中国移动 China Mobile | ZTE中兴

5G+工业互联网安全白皮书

参与编写单位：

中国移动通信集团有限公司

中兴通讯股份有限公司

中国信息通信研究院

北京邮电大学

三一重工股份有限公司

鞍钢集团自动化有限公司

江苏精研科技股份有限公司

哈尔滨电气集团有限公司

宝武集团韶关钢铁有限公司

编写组成员：

张滨、陆平、袁捷、俞承志、王继刚、张峰、李祥军、王庆、于乐、徐高峰、田慧蓉、郝晓龙、张静、张弘扬、滕志猛、邱勤、赵维铎、郝振武、江为强、程渤、赵帅、林兆骥、李珊、张瑜、魏立平、陈凯、常静、胡晶晶、许志成、王乙鸾、辛毅、杨志远、游世林、李溦

技术联系：

于乐 yule2020@139.com

徐高峰 xu.gaofeng1@zte.com.cn

前言

工业互联网是中国制造智能化、信息化的重要手段，将加速“中国制造”向“中国智造”转型，并推动实体经济高质量发展。党中央、国务院高度重视工业互联网发展，习近平总书记连续四年对推动工业互联网发展做出重要指示。在 2020 年 2 月 21 日，中央政治局会议再次强调，要推动工业互联网加快发展。

2020 年 3 月 4 日，中央政治局常委会作出加快新型基础设施建设进度的重要部署，5G 和工业互联网以其巨大的社会效益和经济效益被同时纳入“七大新基建”。5G 网络的高带宽、低时延、海量连接等特性与工业互联网的需求相吻合，必将成为工业数字化转型的关键基础设施。5G 与工业互联网的融合创新发展，将推动制造业从单点、局部的信息技术应用向数字化、网络化和智能化转变，其叠加倍增效应和巨大应用潜力将不断释放，同时也为 5G 开辟更为广阔的市场空间，从而有力支撑制造强国、网络强国建设。

随着 5G 网络的深度融入，工业网络边界也在不断的延伸，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。要让 5G 网络安全地赋能工业互联网，传统的安全解决方案不能满足所有的需求，必须要建立统一的 5G 工业互联网安全架构，基于工业互联网业务场景提供定制化的 5G 网络安全解决方案，加强工业互联网安全技术保障手段及数据安全防护技术手段建设，才能保障 5G+ 工业互联网行稳致远。

本白皮书针对智能制造、电网、矿山、港口等工业垂直行业在引入 5G 后的普适性安全需求，为 5G+ 工业互联网应用场景的安全防护提供参考。

本白皮书的目标读者包括但不限于工业企业、移动运营商、通信设备提供商、安全产品提供商、安全服务提供商、系统集成商，以及其他关心 5G+ 工业互联网安全相关的机构和个人。

目录

02

5G 与工业互联网融合发展概述

随着 5G 时代的到来，5G 将以其高带宽、低时延、海量连接等特性大幅提升工业互联网的信息化水平，逐步成为支撑工业生产的基础设施。5G 在可靠性和移动性的优势让其有望替代当前工业中广泛使用的有线和 WIFI 网络，5G 的大带宽、低时延，以及边缘计算特性更能推动智能制造中的工业视觉、AR、VR 及工业可穿戴应用快速发展；通过 5G 技术连接、收集并分析海量终端的数据，进而得到设备实时运行信息，最终可达到提质、增效、降成本的效果。

5G 技术应用从移动互联网向工业互联网应用领域扩展，将渗透到工业生产的各个领域，满足前所未有的工业连接和通信需求，主要包括如下三种典型的应用场景：

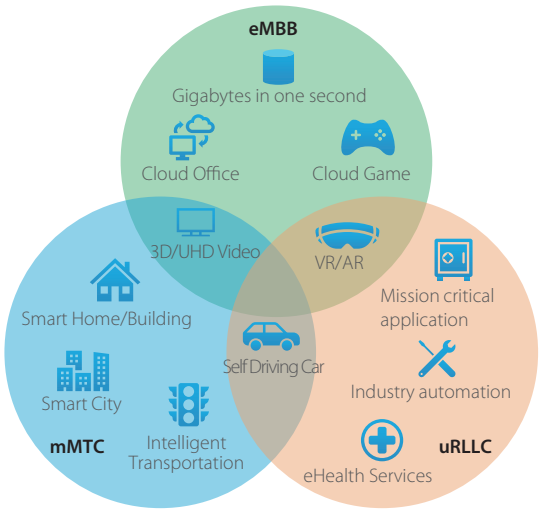


图 2-1 5G 行业应用场景

eMBB（增强型移动宽带）

在 5G 时代，AR/VR、高清视频、3D 等业务的流行将会驱动数据速率大幅提升，峰值速率超过 10Gbps，在工业环境下的具体应用包括 5G+ 机器视觉质检、5G+ 智能制造中的工业巡检无人机、5G+ 智能电网中的高空巡检机器人等。

uRLLC（超可靠低时延通信业务）

5G 网络 E2E 时延 <5ms、安全性和可靠性 >99.999%，能广泛满足工业生产领域的需求。例如 5G+ 港口中的远程操控桥吊作业、精准控制智能装卸，5G+ 矿山中的远程操控挖掘机、无人矿卡等。

mMTC（大规模机器通信业务）

5G 开启了万物互联的时代，其能提供低功耗、大连接（>1M 连接 /km^2）的网络服务，例如 5G+ 工业制造中的工业可穿戴、5G+ 智慧钢厂中的有害气体及温度检测等业务。

5G 网络高速率、超大连接、低时延的特点，将推动工业互联网快速发展和运用。5G 网络提供的灵活定制、弹性部署、多层次隔离等智能网络能力与工业生产中研发设计系统、生产控制系统及服务管理系统等相结合，可以全面推动 5G 工业互联网的研发设计、生产制造、管理服务等生产流程的深刻变革，实现制造业向智能化、服务化、高端化转型。

03

5G 与工业互联网
安全政策与标准

“5G网络的引入，打破了传统工业相对封闭可信的生产环境，病毒、木马、高级持续性攻击等安全风险对工业生产的威胁日益加剧，一旦受到网络攻击，将会造成巨大经济损失，并可能带来环境灾难和人员伤亡，危及公众安全和国家安全。”

