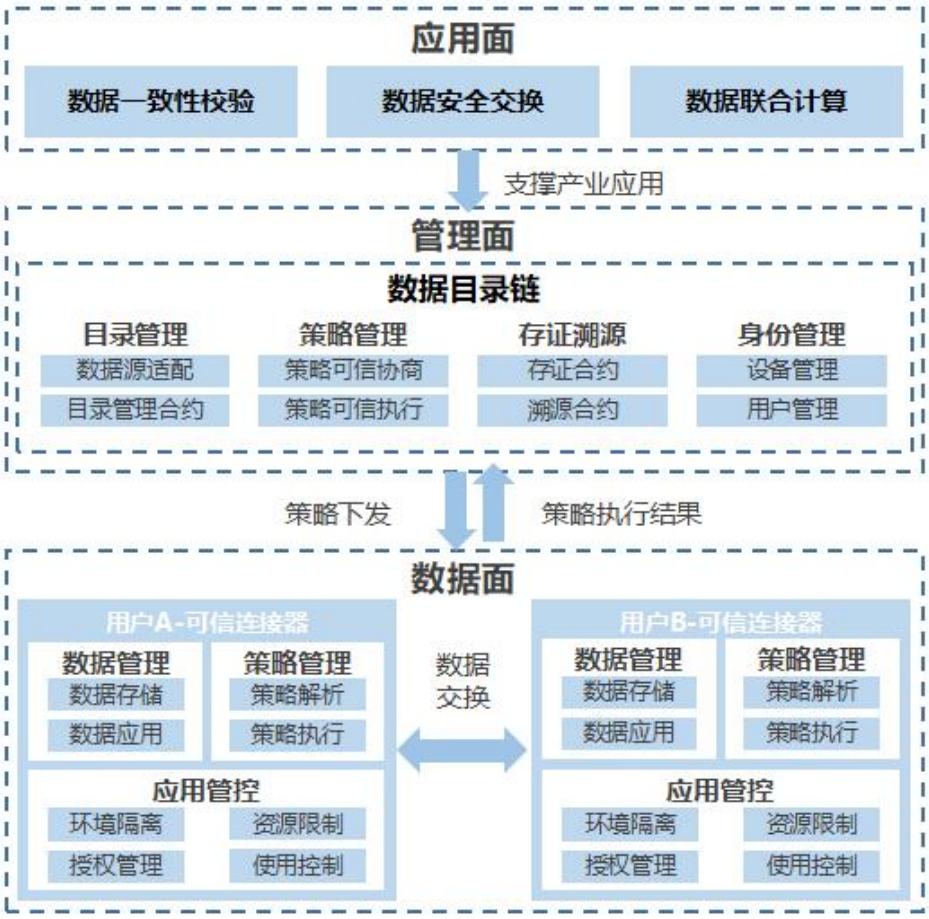

图 4-9 工业数据安全交换系统

数据采集过程中，通过开展数据采集合规性检查，部署工业防火墙、数据标识与溯源、传感器可信安全检测等能力来降低数据安全风险；在数据传输过程中，可通过部署 VPN、加密机、完整性校验、工业防病毒等能力来降低传输数据被嗅探、被攻击者拦截和传输数据包被修改等风险；数据处理可通过部署数据加密、机密计算等能力降低数据被未授权查看、使用、恶意篡改、伪造等风险。

3. 具体应用场景和安全应用模式

基于 5G 专网的可信数据空间安全架构基于多因素身份认证、终端零信任、数据加解密等技术，对工业网络终端和数据安全进行全方面防护。可信数据空间通过技术、法律和治理框架的结合，构建了一个安全、可信、可控的数据共享环境。它不仅解决了数据流通中的安全和隐私问题，还推动了数据作为生产要素的价值释放，为数字经济的发展提供了有力支撑。

（1）企业终端安全可信应用模式

方案针对工业园区，实现对园区内终端和网络设备的全面安全监管。在网络构建上实施细粒度的网络访问控制与隔离方案，确保了数据采集的精确性和安全性。通过多因素身份认证技术，确保只有授权的设备和用户可以访问生产数据。利用 5G 网络切片技术，为生产数据传输提供隔离的网络环境，防止数据被篡改或窃取，采用加密技术保护数据传输和存储过程中的隐私，利用数据沙箱技术在安全环境下进行数据分析和处理。适用于工业企业的 IT 和 OT 融合环境，尤其是面对复杂多变的网络威胁，需要对访问权限进行严格管控的场景，如智能制造工厂的生产网络、关键基础设施的监控与数据采集系统等，可有效降低因网络攻击导致的生产中断风险。

（2）企业数据安全可信应用模式

工业互联网企业对企业园区内工业网络数据进行全面采集，实时监测数据流量，对数据深度分析后进行可视化展示，辅助安全管理人员掌握网络总体态势。在企业园区内实施对工业网络数据的全面采集和实时监测，通过对数据流量的细致分析，将关键信息以可视化的形式展现，直观的展示方式辅助了安全管理人员快速把握网络的总体态势。结合数据威胁监测，及时识别潜在的网络威胁，以人机共智的方式辅助管理人员迅速做出响应，有效提升了企业对网络安全威胁的防御能力。适用于对工业网络安全态势感知和管理有较高要求的企业，如大型工业企业、关键基础设施运营企业等，能够帮助企业全面掌控网络安全态势，及时发现和处置安全威胁，提升网络安全管理水平。

（3）企业网络安全可信应用模式

根据承载业务特点等因素，对工业控制网络实施分区分域管理，部署工业防火墙、网闸等设备实现域间横向隔离；当工业控制网络与企业管理网或互联网连通时，实施网间纵向防护，并开展安全审计。同时，对无线通信技术组网制定严格的网络访问控制策略，对无线接入设备采用身份认证机制，关闭无线接入公开信息广播，避免设备违规接入。适用于工业企业内不同业务系统之间、工业控制网络与外部网络之间需要进行严格隔离和防护的场景，如化工企业的生产控制网络与办公网络的隔离、智能制造工厂内不同生产区域网络的分段管理等，可有效防止网络攻击从一个区域扩散到另一个区域，降低安全风险。

4. 安全及可靠性

（1）安全性

本方案通过支持数据空间可信技术，将工业网络划分为多个相互隔离的区域，在不同网络区域间调整配置以增强整体安全性，辅助安全管理人员对每个网络区域实施精细化的访问控制，有效减少攻击面和资产暴露风险，提高对异常情况的响应速度。在监测到异常时，迅速限制攻击的扩散，增强业务系统的韧性。此外，本方案提供数据安全可信策略，采用加密技术和数据签名技术，保护数据在存储和传输过程中的安全性和完整性，在利用工业大数据时，只有经过授权才能访问相关的生产质量数据，并且其使用方式、数据流向等都受到严格监控，确保数据使用可信，维护数据安全确保数据的安全性和高效利用。

（2）可靠性

在工业环境下，数据常常需要在不同的设备、系统以及部门之间传输，像从生产车间的现场控制设备传输到企业的中央监控系统，或者从工厂内部传输到远程的运维中心等。采用加密传输、数字签名等技术手段来保证数据传输的可信性，就能让接收方确认收到的数据确实是由合法的发送方发出且未被中途更改，保障数据的完整性和保密性，进而维护数据在传输环节的安全。利用 SSL/TLS 等加密协议，对传输的数据进行加密包裹，在接收端进行解密验证，只有通过验证的、可信的数据才能被接收和使用。

5. 其他亮点

（1）安全方案避免了安全规划能力的单一性，在 5G 网络的基础上，创新性地采用多层次、多维度的安全防护体系，整合多种安全技术和策略，针对工业网

络可信安全的应用场景，充分发挥现有设备的最大功效，无需大量增加新的设备投入，即可显著提升安全防御能力。通过实施精细化的资产管理和优化配置，利用现有的硬件资源来部署、调整安全策略，减少对新硬件的依赖，使得现有设备能够适应新的安全需求，在不增加额外成本的情况下，实现对安全威胁的有效防御。与传统的工业内网防火墙等硬件产品相比，成本大幅降低，同时在安全性和控制灵活性方面都有显著提升。

（2）安全方案作为长期工业网络安全规划，避免了不必要的重复性建设。通过洞察企业信息化总体目标和各阶段的具体实施目标，同步制定工业网络安全规划目标，确保安全策略高效落地执行。从企业发展战略的高度出发，对安全需求进行全面分析，制定工业网络安全框架体系，明确安全建设远景目标和重点方向，确保安全能力的持续提升和优化，实现工业企业安全能力长期稳定发展，为企业提供了一个可持续、可扩展的安全保障体系。

（3）安全方案整合联通安全服务能力，快速补齐企业在安全运维人员缺乏和人员安全能力不足的问题。通过提供专业监测和防护服务，企业无需额外设备投入即可提升新能源工厂的风险监测、异常行为分析和应急响应能力。方案减轻了企业的运维负担，确保了网络环境的安全性和稳定性，为企业的持续发展提供了坚实的安全保障。

2.4.3 下一步实施计划

1. 推广 5G 示范应用标杆

目前，该项目已在新能源工厂成功落地并验证效果，作为集团内部的标杆项目，已向其他新能源工厂进行推广。项目覆盖了公司生产网络中的 200 多台生产设备，为工厂提供了内网范围内的网络微隔离、访问控制和终端行为管理等安全措施。预计到 2025 年，将有超过 10 家工厂采用该安全解决方案，以提升集团整体的网络安全防护能力。

2. 持续推进安全方案建设

项目在工厂的成功实施基础上逐步转化为集团其他业务领域的“一站式”工业网络安全解决方案。方案在工厂的基础上完善方案细节，确保其能够满足不同

业务场景的需求。以工厂为核心，逐步向集团内其他业务领域推广，涵盖电子信息、原材料、消费品等领域，以推动这些领域的智能化工厂发展，为集团其他厂区的工控安全推广建设奠定坚实的基础。

2.4.4 方案创新点和实施效果

1. 方案先进性及创新点

（1）项目创新性地使用基于5G专网的可信数据空间安全解决方案。方案基于5G网络防护体系，优化设备接入、网络接入可信，避免企业安全能力单一、重复投入和无效设备投入，为企业降低投入成本，减轻运维负担。

（2）在资产终端安全接入和识别技术方面，项目创新性地集成了5G接入管理和可信连接器，实现了对设备接入的严格管控和统一身份认证，确保只有验证过的设备能够接入网络，极大提升了网络的安全性和可靠性。

（3）采用创新的安全可信组网策略，构建了一个融合5G技术和生产网络的细粒度网络访问控制与隔离方案，利用5G网络高速率、低延迟的特性，实现对工厂网络访问更为精准的管理和有效隔离。方案提升了工业网络安全管理的精准度和管理效率，确保关键数据在园区内的安全流动和网络稳定。

（4）数据安全创新方案通过部署5G专网和云化工业数据交换方案，实现园区内数据的安全交互，确保数据在园区内部流转，不外泄。方案利用5G网络的高速率、低延迟特性，结合云计算的灵活性和可扩展性，为园区提供了安全高效的数据交互环境。

2. 实施效果

安全方案在工厂中建设跨网络的“一站式”安全可信体系。在试运营阶段，该体系实现了工厂网络的0中断和生产的0中断和100%的安全事件监测发现率。借助安全可信平台，清晰掌握了工厂资产状况，建立动态的资产管控能力。在安全防护方面，平台成功拦截了1173个IP地址的非授权访问，阻断了33个非业务应用和疑似恶意程序，针对应用白名单之外的非业务应用和疑似恶意程序进行阻断，累计发现并拦截不安全软件25个，非业务软件8个；发现了12个网络异

常行为 IP，并迅速响应了 1 次应急事件，展现了高效的安全监控和应急处理能力。

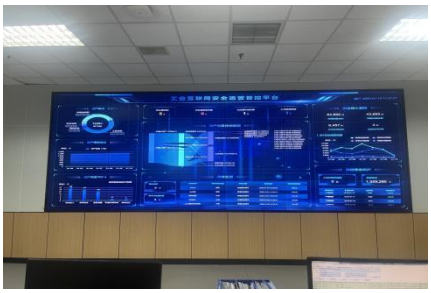

图 4-10 工厂安全和应用监控大厅、大屏

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。

四川长虹新能源科技股份有限公司成立于 2006 年，作为长虹控股集团旗下子公司，集全系列碱性电池、锂离子电池的研发、制造和销售于一体的国家高新技术企业。公司产品广泛应用于消费、工业等诸多领域，销往全球 100 多个国家。长虹新能源始终以推动新能源技术发展和绿色能源应用为己任，致力于成为新能源领域的领导者和创新技术的先行者。公司自成立以来，为工业企业提供了大量优质的解决方案，覆盖电池行业的多个领域。长虹新能源合计拥有 232 项专利技术，以其深厚的研发实力和生产管理能力，为全球知名品牌和高端市场客户提供高性能电池产品和优质服务。

2.5 案例五：山东中烟工业互联网安全防护体系创新实践——山东移动构建“云-边-端-控”协同防御体系

引言：山东中烟工业有限责任公司是中国烟草总公司的全资子公司，是全国19 家卷烟工业企业之一、全国 4 家雪茄生产企业之一，内销卷烟产量居全国第六位。下辖济南、青岛、青州、滕州等四个卷烟生产厂，将军、颐中集团公司两个全资子公司。 总资产规模较大，拥有现代化的生产基地和先进的生产设备，具备较强的生产能力。

随着卷烟厂数字化转型不断深入，信息技术也从单纯的数字化阶段逐步迈向网络化与智能化阶段。在此过程中，企业对智能化数字系统以及数据分析能力的依赖程度日益加深，大量运营数据、客户信息和业务流程均集中于 IT 系统。这就使得 IT 系统稳定运行以及网络安全的重要性大幅提升，成为保障企业正常运营的关键因素。

2.5.1 方案概述

1. 方案背景

随着信息技术的快速发展，企业数字化转型步伐加快，网络边界日益模糊，云计算、物联网、工业 4.0 等新兴技术的广泛应用使得企业面临更为复杂的网络安全威胁。边缘计算、云计算环境的普及，使得数据在传输、存储和处理过程中的安全风险显著增加。同时，工业控制系统与互联网的融合，也带来了前所未有的安全挑战。

外部攻击频发，黑客利用漏洞攻击、DDoS 攻击、恶意软件入侵等手段，试图入侵企业网络，窃取敏感信息、破坏系统或勒索赎金，可能影响卷烟生产系统、供应链管理系统等正常运行，甚至可能导致黑客进一步渗透企业核心网络，获取更重要的商业机密和生产数据，以上均可能对企业造成生产中断、数据泄露、重大经济损失和声誉损害等。内部威胁同样不容忽视，员工误操作、权限滥用、恶意泄露信息或内部人员犯罪等行为，同样威胁到企业的数据安全和业务稳定，干

扰正常的生产经营秩序。与此同时，随着数据安全和个人隐私保护法规的不断出台，企业需确保数据处理和存储符合相关法律法规要求，避免法律风险和罚款。

在此背景下，构建一个高效、智能、全方位的网络安全防护体系成为企业保障业务连续性、数据安全和合规性的关键。

2. 方案简介

构建全方位网络安全防护体系，提升整体安全防护效果，简化运维，为数字转型提供强有力支撑。可实时监测用户业务访问行为，一旦发现异常流量（如DDoS 攻击）和恶意软件（如窃取用户账号信息）等，各功能模块协同工作，保障网络安全和业务连续性。

纵深防御体系通过多层次防护，从网络层、系统层、应用层、数据层到人员层，全方位抵御威胁。例如，黑客可能通过网络漏洞窃取客户资金信息，纵深防御体系能在网络层拦截非法访问，在系统层防止恶意软件入侵，在数据层加密相关信息，有效保障资金和数据安全。同时，单一品牌安全设备功能有限，一旦该品牌设备出现漏洞或被破解，企业网络安全全面受威胁。品牌异构引入不同品牌设备，降低整体安全风险，如企业同时使用 A 品牌防火墙和 B 品牌 IDS，即使 A 品牌防火墙被攻击，B 品牌 IDS 仍可监测异常。

3. 方案目标

（1）构建多层次防御体系：通过部署边缘云边界防火墙、边界防火墙等设备，构建从云端到本地、从外网到内网的多层次防御体系，有效隔离和抵御各类网络攻击。

（2）增强安全监测与响应能力：利用主机防护软件、入侵防御系统、脆弱性扫描等设备，实时监测网络异常行为，及时发现并响应安全事件，缩短响应时间，减少损失。

（3）确保数据合规与安全：通过数据库审计、日志审计等设备，记录并分析数据访问和操作行为，确保数据处理和存储符合法律法规要求，防止数据泄露和滥用。

（4）提升员工安全意识与管理水平：通过堡垒机系统扩容，加强员工对网络安全的认知和管理，规范运维行为，提升整体安全水平。

2.5.2 方案实施概况

1. 方案总体架构和主要内容

在滕州卷烟厂现有的防病毒软件系统的基础上扩容 500 个信创系统(Server 版）防病毒授权，支持部门架构的导入，包含部门规则、部门与 IP 规则、LDAP 规则导入，并可根据 IP 规则一键整理。采用的网络安全终端威胁防御系统基于自主研发的恶意行为分析技术，可对全网终端进行一体化的实时监控，有效预防黑客入侵、病毒攻击、后门等安全隐患。一旦出现恶意行为，终端威胁防御系统会立即发现并处理，控制灾情扩散。

图 5-1 项目总体架构

采用的云安全管理平台可以与山东中烟滕州卷烟厂的业务超融合平台松耦合，便于适应多厂商超融合平台，可与现有超融合平台对接，支持基于同一套安全防护组件来防护现有的超融合平台的用户业务，且此次项目所使用产品及软件均为国产化信创设备，满足国家、政府的安全性要求。

2. 具体应用场景和安全应用模式

（1）主要建设内容及特点

边缘云边界防火墙设备：部署于云平台的边缘，采用先进的威胁防御技术，有效隔离云环境与传统 IT 环境，确保云上业务安全隔离与访问控制。

边界防火墙设备：在内网与互联网之间设立坚实的边界防护，实施严格的访问控制策略，防止非法入侵和数据泄露。

主机防护软件：在关键服务器上部署主机入侵防御系统，实时监测并防御针对主机的恶意攻击，增强主机安全防护能力。

入侵防御系统设备：部署深度包检测（DPI）和行为分析技术的入侵防御系统，精准识别并阻断各类网络攻击。

数据库审计设备：对网络中的数据库进行全面审计，记录并分析所有数据库操作，确保数据的合规性和安全性。

Web 应用防火墙设备：保护 Web 应用免受 SQL 注入、跨站脚本（XSS）等攻击，确保 web 应用安全稳定运行。

脆弱性扫描设备：定期对网络资产进行脆弱性扫描，及时发现并修复安全漏洞，提升整体网络安全水平。

流量回溯取证重放设备：部署流量回溯系统，对网络流量进行记录和分析，一旦发生安全事件，可迅速回溯取证，为事件处置提供有力支持。

日志审计系统：构建统一的日志审计平台，集中收集并分析各类安全设备的日志信息，实现安全事件的及时发现和响应。

（2）关键核心技术

智能威胁识别与防御：利用机器学习算法，提升防火墙、入侵防御系统等设备的威胁识别能力，实现精准防御。

深度包检测与行为分析：结合 DPI 和行为分析技术，对网络流量进行深度解析和行为模式识别，有效发现并阻断潜在威胁。

统一云安全管理平台：构建集安全策略管理、事件监控、日志审计于一体的统一云安全管理平台，提升网络安全管理的效率和智能化水平。

3.安全及可靠性

（1）网络安全设备异构

采用不同品牌的设备来增强安全性和可靠性：

互联网边界防火墙设备选用天融信，入侵防御系统设备选用启明星辰，两者非同一品牌设备；互联网边界防火墙设备选用天融信，web 应用防火墙设备选用绿盟，两者非同一品牌设备；互联网边界防火墙设备选用天融信，流量回溯取证重放系统设备选用奇安信，两者非同一品牌设备。

入侵防御系统设备选用启明星辰，web 应用防火墙设备选用绿盟，两者非同一品牌设备；入侵防御系统设备选用启明星辰，流量回溯取证重放系统设备选用奇安信，两者非同一品牌设备。

web 应用防火墙设备选用绿盟，流量回溯取证重放系统设备选用奇安信，两者非同一品牌设备。

（2）一体化平台边缘环境网络安全防护设备异构

使用产品边缘云边界防火墙设备（天融信）与 web 应用防火墙设备（绿盟）非同一品牌设备，以实现真正的异构性，增强系统的安全性和抗攻击能力。

品牌异构引入不同品牌优势设备，增强了整体防御能力。结合不同品牌防火墙、IDS/IPS 等设备的优势，攻击拦截成功率大大提升。

2.5.3 下一步实施计划

基于山东中烟项目的成功经验，为持续深化网络安全防护体系建设并推动行业应用，制定分阶段实施计划，通过本项目的实施，山东中烟卷烟厂的网络安全防护能力得到了有效提升，本案例具有较高的可推广性，可使用于以下单位和领域:

省外同类型企业: 企业拥有复杂的网络环境和丰富的业务场景，需要构建全方位的安全防护体系。搭建“云-边-端”协同防护体系，针对生产网、办公网、物联网等不同场景定制安全策略。

中小型企业: 中小型企业虽然资源有限，但同样需要关注网络安全。本案例中的部分设备或策略可以根据其实际需求进行灵活配置和调整。可推出轻量化安全服务包（含防火墙基础配置模板、漏洞扫描工具、员工安全意识培训课程），降低部署成本。

2.5.4 方案创新点和实施效果

1. 方案先进性及创新点

网络安全设备异构：多生态协同防御矩阵，通过部署不同品牌的网络设备，能够增强防护能力，避免单点故障、适应复杂的网络环境，并且提高网络的安全弹性，使网络能够在遭受攻击后快速恢复正常运行。

混合品牌部署：构建异构防御链，规避单一技术路线漏洞。

2. 实施效果

（1）构建全方位安全防御体系，显著提升网络安全防护能力

自部署边缘云边界防火墙、边界防火墙等设备以来，卷烟厂的网络安全防护体系得到了全面升级。这些防火墙设备不仅有效隔离了不同安全域，还通过智能威胁识别技术，精准阻断了外部攻击和内部泄露风险，确保了关键业务系统的连续性和数据的完整性。同时，主机防护软件和入侵防御系统设备的协同作用，进一步提升了系统对恶意软件和未知威胁的防御能力，显著降低了安全风险。

（2）强化数据安全与合规性，降低法律风险

数据库审计设备的部署，实现了对数据库操作行为的全面监控和审计，确保了数据的合规使用和安全性。此外，通过日志审计系统对各类安全事件的记录和分析，能够及时发现并处置潜在的数据泄露风险，有效降低了因数据安全问题引发的法律风险。

（3）增强应急响应能力，为安全事件处置提供有力支持

流量回溯取证重放设备和脆弱性扫描设备的应用，显著增强了我们的应急响应能力。一旦发生安全事件，我们能够迅速回溯并重现攻击过程，为事件处置和应急响应提供了宝贵的线索和证据。同时，定期进行的脆弱性扫描和风险评估，帮助我们及时发现并修复安全漏洞，降低了被攻击的风险。

2.5.5 单位基本信息

中国移动通信集团山东有限公司（以下简称"山东移动"）隶属于中国移动通信集团公司，组建于 1999 年 7 月。公司下设 17 个市级分公司，以及 125 个县（市、区）级分公司。截止 2024 年 12 月，山东移动基站总数 35 万个，其中 4G 基站数量超过 22 万个、5G 基站数达 13 万个，5G 基站数占全省 5G 基站总数的半数以上。手机用户超 7047 万（其中 4G 用户超 4000 万）、有线宽带用户突破 2063 万、物

联网接入用户超1.4亿，综合实力位列全省通信运营商之首。目前山东移动打造了全省覆盖规模最广、网络质量最优、客户满意度最高的4G精品网络，人口覆盖率达到99.9%，地理覆盖率达到99.2%，重要公共场所和旅游景点、高速公路、国道、省道全线以及铁路沿线、近海区域实现100%覆盖，全省乡镇及以上区域、高速铁路、公路的连续覆盖率达到97%以上。于此同时，山东移动针对城区、高铁、高速路、风景区等重点场景，通过灯杆站、一体化皮站等方式，采用覆盖、小微站、楼间对打等灵活手段不断改善客户体验，解决网络深度覆盖问题。核心城区平均下行速率达到48Mbps，高铁下行速率达29Mbps，高速公路下行速率达35Mbps，全省领先。借助山东移动庞大的客户规模为政府有效决策提供了准确的数据支持。全国最大的数据中心（华东地区）就落户在山东移动大数据中心。