2015 年 12 月 23 日乌克兰电力系统遭受攻击，黑客将 BlackEnergy 恶意软件植入乌克兰电力部门，造成电网故障并导致伊万诺 - 弗兰科夫斯克地区大约一半的家庭停电 6 小时。

针对工业互联网安全事故频发的现状，政府和标准组织从多个层面进行支撑保障，共同促进工业互联网安全生态建设。

2018 年 8 月 3 日晚，台积电营运总部和新竹科学园区的 12 英寸晶圆厂的电脑，遭到勒索病毒入侵，生产线全数停摆。几个小时之内，台积电在台湾北、中、南三处重要生产基地均未能幸免。各厂区直到 6 日才陆续全部恢复正常生产。这一事件直接影响台积电三季度 3% 的营业收入，公司的毛利润率下降一个百分点。

2018 年 8 月 4 日，攻击者使用恶意软件 TRITON 攻击中东某关键基础设施内的施耐德 Triconex 安全仪表系统（ SIS ），造成 SIS 系统失效，进而导致工业生产过程自动关闭。

2019 年 3 月 19 日挪威铝业公司 Norsk Hydro 遭到 LockerGoga 勒索软件攻击，致使主机死机，造成多个工厂关闭，部分工厂切换为手动运营模式，生产业务中断。

3.1 安全政策

为加强对工业互联网的安全管理，引导工业互联网安全有序的发展，各国政府相继出台多个法律法规和政府指导。

在国内，2017 年 6 月起正式实施的《中华人民共和国网络安全法》要求对包括工控系统在内的“可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”实行重点保护。2017 年 12 月发布的《关于深化“互联网 + 先进制造业”发展工业互联网的指导意见》以“强化安全保障”为指导思想、“安全可靠”为基本原则，提出“建立工业互联网安全保障体系、提升安全保障能力”的发展目标。2019 年 8 月工信部联合十部委下发《关于加强工业互联网安全工作的指导意见》，体系化推进工业互联网安全工作，全面提升工业互联网创新发展安全保障能力和服务水平。2019 年 12 月 1 日施行网络安全等级保护 2.0 标准，即《信息安全技术网络安全等级保护基本要求》，其中特别增加了对工业控制系统的安全要求。

国际上，2015 年 6 月美国国家标准与技术研究院发布《工业控制系统安全指南》，梳理工业控制系统典型威胁，提出安全防护技术框架。2019 年 5 月 ENISA(欧盟网络信息安全局) 发布《工业 4.0 网络安全：挑战与建议》报告，提供了可实施的安全措施，以加强欧盟工业 4.0 网络安全。2020 年 1 月欧盟出台《5G 网络安全欧盟工具箱》等一系列 5G 安全措施，应对 5G 网络安全问题。

2020 年 1 月美国出台《保障 5G 安全及其他法案》，提出“安全的下一代移动通信战略”。以解决 5G 和未来几代无线通信系统所面临的安全漏洞等问题。

3.2 安全标准

国内外相关标准组织针对 5G、工业互联网及应用等多个层面发布了标准规范。工业互联网产业联盟 2018 年相继发布《工业互联网安全防护总体要求》和《工业互联网平台安全防护要求》，规定了工业互联网应用场景下各组成对象不同安全等级的安全防护要求。针对 5G 网络安全，3GPP 发布了 TS33.501《Security Architecture and Procedures for 5G System》，中国通信标准化协会发布了 YD/T 3628-2019《5G 移动通信网 安全技术要求》。

2018 年 4 月 德国工业界牵头成立了 5G 产业自动化联盟 "(5G ACIA)，推动 5G 在工业生产领域的落地。在同年的德国汉诺威工业博览会上，发布了包含预测性维护网络、运动控制同步场景、绘图运动控制等工业互联六大场景的 TSN+OPCUA (OPC 统一架构) 测试床。

5G 与工业互联网融合发展，相关安全标准也在陆续出台和丰富，比如中国通信标准化协会发布的《工业通信网络 网络和系统安全 系统安全要求和安全等级》，3GPP 发布的 TS 22.104《Service requirements for cyber-physical control applications in vertical domains》。

这些安全标准的制定为 5G 与工业互联网的安全融合奠定了基础，对建立 5G 工业互联网一体化防护体系提供了标准依据。随着我国在新基建相关领域的持续发力，相信会有更多针对 5G 工业互联网场景的安全标准出台，为 5G+ 工业互联网应用的发展保驾护航。

04 5G 与工业互联网带来新的安全挑战

5G与工业系统的深度融合势必将大量的ICT系统威胁和挑战带入工业OT网络，使得5G+工业互联网与传统的工控系统安全和互联网安全相比，其安全挑战更为艰巨。

以下根据防护对象不同，分别从工业网络、工业控制、工业数据、终端接入、工业应用五个层面来分析5G与工业互联网融合面临的安全威胁。

4.1 网络安全

5G 采用网络切片，为不同工业互联网业务提供差异化的服务，网络化协同、个性化的安全定制等不仅要求网络提供安全服务的保障，也对网络的安全隔离能力提出更高的要求。其面对的安全挑战包括非法访问、资源争夺、非法攻击等切片间安全威胁，不同安全域间的非法访问、用户数据被窃听、针对公共 NF 的拒绝服务攻击等切片内安全威胁，外部网络的非法访问、病毒木马攻击等切片与 DN 网络间的安全威胁，非法租户的非法访问、管理员权限滥用、切片敏感信息的篡改等切片管理的安全威胁。

5G 网络由于采用了 SDN、NFV 等大量新 IT 技术，网络传输链路上的软、硬件安全威胁业随之带入工业互联网。工业互联网要求 MEC 尽可能靠近业务场景以满足其对低时延业务的需求，随之而来的 5G 核心网 UPF 下沉造成网络边界模糊，传统物理边界防护难以应用。另外，由于性能、成本、部署灵活性要求等多种因素制约，MEC 节点的安全能力不够完善，可抵御的攻击种类和抵御单个攻击的强度不够，容易被攻击。

4.2 控制安全

工业控制、工业机器人等场景对时延的要求极高，需要控制信令端到端的精确传送。只有保障 5G 网络环境下时延与时延抖动需求，才能实现上述场景中多个控制系统的协作，如机械手臂的联动、工业设备的同步加工等。

工业控制协议、控制平台、控制软件在设计之初可能未考虑完整性、身份校验等安全需求。为此，其授权与访问控制不严格，身份验证不充分，配置维护不足，凭证管理不严。应用软件也持续面临病毒、木马、漏洞等传统安全挑战。5G 网络使得原来不联网或相对封闭的控制专网连接到互联网上，这无形中增大了工控协议与 IT 系统漏洞被利用风险。

4.3 数据安全

5G 网络基于 NFV、云计算、虚拟化技术使得安全边界模糊，流量不可见。MEC 节点位于网络边缘，处于运营商控制较弱的开放网络环境中，数据窃取、泄露的风险相对较高。

工业互联网的多业务场景要求安全与业务需求、接入技术、终端能力等相结合，为此对数据管控有更严格的要求，要求企业数据不出园区。这对 MEC 中数据存储、传输、处理的安全性提出了较高的要求。

MEC 通过 API 接口开放给第三方应用，使得企业内部生产管理数据、生产操作数据以及工厂外部数据的开放、流动和共享带来前所未有的风险，使得行业数据安全传输与存储的风险大大增加。

4.4 接入安全

5G 网络增大了大量工业 IT 软件漏洞被利用风险。5G 开启了万物互联时代，5G 与工业互联网的融合使得海量工业终端接入成为可能，同时也带来攻击风险点的增加，终端设备本身，包括所用芯片、嵌入式操作系统、编码规范、第三方应用软件以及功能等，均存在漏洞、缺陷、后门等安全问题暴露在相对开放的 5G 网络中，存在被利用的风险。

多种类终端接入加剧了恶意应用威胁渗透，巨量化、泛在化的智能终端易被利用成为新攻击源。一方面在 mMTC 场景下，成千上万的终端接入 5G 工业互联网，一旦这些终端被入侵利用，形成规模化的设备僵尸网络，将成为新型高容量分布式拒绝服务（DDoS）攻击源，进而对工业应用、后台系统等发起攻击；另一方面，终端提供的数据信息量巨大，分类众多，应用场景多元化，但缺乏统一的安全标识和认证管理机制，这也增加了网络管理的难度。

4.5 应用安全

5G 网络基于网络能力开放技术，与工业互联网深度融合，使得工业互联网可以充分利用其网络能力灵活开发新业务，但也带来新的风险和挑战，攻击者可以利用 5G 网络能力开放架构提供的应用程序编程接口（API）对网络进行拒绝服务攻击，比如利用部署在 MEC 平台上的第三方 APP 对 MEP 发起攻击。另外，多个 APP 间也存在互相非法访问的安全风险。

随着跨行业应用的开展，需要开放共享相应的用户个人信息、网络数据和业务数据，这些信息和数据从运营商内部的封闭平台开放共享到工业互联网企业的开放平台上，运营商对数据的控制力减弱，数据泄露的风险增大。

5G 网络能力开放架构面临网络能力的非授权访问和使用、数据泄露、用户和网络敏感信息泄露等安全风险。边缘云平台（MEC）及服务也面临着虚拟化中常见的违规接入、内部入侵等内外部安全挑战，特别是 MEC 上应用程序缺陷，增加了非授权访问风险。

05

5G+ 工业互联网
安全参考架构

5.1 设计理念

5G+ 工业互联网安全以 5G 自身安全能力为基础，结合工业互联网实际应用场景安全需求，通过融合创新，将零信任、内生安全等前沿安全理念融入定制化安全方案中，形成整体的 5G+ 工业互联网一体化安全架构。

为应对 5G 引入后工业互联网所面临的各种安全威胁，主要从事前防范、事中监测和事后应急三大环节构筑防护措施视角。事前部署相应的防护监测设备及措施，实时感知内部、外部的安全风险，针对网络不同域不同逻辑层部署采集功能，完成全网信息采集。事中通过大数据智能分析等手段，进行海量信息的综合处理，并利用安全威胁特征库来分析识别安全威胁。根据智能决策的理论、模型、方法，针对发生的安全威胁做出全面综合科学的响应决策。事后根据响应决策，研究实施响应处置的方法，包括大容量威胁流量清洗追踪溯源等，能够实时完成威胁处置等。

此外，5G 技术发展以及应用场景具有广泛性、开放性、挑战性和多元性，既需要明确网络运营商、设备供应商、行业应用服务提供商等产业链各环节不同主体的责任和义务，不过分关注或放大单一环节责任，又需要加强各主体之间的协同合作，充分发挥政府部门、标准化组织、企业、研究机构和用户等各方的能动性，明晰各方安全责任，打造多方参与的 5G 安全治理体系。