2017年以来，坚持以习近平新时代中国特色社会主义思想为指引，坚决落实省委省政府决策部署，将企业发展融入我省经济社会发展全局，持续发挥通信运营商信息化优势，助力山东新旧动能转换、数字山东建设。2019年山东移动被评为“山东省优秀企业”。一是按照习近平总书记提出“加快5G网络、数据中心等新型基础设施建设”，我省《关于山东省数字基础设施建设的指导意见》等要求，山东移动坚决落实上级决策部署，集中优势资源，大力推动5G、数据中心等新型基础设施建设，促进信息技术与经济社会各领域深度融合，为我省高质量发展提供信息动力；二是在基础通信网络建设、宽带提速、网络覆盖方面不断创新，持续发力：三是落实国务院“提速降费”的要求，在省内积极推动专线（宽带）提速降费，全省移动宽带用户率先迈入光纤百兆时代；四是与铁塔公司密切合作，优选4G、5G基站地址，逐步解决覆盖死角；五是通过自有“云管端”服务能力，提供基于设计、建设、维护等一站式集成服务，为推动全省智慧政务建设、促进新旧动能转换贡献自己的力量。

2.6 案例六：石油行业一体化安全运行中心建设案例——长庆油田 IT&OT 一体化网络安全运行中心建设

引言：长庆油田是隶属于中国石油天然气股份有限公司的地区性油田公司，公司的主营业务是在鄂尔多斯盆地及外围盆地进行石油天然气及共生、伴生资源和非油气资源的勘查、勘探开发和生产、油气集输和储运、油气产品销售等。随着长庆油田的数字化转型和网络升级改造，当前的油气生产业务对网络基础设施的依赖度越来越大，网络安全作为基础设施建设核心，一旦发生网络安全事件将会对生产业务造成不可逆的影响。同时，长庆油田正处在数字化转型的关键阶段，而网络安全作为业务数字化转型的底板工程，必须同时补强 IT 和 OT 网络安全能力，筑牢网络安全防线，打造 IT&OT 一体化网络安全防护能力，护航长庆油田数字化转型，保障油气生产业务安全稳定运行。

2.6.1 方案概述

长庆油田 IT&OT 一体化网络安全运行体系建设内容是：以安全运行中心建设为核心，以合规性安全要求为支撑，面向等级保护、安全管理制度和安全应急体系等建设任务，聚焦工控网络安全战斗力生成，整合机构人员、协调机制、管理制度、工作流程、安全服务管理和安全手段措施等方面，封装为统一接口的可交付安全能力，形成强后台、精前台的工控网络安全运行模式。

1. 方案背景

随着长庆油田的数字化转型和网络升级改造，“云、大、物、移、智”等新技术在油田大量应用，使 IT 和 OT 深度融合，促进了油气生产管理。同时，从互联网传进来的各种网络风险逐渐渗透到 OT 系统，使得生产网工控安全形势也日益复杂和严峻，并呈现出一些新的特点和趋势，这对于长庆油田的工控安全管理工作也提出了新的挑战。因此，必须采取有效的、针对性的 IT 和 OT 安全融合措施，以保障工业生产安全运行。

2. 方案简介

近年来，国家高度重视工业互联网信息安全工作，在国家监管层面，国务院、网信办、公安部等部门出台的网络安全相关政策标准在安全运行和管理方面也提出了明确的要求。在中石油内部监管层面，集团公司已经建成了网络安全运行中心对各下属单位进行网络安全监测，督促各单位处置网络安全问题。长庆油田高度响应国家及行业政策要求，基于长庆油田的实际业务需求，结合当前的安全建设现状，通过与行业知名网络安全企业奇安信科技集团股份有限公司（以下简称奇安信）合作，基于“数据驱动安全”的理念，运用大数据技术及信息协同为驱动能力，建立以业务服务为目标的长庆油田工控网络安全运行中心，该建设是在长庆油田已有安全基础上，重构一种新的安全效能倍增模式，全面融合 IT 和 OT 安全数据，构建以“合规为底线”面向“实战化”的生产网安全防护体系，同步完善生产网工控安全管理制度，实现生产网稳定、高效、安全运行。

3. 方案目标

基于长庆油田的实际业务需求，结合当前的安全建设现状，长庆油田 IT&OT 一体化网络安全运行中心的建设是在长庆油田已有安全基础上，重构一种新的安全效能倍增模式。

网络安全运行中心的建设目标有以下几点:

（1）从长庆油田的实际业务发展目标和安全运行需求的角度出发，打造匹配业务需求的网络安全能力，使安全能力与业务高度融合，贯穿业务的建设、使用、管理、运维等全周期。

（2）构建实现从被动、静态、单点的工控安全防御体系到主动、动态、整体的工控安全防护体系的转变，以保障业务安全可靠为前提，持续提升整体生产网安全防御、检测、响应能力，并具备一定的威胁溯源反制能力。

（3）高效整合技术、工具、服务、流程、人员等全要素，打通工控安全预防、保障、监控、应急等全流程，实现已有安全能力和未来安全能力的统筹中心，通过自动化机制落地，构建面向业务的体系化安全运行能力。

（4）基于安全运行中心体系的构建，探索长庆油田工控网络安全架构的建设路径。安全运行体系作为整体安全架构的重要组成部分，是安全能力和需求演进到一定阶段的必然选择。整体安全架构的演进，依赖于安全运行体系的有效落

地。未来的安全运行体系将更多实践以防御、检测、响应和预测为主的自适应安全架构，并不断融合新的网络安全理念，丰富和完善组织网络安全架构的实践。

2.6.2 方案实施概况

长庆油田 IT&OT 一体化工控网络安全运行中心围绕油气生产业务需求，打造 IT/OT 一体化创新安全防护体系。平台主要应用了工业流量探针，含工业防火墙、工业主机防护等设备，以工业安全事件告警与分析为主线，持续监测全局工业安全风险，形成网络监测、行为审计、访问控制、主机管控、脆弱性识别、态势监测、运行分析等综合安全能力。对内，将云、网、边、端四个方向的流量、日志、资产、漏洞信息汇聚到安全运行平台，进行多源异构安全大数据智能检测与高效分析；对外，对接奇安信威胁情报中心，分析安全威胁数据、多源情报数据，跟踪 APT 事件，为安全运行中心提升未知威胁检测、威胁溯源分析、主动防御等高级防护能力。同时，组建安全运行团队明确组织结构与安全运行权责，将不同等级不同类型的安全事件分配到不同能力不同岗位的安全人员，实现网络安全的“分级诊疗”。实现工业安全设备集中管理与监控、日志集中采集与管理、威胁统一分析与运营、事件应急响应与处置等核心功能，有效帮助保障生产的连续性，在满足工业安全合规需求的同时，为长庆油田工业安全运营体系建设提供决策支撑。

1.项目总体架构和主要内容

长庆油田 IT&OT 一体化工控网络安全运行中心总体架构设计是依据《网络安全法》、《等级保护 2.0》、《关键信息基础设施保护条例》等相关法律法规，根据中石油集团公司对于数字化转型的目标，结合长庆油田公司实际工控安全需求进行的总体设计，工控安全运行中心通过搭建运行团队、构建管理机制、梳理运行流程，建设工控安全运行平台和运行团队，形成“组织+流程+工具”的体系化安全运行。通过持续运行，逐步建立起长庆油田公司工控网络安全运行指标体系。总体架构如下:

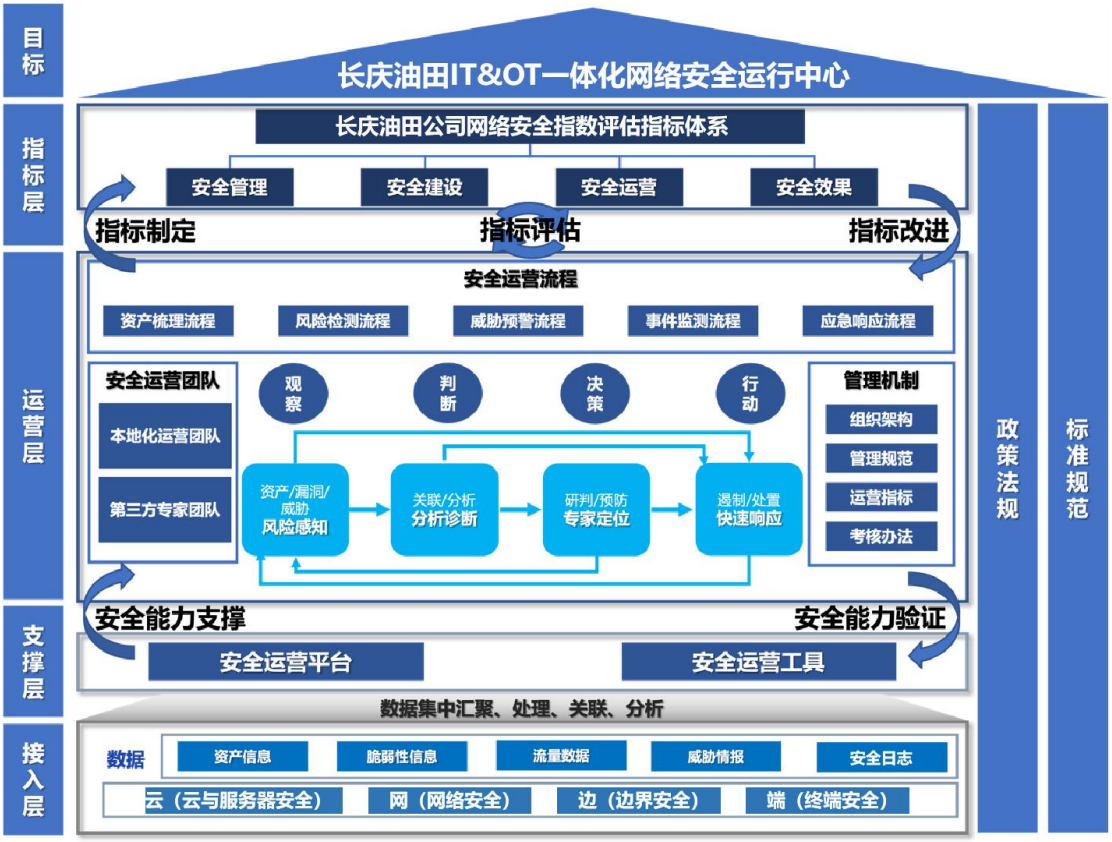

图 6-1 工控网络安全建设拓扑图

➢ 接入层

接入层是平台的数据来源，通过打破长庆油田公司网内安全信息孤岛，核心通过采集生产网工控边界安全、工控主机安全等的资产信息、脆弱性信息、流量数据、日志数据，同时汇聚了办公网（IT）、社区网等资产风险信息，为支撑层提供多维数据支撑。

➢ 支撑层

支撑层是平台技术基础，依托工控安全运行平台和相关安全运行工具对采集的原始数据进行预处理、过滤、转换、聚合等，并进一步处理成上层所需的各种业务数据和配置数据等，基于产品应用功能与数据之间抽象的通用处理关系，并通过关联分析引擎、漏洞匹配引擎、学习训练引擎、安全基线引擎、风险评估引擎、工作流引擎、内生安全引擎、大数据检索、策略管理引擎等，结合威胁情报数据进行数据关联和数据分析，为运行团队提供技术支撑。

➢ 运行层

运行层是平台的核心，通过搭建运行团队、构建管理机制、梳理运行流程，将组织、流程和工具有机结合在一起，实现工业集中统一管理、工业日志集中审计、工业安全运营分析、工业安全事件响应处置、组态化的工业态势感知大屏，强化风险感知、分析诊断、专家定位、快速响应能力。

➢ 指标层

指标层是在对长庆油田公司工控网络安全运行过程中不断沉淀形成的，运用指标体系一方面对长庆油田公司网络安全治理水平进行评估，一方面推动网络安全治理水平的不断改进，形成长庆油田公司网络安全可持续发展。

2. 网络、平台或安全互联架构

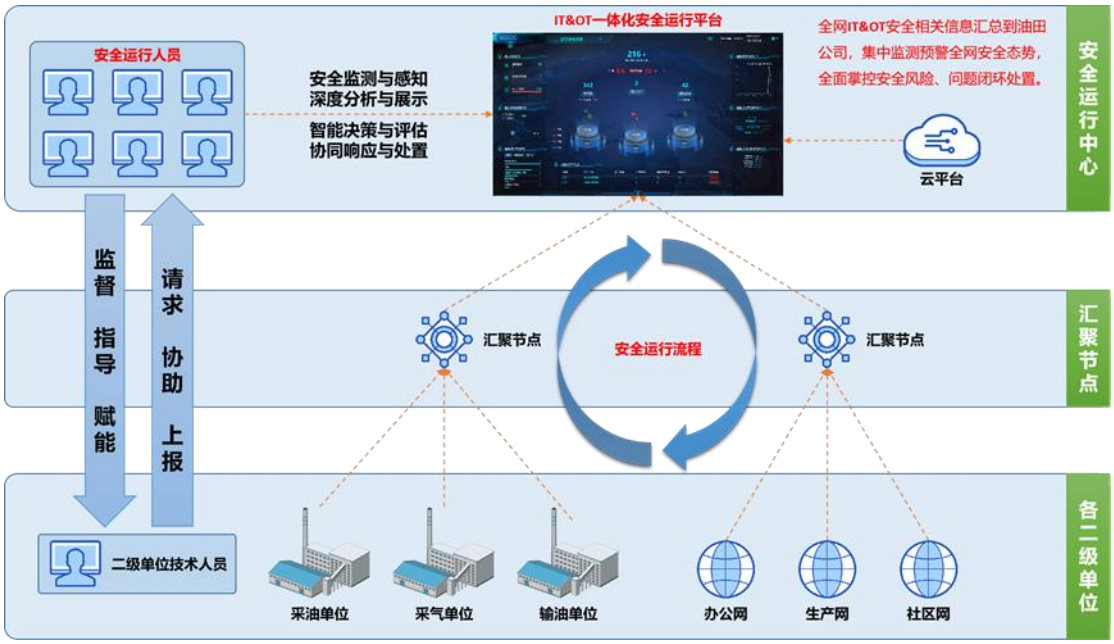

图 6-2 工控网络安全建设拓扑图

如上图所示，IT/OT 一体化工控安全运行中心整体架构包括安全运行人员、安全运行平台、安全运行流程三部分组成。安全运行平台通过收各二级单位办公网、生产网、社区网以及油田公司云平台的安全数据，利用关联分析、机器学习、威胁情报等技术，帮助长庆油田持续监测网络安全态势，实现从“被动防御 ”向 “主动防御” 的进阶，为安全管理者提供风险评估和应急响应的决策支撑，为安全运行人员提供威胁发现、调查分析及响应处置的安全运行工具。安全运行人员需要明确组织结构与安全运行权责，可分为油田公司安全运行人员和二级单位安全运行人员两部分，二级单位安全运行人员负责对本单位发现的安全事件进

行上报，并可请求油田公司协助处置安全事件，油田公司安全运行人员负责对各二级单位安全运行人员进行监督、指导、赋能。安全运行流程需要制定各类安全运维制度和事件处置流程。通过安全运行人员、安全运行平台、安全运行流程三者的能力配合，最终，可实现全网安全相关信息汇总到油田公司，集中监测预警全网安全态势，全面掌控安全风险、问题闭环处置。

3.具体应用场景和应用模式

（1）IT/OT 资产管理

对长庆油田 IT/OT 网络中的所有硬件设备（如 PLC、DCS、SCADA 系统、RTU 等）、软件组件（操作系统、应用软件、固件版本等）、网络设备（交换机、路由器、防火墙等）以及相关的 IT/OT 融合设备进行资产识别与记录，实现资产的全面、精准识别。通过持续监测，及时发现新增、变更或退役资产，确保资产清单的实时性和准确性。

（2）IT/OT 系统漏洞管理

识别、评估、管理和修复长庆油田 IT/OT 系统中的安全漏洞，以降低系统遭受恶意攻击的风险，保障关键基础设施的稳定运行。

a.漏洞评估与优先级排序:

依据漏洞的严重程度（CVSS 评分）、利用难度、现有防护措施的有效性、资产重要性、暴露面大小等因素，进行综合风险量化评估。

b.漏洞验证与深入分析:

漏洞复现: 在隔离的测试环境中，对高风险漏洞进行安全研究人员主导的复现验证，确认漏洞真实存在且可被利用。

漏洞利用路径分析:分析攻击者可能利用漏洞入侵系统的具体步骤和所需条件，了解攻击链路，为防御策略设计提供依据。

临时缓解措施:在正式补丁发布前,为高危漏洞提供临时性的缓解措施建议，如防火墙规则调整、访问控制强化、监控告警设定等，以缩短漏洞暴露时间。

c.补丁管理与修复支持:

补丁获取与验证: 跟踪厂商发布的官方补丁，及时获取并验证其适用性、兼容性和安全性，确保补丁的有效性和低风险性。

补丁部署规划：根据生产环境的敏感性、停机窗口、补丁安装复杂度等因素，制定详细的补丁部署计划，包括备份、测试、上线、回滚等环节。

d.漏洞管理平台与自动化：

提供统一的漏洞管理，实现漏洞的集中存储、查询、统计、报告等功能，便于用户直观掌握漏洞态势。

（3）IT/OT 恶意行为处置

长庆油田 IT&OT 一体化网络安全运行中心对网络环境中检测到的各类恶意活动进行及时、有效的识别、分析、响应和遏制，以保护信息系统免受攻击、破坏、窃取或其他恶意行为的侵害。

a.快速响应与应急处置：

响应预案：预先制定针对不同类型恶意行为的应急响应预案，明确责任人、响应流程、工具使用、沟通机制等要素，确保响应行动的迅速、有序。

隔离阻断：在确认恶意行为后，立即采取措施切断其与目标系统的连接，限制其活动范围，防止危害扩大。这包括关闭端口、阻断 IP、隔离设备、禁用账户等手段。

恶意代码清理：使用专业的反病毒、反恶意软件工具，清除系统中已感染的恶意代码，修复被篡改的文件和设置，恢复系统正常功能。

b.事件报告与知识共享：

事件报告：整理恶意行为处置的全过程，编写详细、客观、规范的事件报告，供管理层决策、合规审计、外部监管等用途。

知识库更新：将恶意行为的检测方法、分析结论、处置经验等转化为可复用的知识，更新到安全运行知识库中，提升团队的整体应对能力。

行业协作与情报共享：积极参与行业组织、联盟、论坛等平台，与其他组织共享恶意行为情报，共同提升整个生态系统的安全防御水平。

（4）IT/OT 网络威胁建模

a.威胁需求收集

长庆油田 IT 及 OT 工控安全运行中心收集现网有价值的与安全相关的数据，通过日志泛化的方式令运行工具可识别该日志。提炼出针对具体威胁场景的防护

需求，如阻止特定类型的攻击流量、限制异常网络行为、监控特定协议的异常交互等。

b.威胁模型设计

根据威胁场景需求，设计精准、高效的工控网络安全规则，包括访问控制规则、应用层过滤规则、异常检测规则等。利用模拟工具或沙箱环境，验证规则在真实或模拟工控流量下的拦截效果、性能影响及可能的误报率。

4.安全及可靠性

（1）完善的基础防护能力

本方案为构建长庆油田OT、IT安全能力全面融合的安全运行体系，对长庆油田生产网网络、业务、安全现状进行充分调研分析，帮助长庆油田形成涵盖“网络、边界、主机、设备、应用”的基础防护能力及风险识别能力。网络方面通过OT、IT安全运行系统充分识别风险流量，边界方面通过工业防火墙进行有效的访问控制管理，主机方面通过工业主机防护系统提供差异化的计算环境保护，设备及应用方面通过脆弱性管理系统保障OT、IT设备及系统漏洞可知、可管、可控，并通过安全运行平台构建覆盖长庆油田整体的安全运行管理能力。

（2）先进的加密技术

长庆油田IT&OT一体化工控网络安全运行中心平台采用SSL加密等先进技术，确保数据在传输过程中的安全性。这可以有效防止数据被窃取或篡改。

（3）定期安全更新

长庆油田IT&OT一体化工控网络安全运行中心平台通过定期进行系统安全评估和漏洞扫描，及时修补漏洞，提高了平台的整体安全性。同时，平台具备完善的漏洞监测和响应机制，能够及时发现并处理新出现的安全威胁。

(4）严格的数据管理

长庆油田IT&OT一体化工控网络安全运行中心平台采用先进的加密算法对用户数据进行加密存储和传输，保障用户信息的机密性和完整性。此外，建立隐私保护机制，明确用户个人信息的获取和使用规则，并制定相应的数据保护措施。

5.其他亮点

（1）多源异构安全大数据资产采集与梳理

长庆油田公司工控网络安全运行中心为实现多源异构安全大数据的采集和融合，通过采用基于网络流量的采集与处理技术方法，支持数十种网络协议的识别、解析和检测，实现各类日志、智能应用、PCAP文件回放检测等，支持失陷检测、入侵检测、病毒检测、异常流量、DDoS攻击、应用识别等威胁检测。工业资产的梳理是安全管理平台的基石，提高工业资产管理的准确性是平台非常重要的一项工作。工业资产复杂多样，单独依靠有限的资产特征和指纹信息，无法准确的形成对资产的管理。而且，根据工业业务不同，资产属性也存在很多差异。因此准确高效的实现工业资产台账的建立需要体系化的资产运营过程。

本系统根据工业安全业务的特点，构建了一套完整的资产运营流程。系统在近2000工控资产指纹库的基础上，能够支持多源异构的资产数据来源，并可以根据资产的置信度调整数据源的优先级。在资产属性富化阶段，系统内置了4万条的资产地图库，69类的资产分类库，且均可以实现自定义，同时支持资产属性的自定义添加。考虑到工业资产会根据不同的生产线以及属于不同的业务系统，系统内置了组织架构和业务系统两个资产结构，同时可以新增资产结构，为了丰富资产管理，可以建立资产标签系统，实现快捷资产管理。资产台账形成以后，支持台账的人工批量运营，高效准确实现资产台账的管理

（2）工业大数据安全监测基线

安全基线是面向工业业务的对生产行为的分析， 本质是一种白名单，通过手动创建基线学习任务，指定学习时间，安全基线引擎根据配置的过滤所有条件，从日志或者流量存储中获取数据进行学习，最后生成指定白名单基线。针对工业安全典型场景，采用大数据行为建模分析方法，对工业资产、网络行为、生产工艺建立基线，从而开展异常资产分析、异常网络行为分析、异常工艺行为分析等。长庆油田公司IT&OT一体化工控网络安全运行中心工控关键指令基线，基于工业协议审计的深度，包括五元组、工业协议、指令、寄存器值域等，建立指定时间段的工艺异常行为基线，对偏离安全基线的行为，及时告警。系统支持的工控协议包括DNP3、MODBUS、S7-COMM、OPC-UA、RSSP-1、ENIP/CIP、OPC-DA、IEC60870-5-104、IEC-61850-MMS、OMRON-FINS。支持的关键工艺行为包括但不限于初始化上装、终止上装、放弃控制、获取控制，命令设定、PLC运行、