以系统理念看待 5G 工业互联网安全。构建5G工业互联网威胁监测、全局感知、预警防护、联动处置一体化网络安全防御体系，形成覆盖全生命周期的网络安全防护能力。

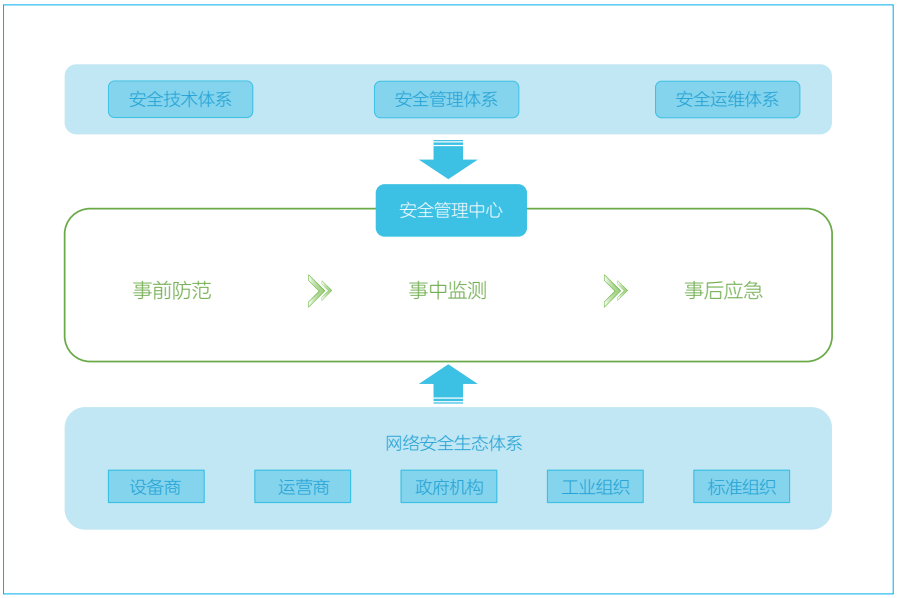


图 5-1 5G+ 工业互联网安全协同联动机制

5.2 一体化的 5G+ 工业互联网安全参考架构

5G 与工业互联网的融合，信息安全涉及到工业互联网的各个层面，单一的安全解决方案不能满足工业互联网信息安全的需要，需要统筹考虑，建立统一的安全防御体系。另外，5G+ 工业互联网安全工作需要从制度建设、产业支持等更全局的视野来统筹安排，让更多企业意识到信息安全的必要性与紧迫性，加强安全管理与风险防范控制。为此，需要通过构建统一的工业互联网信息安全保障体系，较为全面覆盖接入、网络、控制、数据、等安全风险，才能够有效的保障 5G 引入后的工业互联网安全。

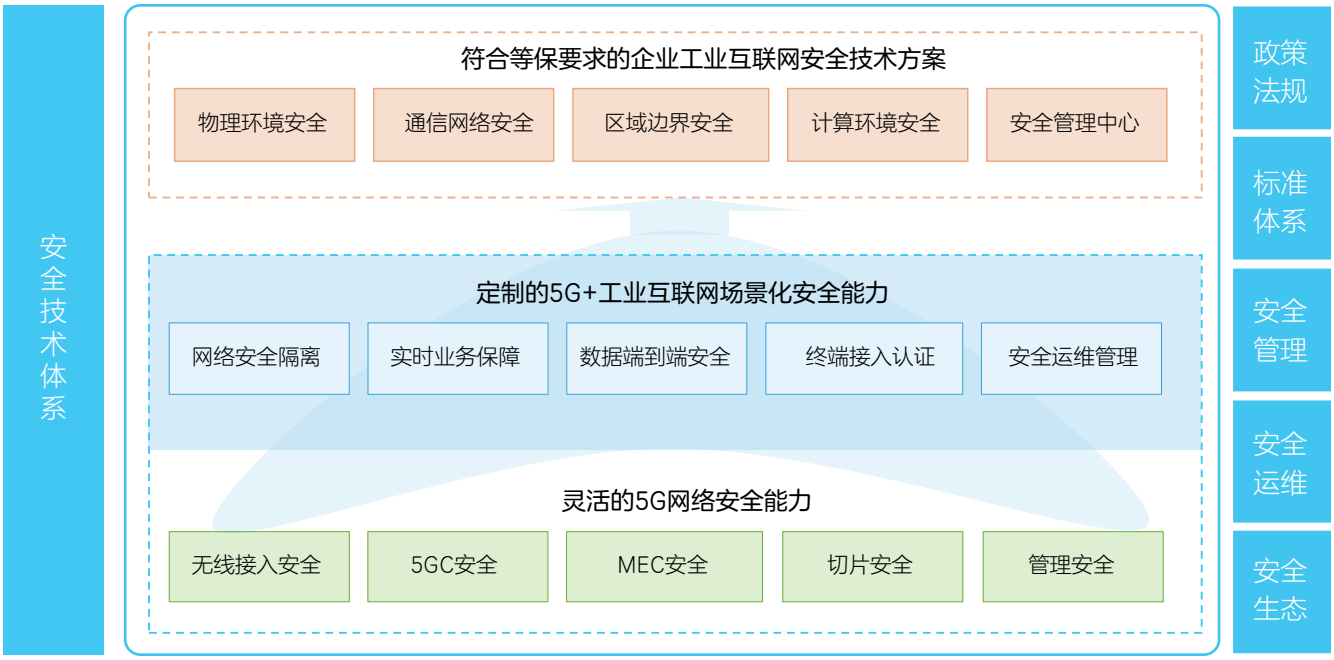


图 5-2 5G+ 工业互联网安全参考架构

5G 工业互联网信息安全保障体系以我国的安全政策、相关法律和行业安全规划为主要指导原则，其包括安全技术体系、安全管理体系、安全运维体系及安全生态体系。安全技术体系以信息安全等级保护等安全要求为依据，包含对工业控制的安全防护、感知终端的安全防护、网络通信的安全防护、系统及应用的安全防护以及数据安全保障，构建一个全面的、端到端的技术防护体系。管理安全体系主要以等级保护、ISO27001 标准为主要依据，在安全机构、安全制度、安全人员及安全建设方面予以管理和规范。而针对工业互联网的安全运维，则是以工业互联网产业联盟（AII）等组织标准为参考，结合工业安全管理中心，将技术和管理及运维流程有效结合，保障工业互联网的运行安全。

本白皮书重点阐述 5G+ 工业互联网安全技术体系建设，下面将分层介绍 5G+ 工业互联网安全技术体系架构。

5.3 符合等保要求的企业工业互联网安全技术方案

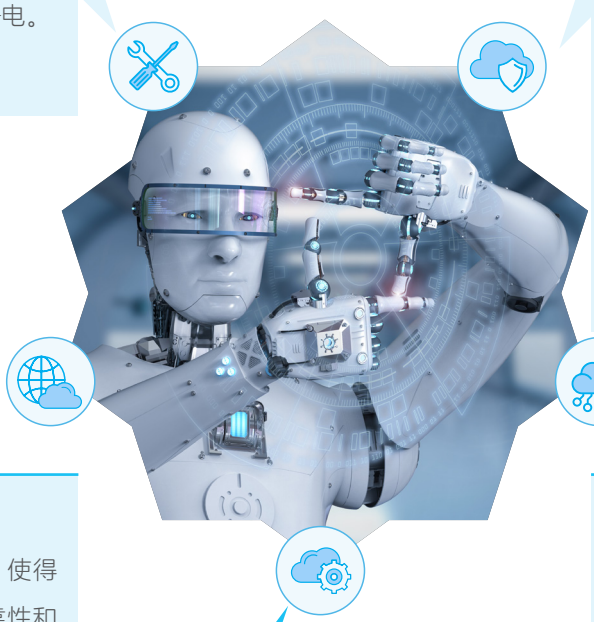
为构建工业智能化发展的安全可信环境，目前大部分企业工业互联网安全方案以《网络安全等级保护基本要求》、《网络安全等级保护安全设计技术要求》等国家标准文件为依据进行系统性设计。在满足相应级别安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心及管理部分要求基础上，最大程度发挥安全措施的保护能力。