写多线圈、步调节命定、单命令、PLC下载块请求、冷再启动等

（3）全方位立体化安全动态监测与可视化呈现

工控网络安全态势可视化是将数据可视化技术应用于网络安全领域，利用人类视觉对模型和结构的理解和获取能力，将抽象的网络和系统数据以图形图像的方式展现出来，帮助安全分析人员感知网络状态，识别工控网络异常和入侵，预测工控网络安全事件发展趋势。它不仅能有效解决传统分析方法在处理海量信息时面临的认知负担过重、缺乏对网络安全全局的认识、交互性不强、不能对网络安全事件提前预测和防御等一系列问题，而且通过在人与数据之间实现图像通信，使得人们能够感知到网络安全数据中所隐含的模式，为描述事件发展趋势和发现潜在安全威胁提供有力的支持。相对于地理空间和物理实体的可视化，态势感知的可视化挑战主要在于对抽象概念要素的处理，即数据信息的可视化，虽然对原始数据或海量数据进行可视化的技术很多，但仍难以全面准确表示态势、较好呈现当前状态和未来趋势，如何快速、准确、完整、有效地将态势传达给安全决策者是具有挑战性的问题。本平台通过基于宇宙星系的安全态势监测与可视化设计，提升目标网络的资产态、分布态、运行态、威胁态、安全态等综合状态实时呈现能力，通过基于多部门分级联动的安全态势监测与可视化设计，实现态势感知多级呈现与级联管理。

2.6.3 下一步实施计划

1. 安全运行平台能力提升

遵循安全能力“同步规划、同步建设、同步使用”的原则，本期方案功能规划预留了充分的能力提升空间。下一步计划将IT&OT一体化网络安全运行平台进行持续能力提升，当前安全处置仍需人工审核，在进一步积累安全场景、安全处置剧本、安全响应标准动作的帮助下，逐步完善运行平台SOAR的能力，充分结合业务分类分级管理运行，将可控低影响的安全事件，逐步依托安全剧本自动化处置，进一步提升安全处置效率，将安全运行人力进一步释放。

2. 资产暴露面监测持续完善

根据长庆油田业务的不断发展，下一步将对资产、风险、策略、组织、人员等类型数据进行融合治理，构建完整的资产地图。通过数据碰撞持续监测资产安全姿态，驱动常态化安全运行，达成持续收敛资产攻击面的效果安全响应融入整体安全运行平台体系，保障安全防护与资产暴露面同步管理、敏捷支撑。

3.解决方案行业推广

伴随着本方案标杆案例的持续运行完善，业务安全处置模型的不断积累，安全运行功能的实用落地，安全指标维度的丰富积累。下一步计划发挥长庆油田在石油行业的案例示范影响效力，在石油行业中进行构建 OT、IT 安全能力全面融合的安全运行体系解决方案的持续推广，助力石油行业网络安全产业不断发展。

2.6.4 方案创新点和实施效果

1.项目先进性及创新点

长庆油田 IT&OT 一体化工控网络安全运行体系是一种新安全效能倍增模式，本质是从实际业务发展目标和安全需求角度出发，聚焦特定生产网工控网络安全能力形成，打通工控安全系统建设、使用、管理、培训等全周期，有机整合专业人才、技术、产品、服务、流程等全要素，串接工控网络安全预防、保障、监控、应急等全流程，构建面向用户的体系化安全能力交付的“交钥匙”工程，实现从被动、静态工控网络安全系统建设管理，到主动、动态工控网络安全赋能的转变，在保障业务安全可靠的同时，滚动提升整体防御能力。

长庆油田 IT&OT 一体化工控网络安全运行体系建设思路是:创新采用集约化管理运行模式，集聚安全手段、安全能力、安全人员等资源，以扁平化方式面向用户统一提供安全服务、开展安全监管；以等级保护要求为基准建立标准化网络安全配置和运用模式，快速灵活交付各单位部署，填平补齐分散单位的防护水平；在安全运行中心的统筹下实现联合同步防御，打通风险评估、运维保障、监测预警、应急响应各环节，共享安全情报和知识库，协同执行防御任务，大幅度提升整体工控网络安全协同防御能力。

2. 实施效果

（1）打破安全孤岛、IT&OT 一体化防护

可对全网各类工控安全设备日志统一采集、管理、检索和管理分析，突破安全设备数据孤岛，从而构建覆盖全网的 IT&OT 一体化纵深防御体系。

（2）快速处置响应、统一指挥决策

通过对告警、事件、漏洞等安全隐患集中管理，将所有安全日志数据汇总并分析，按照不同维度进行大屏幕的安全态势进行综合展示，可以实现提升安全检测能力、快速响应能力及追踪溯源能力。

（3）全面安全监管、智能调度响应

以先进成熟的大数据技术，构建全面、智能、可视化的安全监管框架，建立一个全面、智能、可视化的监管中心，持续识别风险、全面掌握安全控制现状、及时监管应对内外威胁，提供可视化的整体信息安全视图，为监管部门和监管人员提供一个智能的指挥调度响应平台，为各级管理人员提供安全决策依据。

2.6.5 单位基本信息

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，在人员规模、收入规模和产品覆盖度上均位居行业第一。

中国电子信息产业集团（CEC）于 2019 年 5 月战略入股奇安信，奇安信正式成为网络安全国家队。同年 12 月，奇安信成为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商。2020 年 7 月 22 日，奇安信在科创板挂牌上市。作为中国电子信息产业集团核心网络安全企业，奇安信深度参与中国电子“PKS”信创体系，创新地把安全能力植入到飞腾 CPU 和麒麟操作系统里，让安全软件在应用层就能利用 CPU 和操作系统的能力，打破 Wintel 体系对中国的影响。目前正对“PKS”体系进行拓展升级，以更好地保障我国重要信息系统的网络安全。

奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态

势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟(CCIA)发布的2021年、2022年、2023年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

中国石油长庆油田公司(PCOC)是隶属于中国石油天然气股份有限公司（PetroChina）的地区性油田公司，总部设在陕西省西安市，工作区域在中国第二大盆地--鄂尔多斯盆地，横跨陕、甘、宁、内蒙古、晋五省（区），勘探总面积37万平方公里。公司有24378名员工，其中专业技术人员3854人，占员工总数的15.8%,高级技术专家315人，中级技术人员1165人，博士12人，硕士150人，本科学历1967人。公司拥有资产总额390.51亿元。

长庆油田作为我国第一大油气田，油气当量不断突破，目前已配套建成国内最大规模的油气生产物联网系统，油气井（站）不断快速扩增，信息化、数字化、智能化发展亟需替代人工，生产安全成为巨大挑战。目前，长庆油田正处在数字化转型的关键阶段，数字和智能化事业部的成立，会加快落实信息化建设的六统一要求，进一步提升长庆油田的管理效率，提高数字化转型的质量，为保障国家能源安全贡献更大力量，而网络安全作为数字化发展的地板工程，将全力助力长庆数智建设,筑牢网络安全屏障,为长庆油田数字化转型和智能化发展保驾护航。

2.7 案例七：5G+工业互联网的安全检测与防护综合管理服务平台——筑牢网络安全防线，护航企业安全发展

引言：比亚迪 5G+全连接工厂建设基于 5G 切片网络技术的专网，分别在比亚迪的多个厂区总计部署了 20 多个 5G 基站，构建“5GSA+MEC”云边端结合的新型网络架构和企业专网，实现了河南省首个 UPF 下沉园区，MEC 商用专网模式落地。落地了 5G+安防机器人、5G+全连接机床联网、5G+重载机械臂、5G+远程操控、5G+云化 AGV 等应用场景，实现 5G 技术与数字化设计、智能化生产和网络化服务的融合应用。

5G 网络作为比亚迪的关键基础设施，对于企业安全的重要性不言而喻，5G SA+MEC 组网下，比亚迪各个厂区信息采集的面会越来越广，数据量呈现爆发式增长的态势。因此 5G 的数据安全问题亟须解决，主要面临的安全风险可归纳为如下 8 类。

- **比亚迪多厂区间网络服务安全挑战**

在比亚迪的移动边缘架构下，接入设备数量庞大，类型众多，多种安全域并存，安全风险点增加，并且更容易实施分布式拒绝服务攻击。5G 边缘计算节点部署位置下沉，导致攻击者更容易接触到边缘计算节点硬件。攻击者可以通过非法连接访问网络端口，获取网络传输的数据。此外，传统的网络攻击手段仍然可威胁边缘计算系统，例如，恶意代码入侵、缓冲区溢出、数据窃取、篡改、丢失和伪造数据等。

- **全连接工厂硬件环境安全挑战**

相比河南移动核心网中心机房完善的物理安全措施，比亚迪边缘计算节点部署自己的机房，所处环境复杂多样，往往防护与安保措施较为薄弱，存在受到自然灾害而引发的设备断电、网络断链等安全风险，此外更易遭受物理接触攻击，如攻击者近距离接触硬件基础设施，篡改设备配置等。攻击者可非法访问物理服务器的 I/O 接口，获得敏感信息。

比亚迪的边缘节点远离移动云中心的管理，被恶意入侵的可能性大大增加，而且比亚迪边缘节点使用轻量级容器技术，但容器共享底层操作系统，隔离性更

差，安全威胁更加严重。因此，仅靠软件来实现安全隔离，很容易出现内存泄露或篡改等问题。基于硬件的可信执行环境 TEEs（如 Intel SGX, ARM TrustZone, and AMD 内存加密技术等）目前在云计算环境已成为趋势，但是 TEEs 技术在工业边缘计算、企业和 IoT 边缘计算、电信运营商边缘计算等复杂信任场景下的应用，目前还存在性能问题，在侧信道攻击等安全性上的不足仍有待探索。

● 比亚迪工业互联网平台安全挑战

5G 边缘计算平台 MEP 本身是基于虚拟化基础设施部署，对外提供应用的发现、通知的接口。攻击者或者恶意应用对 MEP 的服务接口进行非授权访问，拦截或者篡改 MEP 与 APP 等之间的通信数据，对 MEP 实施 DDoS 攻击。攻击者可以通过恶意应用访问 MEP 上的敏感数据，窃取、篡改和删除用户的敏感隐私数据。

● 终端应用安全挑战

比亚迪的边缘计算节点连接海量的异构终端，承载多种全连接工厂的应用，终端和应用之间采用的通信协议具有多样化特点，多数以连接、可靠为主，并未像传统通信协议一样考虑安全性，所以攻击者可利用通信协议漏洞进行攻击，包括拒绝服务攻击、越权访问、软件漏洞、权限滥用、身份假冒等威胁。

比亚迪企业的应用种类繁多，随着承载高可靠、低延迟类应用，边缘计算平台上更容易受到 Doss 攻击，从而造成重大的损失。由于边缘计算节点的资源受限，可能因为缺乏有效的数据备份、恢复、以及审计措施，导致攻击者可能修改或删除用户在边缘节点上的数据来销毁某些证据。

● 管理安全挑战

管理安全威胁主要包括恶意内部人员非法访问、使用弱口令等。对于比亚迪将意味着有大量的应用节点需要进行管理和运维。

为了节省人力，若依赖远程运维，如果升级和补丁修复不及时，会导致攻击者利用漏洞进行攻击。

● 数据安全挑战

比亚迪工业互联网平台可收集、存储与其连接设备的数据，包括应用数据、用户数据等。其数据面临的安全风险包括数据损毁风险、数据泄露风险。

2.7.1 方案概述

本方案基于比亚迪5G+全连接工厂环境的威胁防护识别、软件定义安全、人工智能安全分析研判和UEBA等技术建设5G网络安全防护系统，系统实现了如下安全防护内容:

远控业务安全—边缘主机安全防护：利用边缘轻量agent与云端联动的方式实现比亚迪虚拟机安全可视化管理和检测。以风险分析为基础，入侵监测为核心、管理加固为辅助，确保比亚迪生产环境安全。

大流量实时安全分析：对于大视频实时回传需求，网络边缘数据流量将大幅提升，现有网络中部署的防火墙等安全设备在流量检测、链路覆盖、数据存储等方面将难以满足超大流量下的安全防护需求，采用NTA流量采集技术，对流量进行深度解析分析，实现流量中的通联记录和传输内容进行深度分析。

业务安全监测：通过NTA采集解析的信令数据，运用大数据、机器学习算法主动监测并预防5G网络比亚迪令交互带来的风险，对网络安全事件深度挖掘，结合网络的基础设施情况和运行状态，对网络安全态势做出评估，对未来可能遭受的网络攻击进行预测，提供针对性的预防建议。

资产探测与漏洞扫描主动获取工厂资产与漏洞，通过前台业务使用者、管理用户视角对系统业务和系统进行安全风险分析，揭示漏洞存在。

拟态诱捕补充全连接工厂网络边界安全，提升安全威胁入侵防护能力。

综合智能基线分析提升全连接工厂安全预警水平：利用聚类、决策树、强化学习等手段，将人工智能技术融入全连接工厂中，形成一系列的智能检测基线，降低网络安全和业务安全等风险，缩短应急响应时间，为智能化运营提供支撑。

项目主要功能分解为如下子系统实现:

1)MEC安全云平台

2)边缘安全保护引擎

3)边缘侧5G核心网安全保护子系统

4)用户监控与审计子系统

5)物理探针流量采集子系统

6)虚拟化流量采集子系统

7)威胁感知检测子系统

8)防火墙子系统

9)主动诱骗服务子系统

10)病毒及僵木蠕、钓鱼查杀子系统

11)虚拟安全补丁服务子系统

12)DDoS 攻击防护子系统

13)威胁防护处理子系统

1. 方案背景

在新能源汽车领域，中国逐渐崛起成为全球的重要影响力，而在这个充满机遇与挑战的赛道上，中国新能源汽车市场变得日益拥挤，各个新兴品牌纷纷涌现，竞争愈发激烈。在这个充满活力的环境中，比亚迪作为中国新能源汽车领军企业，正面临着前所未有的挑战和压力。

在这种背景下，提升产能成了比亚迪当下的重要课题。随着市场需求的增长，比亚迪需要迅速扩大生产规模，以满足日益增长的订单和市场需求。然而，面对新能源汽车市场的不确定性和技术变革，如何在保持质量和效率的同时实现产能的提升，是比亚迪需要克服的难题。

比亚迪不仅需要关注技术创新，还需要优化生产流程、提高供应链的协同效率，并在市场竞争中找到差异化的竞争策略。面对新能源汽车领域的多方面挑战，比亚迪必须保持敏锐的市场洞察力和持续的创新能力，以在激烈的竞争环境中取得持续的成功。

2. 方案简介

本项目的定位为向比亚迪提供 5G+全连接工厂安全整体解决方案。通过部署，不仅向比亚迪 5G+全连接工厂补充基础架构和设施的安全防护能力，同时也为比亚迪提供持续运营 5G+全连接工厂安全风险的监测工具。

3. 方案目标

1)支持多级部署和统一管理，对 MEC 设备带宽、网络延时等性能影响总体不大于 5%。

2)依照安全功能支持不同 MEC 网元，支持自动部署、适配多类型网元加载不同安全功能。

3)支持对已知威胁阻断，可定义网络阻断机制规则，防 DDoS 攻击、阻止非法访问，进行七层内容过滤，采用虚拟补丁防护已知网元漏洞，查杀病毒、木马、蠕虫、钓鱼等威胁。

4)支持可疑威胁检测，利用 UEBA 检测恶意威胁行为、利用机器学习检测威胁事件，具备调查取证、危害隔离、损害清除等能力。

2.7.2 方案实施概况

1. 方案总体架构和主要内容

本项目的定位为向比亚迪提供5G+全连接工厂安全整体解决方案。通过部署，不仅向比亚迪5G+全连接工厂补充基础架构和设施的安全防护能力，同时也为比亚迪提供持续运营5G+全连接工厂安全风险的监测工具。

本项目总体功能架构如下图所示。产品由五个层面的功能组件实现，分别为可视化层、中心安全云业务层、边缘安全编排层、安全能力系统层、数据采集层。

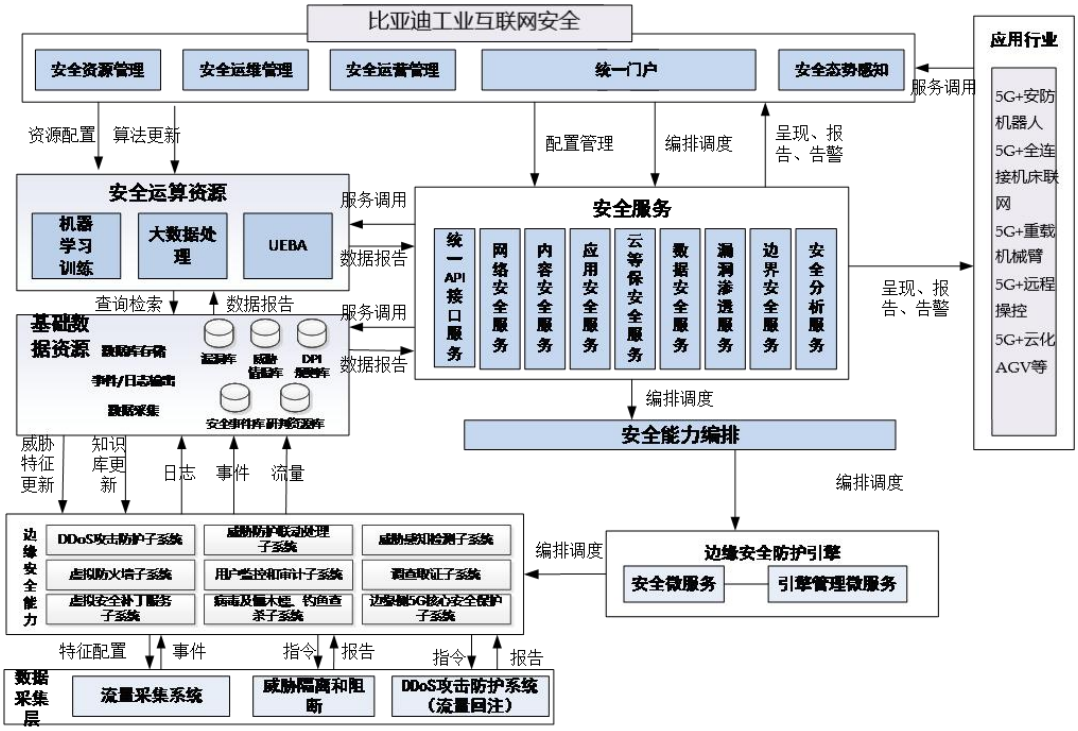

图 7-1 总体功能架构

在可视化层，产品通过安全统一管理平台为比亚迪5G+全连接工厂提供安全

资源管理、安全运维管理、安全运营管理、统一门户、安全态势感知服务。

在中心安全云业务层，产品通过安全云实现比亚迪5G+全连接工厂基础数据资源统管、安全运算资源统管、安全能力编排。MEC安全云支持统一API接口服务、网络安全服务、内容安全服务、应用安全服务、云等保安全服务、数据安全服务、漏洞渗透服务、边界安全服务、及安全分析服务。通过整合数据、运算、安全服务能力为5G+安防机器人、5G+全连接机床联网、5G+重载机械臂、5G+远程操控、5G+云化AGV等5G应用。

边缘安全能力层部署适应VI环境的虚拟机安全等服务能力，这些能力由DDoS攻击防护系统、威胁感知检测系统、威胁防护处理系统、虚拟防火墙系统、用户监控及审计系统、蜜网溯源服务系统、虚拟安全补丁服务系统、病毒及僵木蠕、钓鱼查杀系统以及边缘侧5G核心安全防护系统。

边缘安全编排层由安全微服务和引擎管理微服务构成。边缘安全编排层均部署于边缘MEC节点的虚拟化技术设施（VI）中。在虚拟化安全防护实施的初期，产品为避免重复研发NFV适配的重复性开销，以边缘安全防护引擎充当NFV和安全（保护功能）微服务间的中间层，实现NFV标准处理的快速实施。

数据采集层主要提供信令面和数据面的流量采集，并对采集到的信令面流量进行分发，对用户面流量进行筛选和过滤。由物理探针流量采集系统（物理探针）、威胁隔离和阻断、DDoS攻击保护系统等组成，实现本系统在物理网络层面的流量采集、阻断、隔离和必要的流量回注处理。

2. 具体应用场景和安全应用模式

面向工业企业，提供流量安全检测、暴露资产测绘、漏洞风险检测等服务；面向行业监管，提供行业安全风险监测、安全核查、事件通报等服务。本案例在移动具有可复制性，广泛应用于工业互联网领域，为工业企业提供一站式的安全保障服务。

3. 安全及可靠性

在安全层面，平台构建纵深防御体系，采用数据加密、身份认证、访问控制等技术防范网络攻击，结合 AI 驱动的威胁检测与实时监控系统，快速识别并阻断异常行为，确保工业数据全生命周期安全；在可靠性方面，依托高可用架构设

计、冗余容灾机制及设备健康管理功能，实现关键业务连续性，同时通过工业协议深度解析、漏洞修复与固件升级机制，提升设备及系统的抗风险能力。平台需满足工业场景严苛的实时性、稳定性要求，并通过安全合规认证，为智能制造提供可信赖的数字化底座。

4. 其他亮点

经济效益：通过实施智能化改造，比亚迪核心业务指标大幅提升：设计、工艺节省 40%以上的生产服务时间，产品研制周期缩短 50%；实现图纸、工艺无纸化，每年节约 200 万。工人每天节省生产准备时间 1 小时/每台机床，机床利用率提高 15%以上；生产效率提高 30%。提高质量管理水平，降低产品不良品率 30%。管理成本降低 30%以上，能源利用率提高 20%以上。

社会效益：比亚迪将借助本次项目带来的数字化转型契机，对生产制造行业的整个价值链产生了影响，包括与上流供应商整合数据、实现开放式创新、打造智能工厂、与“数字消费者”互动。形成创新土壤环境，发掘并且培养了大批高端技术型人才，提高了人力资源质量，减轻了就业压力，肩负起社会责任。

2.7.3 下一步实施计划

（1）基础建设强化

完善平台分层架构（边缘层、网络层、平台层、应用层），推进设备协议兼容与异构数据统一治理；

开展工业资产全量测绘与漏洞基线管理，完成高危设备固件升级与安全补丁覆盖；

建立符合行业标准（如等保 2.0、IEC 62443）的合规性框架，通过第三方安全认证。

（2）智能化能力升级

深化 AI 在威胁狩猎、异常流量分析中的应用，构建基于行为分析的零信任动态访问控制模型；

开发工业场景定制化攻击链仿真平台，提升 APT 攻击、勒索软件等高级威胁的主动防御能力；

推动“安全即服务”（SECaaS）模式，支持微服务化安全组件的灵活部署与策略编排。

（3）生态协同与场景适配

联合设备厂商、云服务商、安全企业共建威胁情报共享联盟，实现跨平台联防联控;

针对典型场景（如能源、制造）细化安全基线，设计低时延、高可靠的轻量化边缘安全方案;

建立工业安全人才培养体系，开展攻防演练与应急响应实战化培训。

（4）可靠性持续优化

推进分布式冗余架构与无感热升级技术,保障关键业务在攻击或故障下的分钟级恢复能力;

构建设备健康度预测模型，通过数字孪生技术实现故障预判与风险自愈。

通过分阶段落地、迭代验证，最终形成覆盖“感知-防护-响应-恢复”全链条的工业互联网主动免疫体系。

2.7.4 方案创新点和实施效果

1. 方案先进性及创新点

1）技术融合创新

AI 驱动的主动防御体系：结合机器学习与工业知识图谱，实现威胁的精准预测与自动化响应，突破传统被动防御模式。轻量化边缘安全架构：针对工业现场资源受限场景，研发低功耗、低时延的边缘安全网关，支持协议深度解析与实时入侵检测。数字孪生安全验证：通过构建物理设备与虚拟孪生体的双向映射，实现攻击模拟、漏洞预判及安全策略的动态优化。

2）机制与模式创新

零信任动态访问控制：基于设备行为画像与上下文感知，动态调整权限，解决传统静态授权在工业环境中的僵化问题。工业威胁情报共享联盟：联合产业链上下游企业，形成跨行业、跨区域的威胁情报协同防御网络，提升全局安全态势

感知能力。安全即服务（SECaaS）：以微服务架构提供按需订阅的安全能力（如漏洞扫描、日志审计），降低中小企业安全部署门槛。

3）生态协同创新

工业协议兼容性增强：支持 OPC UA、Modbus 等主流工业协议的深度解析与安全加固，打破异构设备互联的安全瓶颈。标准化合规框架：结合等保 2.0、IEC 62443 等国内外标准，形成可复用的行业安全基线，推动生态统一。