物理安全

机房场地物理位置选择、物理访问控制、防火、防水和防潮、温度控制、电力供应、电磁辐射，以及工业设备防盗和防破坏、防雷击、防静电。

安全管理中心

划分独立的安全运维区域，建立安全的信息传输路径，对网络中的安全设备进行集中管控。在设备上采取审计措施，对链路、设备和服务器运行状况进行监控并能够告警。对安全策略、恶意代码、补丁升级进行集中管理，对安全事件能够有效识别、及时预警和动态分析，展现全网安全态势。



安全通信网络

设计合理的工业互联网架构，使得网络的数据传输效率以及可靠性和安全性得以保证，数据加密后传输，保证数据的完整性和保密性，防止他人破坏，创建安全的通信传输通道。划分安全域，保证工厂内有线与无线网络的安全，工厂外与用户、协作企业等实现互联的公共网络（包括标识解析系统）安全。

区域边界安全

根据访问控制策略在网络边界及区域间设置访问控制规则，建立基于身份鉴别要求的边界防护。在网络边界、重要网络节点进行安全审计，对重要的用户行为和重要安全事件进行审计。对突发安全事件具备检测的能力、响应处置能力、溯源分析能力。

计算环境安全

采用访问控制技术对登录工业互联网平台及各类型智能设备的主体进行身份确认，分配适当的访问和使用权限，保证工业系统资源受控合法地使用。使用安全审计技术对重要的用户行为和重要安全事件进行审计。智能装备系统采用最小安装、限制终端接入、入侵检测及报警、数据有效性检验以及系统漏洞的发现与修补等策略，减少主机对外暴露的漏洞。采用校验技术或密码技术保证重要数据在传输过程中的完整性、保密性。

06 定制的 5G+ 工业互联网场景化安全能力

作为工业互联网的重要基础设施，5G在使能工业互联网的过程中，要结合具体的业务场景，基于5G网络自身的安全能力提供定制化的安全方案，来满足工业互联网自身的等级保护需求。

灵活的 5G 网络安全能力

5G 网络为应对新技术新架构带来的安全挑战，参照 ITU X.805 定义的安全体系架构和 3GPP TS 33.501 等 5G 安全规范，同时遵循《电信网和互联网管理安全等级保护要求》，提供了无线接入安全、5GC 安全、MEC 安全、切片安全及管理安全端到端的安全通信能力。

- 接入安全：包含终端的接入认证、终端的访问控制以及数据传输的安全设计。定义多重接入认证和信息加密方式，从较粗粒度的网络级认证到细化的切片认证，以及进一步的数据网络认证，不同的业务可以灵活配置不同级别的认证策略或者策略组合，以满足不同行业的接入安全需求。

- 5GC 安全：5G 核心网络功能虚拟化的特点，使得虚拟化平台的可管可控的安全性要求成为 5G 安全的一个重要部分。虚拟网络安全防护的基本手段是对网络中的各个功能网元，以及管理网元，按照其重要性程度，划分不同的安全等级，并根据各个安全等级设置不同的安全域。每个 NF 网元只能属于一个安全域，每个安全域建议分配专用的硬件资源池；域间访问要通过虚拟安全设备做防护；域内可根据网元种类、归属地区等划分子域；安全资源池提供 FW/VPN/WAF/IPS 等安全服务，通过 MANO 统一编排。

- MEC 安全：5G 网络中引入了边缘计算（MEC），满足 5G 业务本地化、差异化、低时延的诉求。MEC 本质上也是一个小型的云数据中心，这部分的安全设计主要参考等保等相关的技术要求，结合 MEC 本身的业务特点，构建从物理安全、基础设施安全、系统及平台安全、业务及数据安全、管理与运维安全等端到端的安全解决方案，打造“放心”的边缘计算平台。

  在安全解决方案中，需要重点关注对第三方 APP 的安全防护。首先，采用安全隔离手段实现 MEP 与 APP、APP 与 APP 的安全隔离（比如部署 FW、划分 VLAN 等）。另外，由于 APP 以虚拟化网络功能 VNF 的方式运行在 NFV 基础设施上，当 APP 以虚拟机或容器部署时，可参考虚拟层安全要求和容器安全要求，采用安全措施实现 APP 使用的虚拟 CPU、虚拟内存以及 I/O 等资源与其它虚拟机或容器使用的资源间的隔离，同时也要保证 APP 镜像和镜像仓库具有完整性和机密性、访问控制的安全保护。

- 切片安全：区别于传统物理专网的私有性与封闭性，5G 网络切片是建立在共享资源之上的虚拟化专用网络，切片安全除了提供传统移动网络安全机制之外（例如接入认证、接入层和非接入层信令和数据的加密与完整性保护等），还需要提供网络切片之间端到端安全隔离机制，包括端到端切片隔离、切片与用户间安全隔离、切片与 DN 间安全隔离。

- 管理安全：首先对网络运维和管理人员，提供统一的安全接入门户，实现用户的集中管理、接入认证、访问日志审计等功能。然后是安全按需编排，提供差异化安全服务，即通过为每种业务提供单独的网络切片，以及结合业务安全需求，为切片按需编排对应的安全能力，并且能弹性伸缩，以达到为各种应用提供差异化的安全服务。最后是网络能力开放安全管理，在运营商将网络能力开放之前，需要对能力开放给租户进行授权，租户需要在认证和授权通过之后，才能访问网络能力，不同的角色将获取不同的网络接入权限，租户和网络之间通过建立安全隧道，保证操作和运营数据的安全传输。

5G+ 工业互联网场景定制化安全能力

5G 继承了传统的通信网络安全体系，能够保障人和人之间的安全通信，但对于垂直行业，特别是对安全要求严苛的工业系统，5G 提供的基础安全能力无法满足不同业务场景下的安全需求。为此，需要以 5G 自身安全能力为基础，结合工业互联网特征与运营模式，融合零信任、内生安全等前沿安全技术，构建定制化的 5G+ 工业互联网安全能力。

以下章节将从 5 个方面详细阐述定制化的 5G+ 工业互联网安全能力。

6.1 差异化切片满足企业网络安全隔离需求

5G 网络切片是基于无线接入网、承载网与核心网基础设施，以及网络虚拟化技术构建的一个面向不同业务特征的逻辑网络。运营商可以为不同行业应用在共享的网络基础设施上通过能力开放、智能调度等技术构建网络切片，提供差异化的网络服务。这也对安全提出了新的挑战，包括切片间非法访问、切片内不同安全域间的非法访问等多种安全威胁。

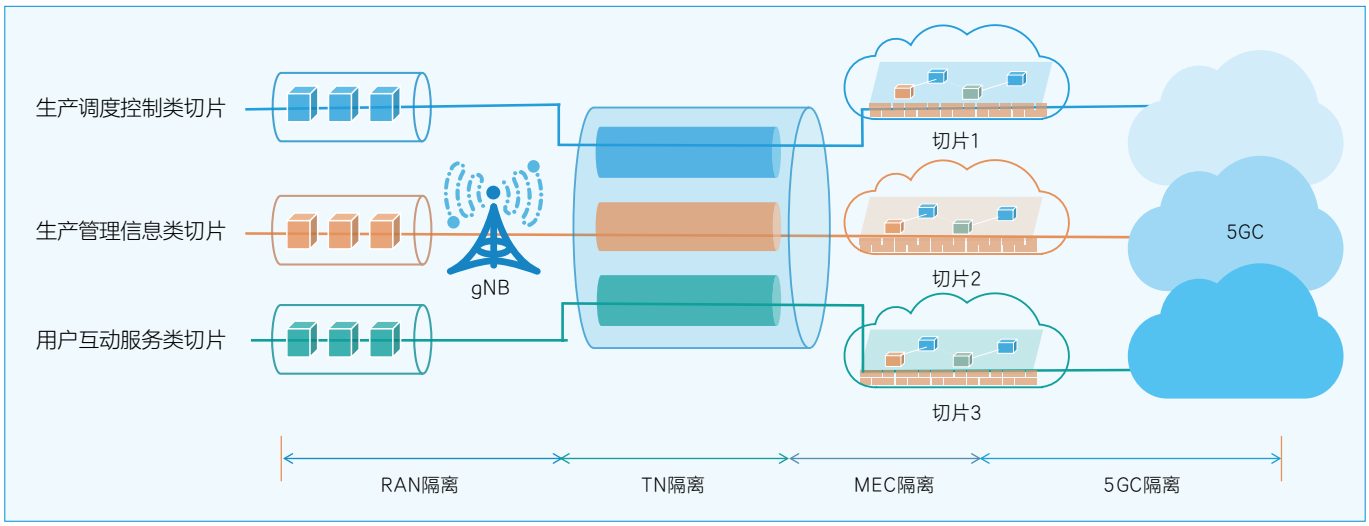


图 6-1 端到端网络切片隔离

为了安全地支持各种差异化的业务场景，需要提供网络切片隔离，为不同业务提供差异化的安全服务。通过一套参数配置，实现切片的资源隔离和业务质量保障，可以根据行业的安全隔离要求和需要保障的关键 SLA 选择不同类型的切片，并进行参数配置，从资源隔离和业务保障的角度，无线网络可以提供多种切片隔离技术。如下图所示，工业互联网切片隔离方案分为四类，分别对应等保 1-4 级，不同业务系统可以根据自身需求选择不同的网络隔离方案。

切片类别	隔离类别	RAN	TN	MEC	5GC
专用切片	完全独占	基站 / 频谱独享	FlexE 隔离	MEC/UPF 业务独享	CPF 全部独享
定制切片 1	部分共享	PRB 独享	VPN/VLAN 隔离	MEC/UPF 企业独享	CPF 全部独享
定制切片 2	部分共享	DRB 共享 5QI 优先级调度	VPN/VLAN 隔离 QoS 资源保障	MEC/UPF 企业独享	CPF 全部独享
普通切片	完全共享	DRB 共享	VPN/VLAN 隔离	VLAN/VxLAN 隔离	CPF 全部共享 UPF 共享

图 6-2 差异化切片隔离方案

6.1.1 RAN 隔离

网络切片在 RAN 侧的隔离主要面向无线频谱资源以及基站处理资源。最高安全等级的工业控制类切片采用独立的基站或者频谱独享。其他类型切片则根据安全需求通过 PRB 独享、DRB 共享、以及 5QI 优先级调度等多种方式组合来实现。

独立基站 / 频谱独享

对于一些强专网的应用（比如工业控制类），或者仅仅只有行业应用需求的局部区域，如无人工厂、无人发电站、矿山等，对通信独立性和可控性要求很高，或者其业务性能要求在共享基站中无法实现，则可以考虑采用独立基站的形式提供无线切片。

另外，对于资源隔离和业务质量保障更高的应用，可以在运营商频谱资源中划分出一部分，比如 5MHz，单独给该切片使用。

PRB 独享

5G OFDMA 系统中，无线频谱从时域、频域、空域维度被划分为不同的资源块（PRB），用于承载终端和基站之间数据传输。对于一些要求资源隔离，且对业务质量保障要求高的切片用户，可以采用配置一定比例的 PRB 给该切片（比如 5%），此时该小区 5% 的空口资源和带宽为该切片专用，不受其它用户影响，PRB 的正交性保证了切片的隔离性，PRB 专用也保证了业务质量的稳定性。

DRB 共享

可以配置 DRB 接纳控制参数，确保切片在特定小区下能够接入的用户数不被其它业务抢占 DRB 接纳控制可以采用灵活的配置策略，既可以固定配置，也可以配置一个较小的比例，超过后还可以在资源池中抢占。