2. 实施效果

比亚迪 5G+全连接工厂安全防护平台，试运行 5 个月后，工控网络安全事件监测审计效果如下：自动发现资产共计 1032 台；监测非法通信和威胁事件共计 56 起；检测工控漏洞共计 32 个。5G 全流量安全监测溯源效果如下：累计监测各类安全威胁事件 20 万起；通过 AI 基线建立监测应用网络和业务交互的质量，包括流量、数据包、响应时间等的业务异常实时告警；发布网络安全报告 3 篇，对相关重点的网络安全事件进行详细分析，为客户提供具体的处置方法。整个项目在为工厂客户提供网络安全建设同时，也相应的提供持续的网络安全服务，从而确保 5G 工厂网络健康有序发展。

2.7.5 单位基本信息

恒安嘉新（北京）科技股份公司是一家专注于网络空间安全综合治理的高新技术企业，深耕工业互联网安全领域多年，致力于为能源、制造、交通等关键基础设施行业提供全场景、智能化的安全防护解决方案。公司以“自主可控、安全可信”为核心理念，依托大数据、人工智能、威胁情报等前沿技术，构建了覆盖工业互联网全生命周期的安全防护体系。在工业互联网安全领域形成了三大核心能力：工业资产识别与管理、工控协议深度解析和异常行为智能检测。其自主研发的“星尘-工业互联网安全监测平台”通过主动探测与被动流量分析技术，实现工业资产动态测绘、脆弱性评估和威胁实时预警，可精准识别 Modbus、OPC、S7Comm 等 50 余种工业协议，支持对 PLC、DCS 等关键设备的异常操作监测。同时，公司推出“天盾-工业防火墙”“磐石-工业安全审计系统”等系列产品，形成覆盖边界防护、入侵检测、日志审计的纵深防御体系。作为工信部工业互联网

安全分类分级管理核心支撑单位，恒安嘉新牵头制定 3 项行业标准，获得 CNCERT 工业安全应急服务资质、等保 2.0 工业控制系统安全扩展要求测评资格。2022 年入选工信部“工业互联网安全深度行”活动优秀技术供应商，服务覆盖 3000 余家工业企业，防护关键生产设备超 10 万台。

郑州比亚迪汽车在新能源汽车领域迅速崛起，已成为行业内的重要力量。公司经营范围广泛，涵盖汽车零部件及配件制造、新能源汽车整车销售、汽车零部件研发等多个领域。在工业互联网的赋能下，郑州比亚迪工厂实现了智能化转型升级。工厂通过构建高质量的行业虚拟专网，下沉 5G MEC 云平台，结合工业 AI 平台，实现了十余种工业互联网融合创新应用。在生产过程中，工业视觉取代了传统的 “人眼 + 人脑” 检测方式，大幅提升了工厂管理效率与生产效率，车标错漏贴率降为 0，车窗涂胶不良品流出由之前的每月 1 - 2 例降到 0，实现了企业精益化管理。同时，基于物体识别、人员 / 车辆跟踪和场景语义分割等 AI 算法，对车间生产安全场景进行实时监测告警，有效降低了工厂安全监管成本和安全事故风险。

此外，郑州比亚迪还引入 “璇玑” 工业互联网平台，构建生产线的虚拟仿真模型，实现工艺参数实时优化，将链条生产线的良品率提升至 99.6%。双方共建的 AI 检测系统，针对微型链条缺陷识别准确率达 99.9%，检测速度较传统方式提升 20 倍，应用于精密零部件来料检验环节，保障了产品质量。

2.8 案例八：基于工业互联网平台打造一体化网络安全监测服务体系——充分发挥基础电信网络安全资源和技术优势，赋能工业企业提升网络安全防护水平

引言：中国移动通信集团山东有限公司（以下简称“山东移动”）隶属于中国移动通信集团有限公司，组建于1999年7月，主要经营移动通信、固定通信以及互联网接入服务等。目前山东省内规模最大的通信企业。在上级单位指导下，山东移动网络安全技术能力建设逐步成熟，目前已具备工业互联网态势感知系统、移动互联网恶意程序监测系统、僵木蠕监测系统、互联网专线信息安全管理系统、IDC/ISP信息安全管理系统、漏洞管理系统、资产管理平台、域名信安系统、安全能力引擎等技术能力。

近年来，山东省深入实施工业互联网创新发展战略，紧抓国家级工业互联网示范区建设机遇，先后出台多个“互联网+先进制造业”相关指导性文件，纵深推进“工赋山东”专项行动。在山东省通信管理局组织牵头，山东移动与省内五家单位共同组织联合体，形成省级工业互联网安全态势感知平台。作为“国家-省级-企业”三级工业互联网安全技术监测平台功能主体，不仅承担省内工业互联网安全监管、风险通报、追踪溯源、威胁处置、数据共享等重任，同时为国家平台、企业平台提供了上下协同、数据共享等能力。

2.8.1 方案概述

山东移动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，基于工业互联网安全态势感知平台打造一体化网络安全监测服务体系，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。面向山东省内重点工业产业园区、各类工业互联网企业、标识解析企业、专线接入企业等，提供工业互联网安全监测服务能力，赋能工业企业健康可持续发展。

1. 方案背景

2021 工信部印发《工业互联网创新发展行动计划（2021-2023 年）》提出，统筹工业互联网发展和安全，提升新型基础设施支撑服务能力，拓展融合创新应用，深化商用密码应用，增强安全保障能力，壮大技术产业创新生态，实现工业互联网整体发展阶段性跃升，推动经济社会数字化转型和高质量发展。

2023 年 3 月，山东省工信厅印发《山东省工业和信息化厅关于印发“工赋山东”2023 年行动计划的通知》提出，以服务支撑制造经济、数字经济、民营经济“三个经济”为重点，以推动制造业数字化转型为突破口，统筹推进网络、平台、应用等体系建设深入实施“工赋山东”专项行动，加快工业互联网规模化应用，推动国家级工业互联网示范区建设迈上新台阶。

为了强化工业互联网的安全保障水平，提升其识别和安全监测发现能力，充分发挥基础电信网络安全资源和技术优势，推动安全技术能力应用赋能，山东移动面向工业互联网等重点场景，在省通信管理局等上级单位指导下打造省级工业互联网安全态势感知平台，为山东省工业互联网企业的网络安全生产提供强大的支持和保障，有效赋能企业提升网络安全防护水平，促进安全监测应用场景拓展，服务模式创新、服务成效提升，从而有力地推动新型工业化沿着健康、稳定、可持续的轨道稳步发展。

2. 方案简介

（1）打造省级工业互联网安全态势感知平台

山东移动省级工业互联网安全态势感知平台利用大数据、云计算、人工智能等分析技术，云、管、边、端一体化安全管控技术，构建省级、企业级二级安全分析监管平台。作为“国家-省级-企业”三级工业互联网安全技术监测平台功能主体，不仅承担省内工业互联网安全监管、风险通报、追踪溯源、威胁处置、数据共享等重任，同时为国家平台、企业平台提供了上下协同、数据共享等能力。

（2）打造工业互联网一体化网络安全监测服务体系

面向山东省内重点工业产业园区、各类工业互联网企业、标识解析企业、专线接入企业等，基于工业互联网安全态势感知平台打造一体化网络安全监测服务体系，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。通过态势信息推送、安全服务订阅、安全分析报告等服务模式，提供网络安全监

测、态势感知、资产管理、风险分析、风险预警、拦截处置、专项分析等服务内容，做到了工业互联网安全保障的闭环，并赋能工业企业提升安全防护能力。

3. 方案目标

强化工业互联网的安全保障水平，提升其识别和安全监测发现能力，充分发挥基础电信企业网络安全资源和技术优势，为山东省工业互联网企业的网络安全生产提供强大的支持和保障，有效赋能企业提升网络安全防护水平，重点解决以下问题。

（1）解决企业网络安全能力防护薄弱的问题

许多工业设备使用的是老旧设施，在设计之初往往缺乏安全考虑，自身网络安全防护能力不足，存在开放高危端口、未安装防病毒软件、缺乏严格的身份认证等风险，容易遭受恶意软件和木马病毒入侵，对工业企业构成了严重的安全威胁。通过工业互联网安全态势感知平台可以进行网络安全威胁或暴露面监测，即使发现风险、整改加固，提升网络安全防护能力。

（2）解决企业网络安全运营成本高的问题

平台为工业互联网企业提供了强大的安全防护能力，显著减少了企业在安全设备、人员和培训等方面的投入。以某工业互联网企业为例，在未使用平台之前，企业每年需投入约 30 万元用于采购防火墙、入侵检测系统等安全设备，雇佣 3 名安全专业人员，年度培训费用约 8 万元。使用平台后，企业安全设备采购投入降低至 10 万元，安全人员减少至 1 名，培训费用降至 2 万元，每年可节省运营成本约 26 万元。

（3）解决企业正常生产运营稳定性的问题

通过工业互联网安全态势感知平台可以进行网络安全威胁或暴露面监测，即使发现风险、整改加固，提升网络安全防护能力。帮助企业有效规避因为勒索病毒、DDoS 攻击等网络安全风险导致企业停产等经营风险。平台的实时预警和应急响应功能帮助企业快速应对安全威胁，有效降低了企业因网络安全事件导致的经济损失风险，提高企业运营稳定性。

（4）解决企业因为新技术带来的安全问题

随着 5G 和工业互联网深度融合，5G 技术的高速率、低时延、大连接等技术能力促进了工业企业生产效能大幅提升。在 5G 工业互联网应用场景中，CT、IT、OT 深度融合已成为必然趋势，在提升效能的同时也增加了互联网资产暴露面，网络安全风险日益增大，整体威胁的发现、感知、响应和处置变得困难。

2.8.2 方案实施概况

工业互联网的核心在于将传统工业设备与信息技术结合，实现智能化管理和控制。这种转型极大地提高了生产效率，但也使工业系统暴露在网络攻击的威胁之下。新一代信息技术的快速发展带来了巨大的机遇，也伴随着严峻的网络安全挑战。算力网络、5G、边缘计算、区块链、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，为工业互联网安全带来新挑战。随着新技术的不断引入，工业互联网安全应用场景也需要不断深入拓展。通过加强安全标准、监测防护、管理设备系统、提升安全意识及促进技术合作，保障数字化转型安全。

1.项目总体架构和主要内容

（1）顶层架构设计

基于工业互联网安全态势感知平台打造一体化网络安全监测服务体系，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。面向重点工业产业园区、各类工业互联网企业、标识解析企业、专线接入企业等，通过态势信息推送、安全服务订阅、安全分析报告等服务模式，提供网络安全监测、态势感知、资产管理、风险分析、风险预警、拦截处置、专项分析等服务内容，做到了工业互联网安全保障的闭环，并赋能工业企业提升安全防护能力。

图 8-1　顶层架构设计

（2）主要服务内容

1）企业资产探测

在运营商大网上通过被动接收流量分析为主，加特定 IP 主动探测的模式来识别暴露在公网上的工业互联网 IP 资产，探测维度包括设备类型、厂家、操作系统、数据库、开放的端口和服务，针对工业平台，进行深入探测，识别出工业互联网 IP 归属行业/单位/地理位置信息、协议开放端口、并对资产分布进行画像等，从而输出山东移动全省工业企业资产识别信息。

2）全省企业安全态势感知

集中展示呈现出区域内工业互联网联网或暴露的工业资产、工业 APP 等情况，以及工业互联网协议应用情况，可按照行政区域、行业分布、业务特点等划分维度。

3）企业用户态势感知

针对特定的企业提供定制化的企业安全事件展示页面，通过分析企业暴露面数据，结合平台的安全事件规则，可直观展示企业面临的安全状况，包括：被攻击的 IP、安全事件类型部分、攻击详细、攻击来源归属地、安全事件的发展趋势等情况。

4）网络安全威胁追踪溯源

平台支持对威胁进行溯源，能根据威胁情报数据和上传的安全威胁分析数据，对攻击者进行关联分析溯源。

溯源功能主要包含以下几个方面：

- 能够根据威胁情报数据进行反查，关联出该攻击的身份信息（包含并不仅限于 IP 地址、地理位置信息等）。
- 能够关联分析出该攻击者的历史攻击信息（包含并不仅限于历史攻击的资产等）。
- 能够对该攻击者的历史攻击信息进行攻击取证（包含并不仅限于攻击对象和攻击频率）。