5QI 优先级调度

对于不需要严格确保资源隔离和业务质量的切片，如视频监控类 eMBB 切片，可采用 5QI 优先级调度方式，可以在兼顾业务质量的情况下节省成本。5QI 优先级调度方式是基于 S-NSSAI 的不同优先级（可以依据切片业务需保障的程度进行配置）和业务的 5QI，在一个调度周期内计算出不同业务流的调度优先级。5QI 软切片的本质是基于调度的，以调度策略来实现业务质量，如带宽、误码率等指标的目标，当基站业务繁忙的时候并不能确保达到该目标。

6.1.2 承载隔离

5G 网络依托数据中心部署，跨越数据中心的物理通信链路需要承载多个切片的业务数据。网络切片在承载侧的隔离可通过软隔离、硬隔离和 QoS 资源保障等多种方案实现。

VPN\VLAN 隔离

软隔离方案基于现有网络机制，通过 VLAN 标签与网络切片标识的映射实现。网络切片具备唯一的切片标识，根据切片标识为不同的切片数据映射封装不同的 VLAN 标签，通过 VLAN 隔离实现切片的承载隔离，实现 QoS 保障，用于办公网及监控网络。

FlexE 隔离

硬隔离方案引入 FlexE 技术，基于以太网协议， 在 L1(PHY) 和 L2(MAC) 层之间创造另一“垫层”，实现 FlexE 分片。FlexE 分片是基于时隙调度将一个物理以太网端口划分为多个以太网弹性管道（逻辑端口），使得承载网络既具备类似于 TDM(时分复用) 独占时隙、隔离性好的特性，从而实现承载侧支持任意子速率分片和隔离，同时又具备以太网统计复用、网络效率高的特点。对于工业控制应用等对时延和安全保障较高的业务可以在承载侧独占时隙从而实现切片硬隔离。

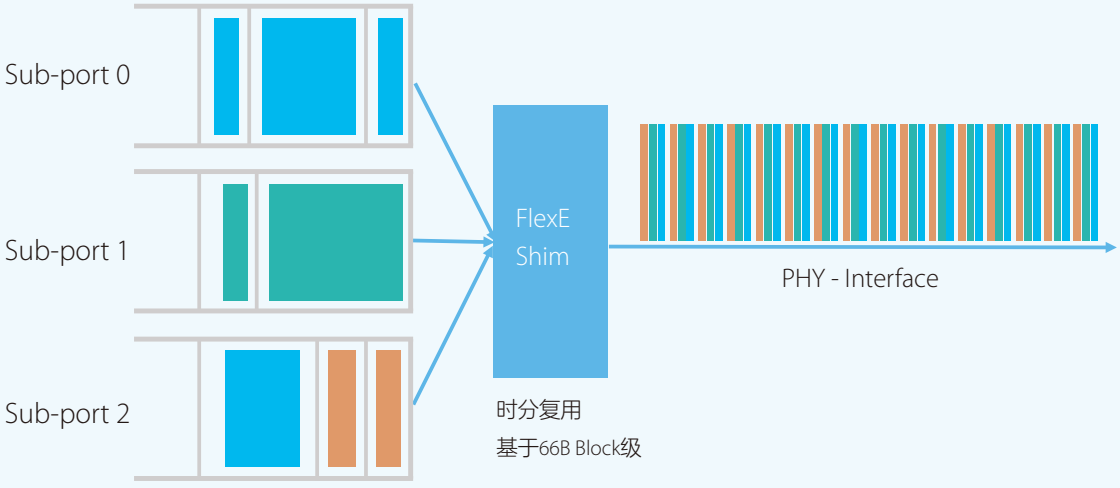


图 6-3 FlexE 时隙交叉交换机制

6.1.3 核心网隔离

5G 核心网基于虚拟化基础设施构建，由很多种不同的网络功能构成，有些网络功能为切片专用（工业控制），有些则在多个切片之间共享，因此在核心网侧的隔离需要采用多重隔离机制。

CPF 独占共享，UPF 独占共享

核心网的所有控制面网元（包括 AMF、AUSF, UDM、UDR、PCF、SMF）、用户面网元 UPF 均新建。适用于如工业控制、典型专网等对安全需求最高的应用场景。

CPF 部分共享，UPF 独占共享

核心网的部分控制面网元（包括 AUSF、UDR、PCF、SMF）独享，AMF 和 UDM 共享，用户面网元 UPF 新建，可根据容量、时延等要求，选择在核心机房或者边缘机房建设 UPF。对于希望数据隔离的大部分切片，或者对部署位置有严格要求（比如工厂、园区）且有本地应用部署需求（MEC）的切片用户，采用这种类型的切片。

CPF 全部共享，UPF 独享

核心网的控制面网元（包括 AMF、AUSF, UDM、UDR、PCF、SMF）共享、NFV 和切片选择相关的控制面网元 NRF、NSSF 共享，用户面网元 UPF 新建，切片通过 S-NSSAI 区分，新建 DNN。应用到如管理信息网等对于安全隔离有一定要求的业务场景。