5）网络安全风险预警通报

可提供网络安全事件的验证工作，可通过可定制化模板自动输出工业网络安全事件监测处置通报，可通过短信及邮件的方式向相关人员进行下发。监管单位下发《网络安全风险告知书》，督促企业予以整改。

6）网络安全风险处置

发现网络安全风险，可提供网络安全威胁处置服务，包括基于移动恶意程序监测系统的拦截处置、基于城域网僵木蠕监测系统的拦截处置 、基于互联网专线管理系统的拦截处置、基于 IDC/ISP 管理系统的网站关停处置、基于 DNS 系统的 DNS 解析处置服务。

2.网络、平台互联架构

山东移动工业互联网安全态势感知平台主要通过对关键网络节点的网安系统（移动互联网恶意程序监测系统、僵木蠕监测系统、互联网专线信息安全管理系统、IDC/ISP 信息安全管理系统）软件改造以及互联网专线溯源取证系统，实现对关键网络节点的工业互联网流量采集、协议解析，监测暴露在公网上的安全事件、工业互联网资产信息、工业互联网应用协议等数据。接收关键网络节点网安系统的监测结果数据进行存储、分析，实现工业互联网资产的通联日志、安全事件等数据的专项监测，实现山东移动工业互联网企业安全监测预警功能，实现对工业互联网资产的精准识别，开展全面的安全风险分析，达成风险预警的高效联动、威胁处置的协同合作、安全态势的精准分析、信息资源的充分共享以及自身安全防护的显著强化等功能。

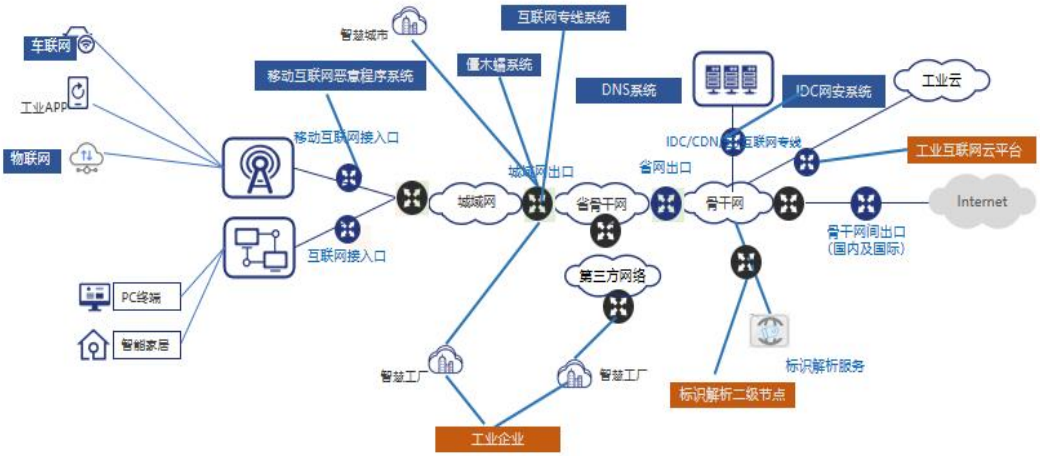

图 8-2　工业互联网平台所涉及网络、平台互联架构

3.具体应用场景和安全应用模式

（1）工业传统安全风险应用场景

借助平台优势，能够为工业互联网企业打造全方位的大网防护体系。在防护过程中，着重针对企业暴露面资产展开多层次的安全防护举措。首先，充分利用基础电信运营企业所具备的大网安全监测和防护能力，为企业构建起第一道坚固的 “防火墙” 防线。这道防线能够对网络流量进行实时监测和过滤，有效抵御外部非法访问、端口扫描、入侵攻击等常见的网络层攻击行为。

与此同时，平台还会结合威胁情报信息，与企业自身部署的防火墙、入侵防御系统（IPS）、主机防护等设备和系统进行协同联动。通过这种方式，能够为企业明确防护的重点方向，实现更具针对性的安全防护。特别是针对企业的各类 Web 应用，平台提供了严格的保护措施。能够精准识别并防止 SQL 注入、跨站脚本攻击等常见的 Web 应用入侵行为，以及有效避免文件上传漏洞、信息泄漏等安全问题的发生，从而确保企业 Web 应用的安全稳定运行。

（2）工业互联网+新技术安全风险应用场景

场景一 工业互联网+5G 场景

5G 技术提升网络速度同时增加攻击面，在 5G 工业互联网应用中，CT、IT、OT 一体化已成为必然趋势，CT-IT-OT 的融合对工业生产环境带来了新的风险，整体威胁的发现、感知、响应和处置变的越发困难。需要进一步加强 5G+工业互

联网安全监测系统，对 5G+工业互联网设备资产、数据资产进行实时监测和风险感知。

场景二 工业互联网+AI 场景

人工智能提高生产效率的同事增加了数据安全风险，在智慧工业园区建设中，众多感知设备的广泛应用使得大量敏感数据被采集，而数据的传输过程中容易受到黑客攻击、数据泄露等风险威胁。需要进一步加强数据安全防护，实现对数据安全事件的统一监测、预警、指挥调度、协同处置，增强数据安全整体治理水平和实战化能力。

4.安全及可靠性

根据工业企业网络安全需求，基于“事前监测、事中处置，事后加固”原则，为企业提供全生命周期网络安全管理服务。通过事前感知工业互联网企业，发现工业互联网资产，识别工业互联网威胁等服务，有效低于网络安全威胁。通过事中高效应急响应，协同联动处置，快速拦截网络安全风险，降低企业损失，维护企业运营稳定性。通过事后专项分析，整改加固等，全面提升工业企业网络安全防护水平。

2.8.3 下一步实施计划

1.升级平台数据，提升安全监测能力

按照部省关于护航新型工业化网络安全专项行动方案要求，升级 5G+工业互联网安全态势感知平台，将运营商 5G 工业互联网安全事件数据、5G 工业园区安全事件数据、物联网卡基础数据、Netflow 数据等接入管局侧平台，提升全省工业互联网网络安全监测能力。

2.拓展服务模式，提升企业防护水平

聚焦工业互联网安全、工控安全等场景，围绕风险在线监测、态势信息推送等方向，拓展服务模式。完善工业领域网络安全监测处置和通报机制，强化工业领域网络安全赋能服务，加强网络安全政策宣贯培训，开展网络安全体检评估，以评促改促建提升企业安全防护水平。

3.深化护航行动，提升综合保障能力

配合监管单位积极开展省内 IP 地址报备信息清查处理工作，提高 IP 地址备案数据准确性，更好为省内工业互联网企业提供安全服务。深化工业互联网安全分类分级及车联网定级备案，督促指导企业排查问题隐患、强化分级防护、开展符合性测评等工作。

2.8.4 方案创新点和实施效果

1.方案先进性及创新点

（1）基于知识图谱关联和自动化分析技术创新，提升工业互联网数据分析能力。

工业企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。利用知识图谱关联可实现对网络空间实体基础属性、网络行为、安全事件、威胁情报的全方位刻画。通过平台增加自动化研判功能，对网络攻击告警进行筛选，将有普遍性的告警无需人工干预可直接进行自动化研判，运营人员只需对复杂的告警进行人工研判、分析，从而大大提升事件研判数量和研判工作效率。

（2）基于多元数据降噪和 AI 技术创新，提升工业互联网威胁告警能力。

利用多元数据降噪剔除噪音和异常数据，采用了智能分类和标记的方法，对数据进行精细化处理。利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，形成工控网络安全在各场景的安全分析与追踪溯源能力。通过引入了深度学习技术，能够自动学习和识别复杂的恶意模式。通过大量的训练数据，模型能够精准地判断出潜在的恶意行为，不仅局限于已知的攻击模式，还能对新型的、变种的恶意活动进行有效的检测。

（3）基于数字化、集约化和服务化的公共服务技术创新，提升工业互联网安全服务成效。

在省通信管理局、省工信厅指导下，协同基础电信企业建立集约化安全支撑

服务资源队伍，同时面向工业企业提供“一站式”安全服务，以省级工业互联网态势感知平台为数字化技术底座，为工业企业提供对常安全监测预警、研判分析能力，提升响应处置效率。帮助各企业提高安全防护意识，显著提高安全防护水平。降低企业网络安全部门的管理成本。

（4）基于多级协同、信息共享、联动处置机制创新，提升网络安全应急处置效率。

建立多级联动、信息共享机制，实现国家、省、企业三级平台间的安全监测数据上报、威胁信息共享及安全事件处置。同时可面向省内管理部门，提供工业互联网安全态势分析、监管数据支撑，掌握重大安全风险及存在风险的企业信息，感知宏观安全态势，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，有效提高应急响应与处置效率。

（5）基于“工业互联网+”思想深度拓展网络安全监测服务应用场景

在传统工业互联网安全风险基础上，基于“工业互联网+”思想，深度分析工业互联网与5G、云计算、大数据、边缘计算、区块链等新一代信息技术融合应用场景下网络安全风险，拓展新型网络安全服务应用场景。在拓展新型网络安全应用场景的基础上，采用云、网、边、端一体化安全管控技术，提高工业企业在安全生产过程中，网络安全风险监测、分析研判、响应处置等防护能力。

2.实施效果

（1）监测成效

2024年，安全平台累计监测到工业企业31833家（较去年增加1212家），其中规模以上企业13386家（较去年增加650家），居全国前列；监测到平台（含物联网平台、车联网平台）1039个，工业互联网资产172372个，识别到设备（工控设备、物联网设备、车联网设备）814.85万个。监测发现存在2071个安全漏洞，涉及省内1381家企业，其中济南、青岛地发现漏洞数量较多。由各类漏洞引发的主要安全问题为“拒绝服务”，涉及漏洞数量969个，占比46.79%。

（2）赋能成效

为强化山东移动工业互联网安全监测服务推广，目前山东移动已将面向工业互联网的安全监测服务纳入山东移动“1+1+3”安全能力运营体系。通过建设“1+1+3”安全能力运营体系（建设 1 个网络安全运营管理平台，1 个安全能力引擎，引入、新建及改造 3 个方面的能力），纳管拉通 O/B/S 三域安全资源实现统一的大安全运营，实现安全能力产品自动下单、开通、计费全流程一体化管理、运营；异构网元能力的统一封装、统一调度，实现安全能力的对外赋能。根据客户需求分析，面向行业客户和中小企业，提供多场景安全防护服务，规划打造标准产品+安全服务+安全解决方案，做强对外服务能力。协同保障重点行业在与其他行业融合发展中的业务安全，具有较好的社会和经济成效。

（3）社会效益

山东省作为工业大省，深入实施“工赋山东”专项行动，以服务支撑制造经济、数字经济、民营经济“三个经济”为重点，以推动制造业数字化转型为突破口，统筹推进网络、平台、应用等体系建设，深入实施“工赋山东”专项行动，加快工业互联网规模化应用。山东移动通过打造工业互联网监测服务体系，护航山东工业互联网高质量发展，为推动国家级工业互联网示范区建设迈上新台阶助力。

一是提高企业安全生产水平。通过“工业互联网+安全生产”模式，企业可以实现安全风险的辨识和计划、隐患治理的管理以及应急管理能力的提升。新一代信息技术的应用使得安全生产从静态分析向动态感知转变，从事后应急向事先预防转变，从单点防控向体系化防控转变。2020 年 12 月至 2024 年 8 月，山东移动支撑监管单位安全监测能力，通信管理局共下发 1051 份《网络安全风险告知书》，督促企业予以整改，帮助企业减少因网络安全风险带来的损失，提升整体安全水平。

二是护航工业企业转型升级。工业互联网作为全要素、全产业链、全价值链连接的枢纽，能够连接生产信息和需求信息，有效实现资源高效配置，促进产业生态协同发展。它能够与制造、能源、交通、建筑、农业等实体经济进行深度融合，推动各行业的转型升级。工业互联网安全作为国家安全的重要组成部分，事关经济发展和社会稳定。通过提高工业互联网安全防护能力，能够护航工业企业

高质量发展，维护社会发展稳定性。

3. 结束语

编制工业互联网典型案例并进行示范推广是工信部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。

本报告面向物联网、5G 泛终端、5G 专网等新技术新场景，能源、汽车、电力等重要行业，以及自适应安全防御体系、安全诊断系统提供安全解决方案和+建设经验，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。