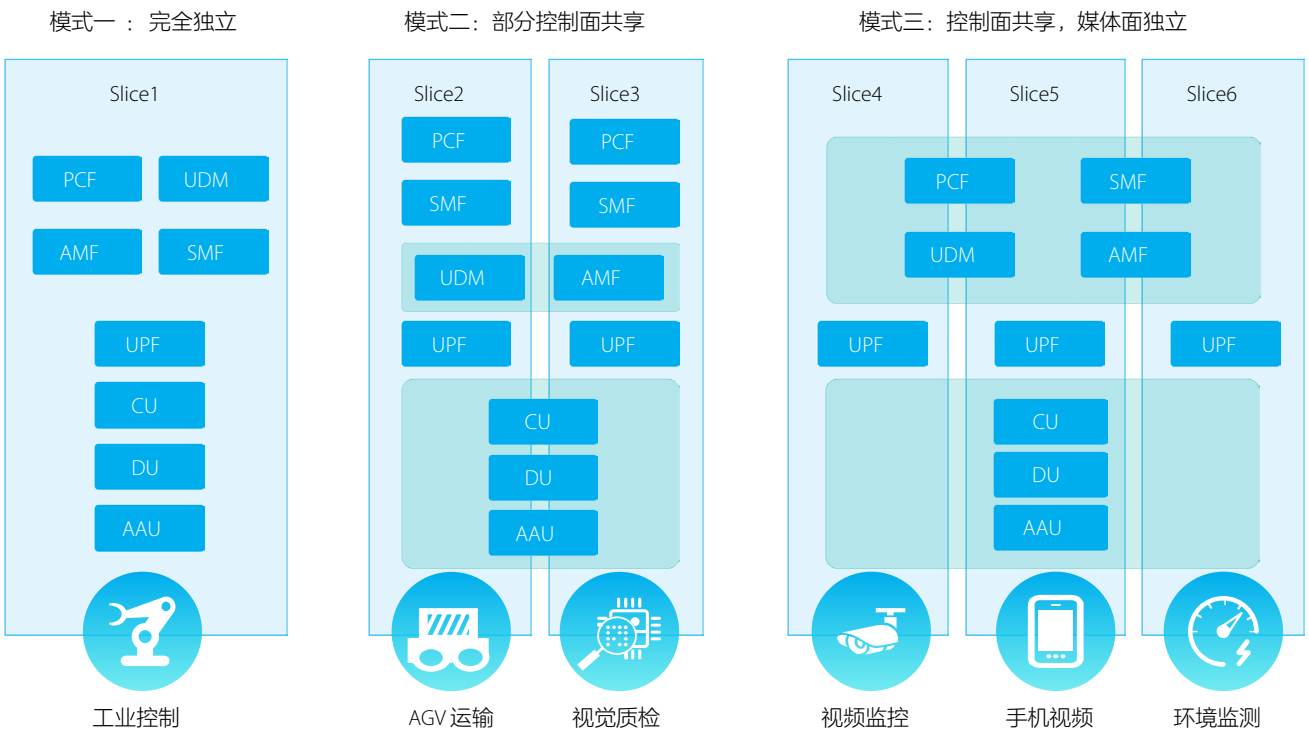


图 6-4 核心网元隔离

6.2 UPF 下沉 +FlexE 支持企业低时延业务需求

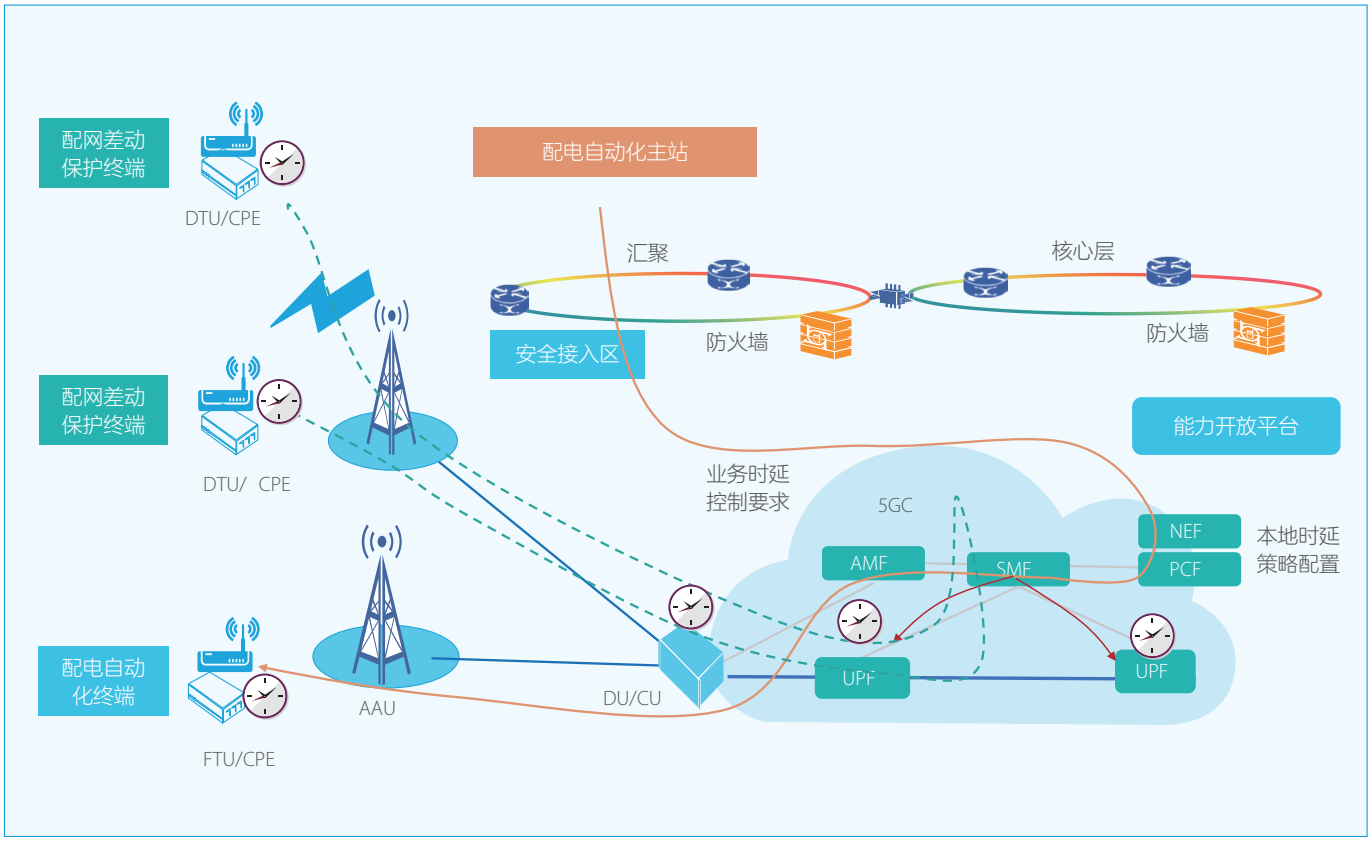


图 6-5 5G 工业应用时延保证

智能车间内设备的互联，以及生产运营的数字化转型，使得工业系统对实时性、抗抖动性的无线网络需求变得迫切，传统无线网络无法满足要求，而 5G 以其高带宽、低时延、大连接的网络特性获得工业生产系统的青睐。

传统端到端移动通信，数据必须流经无线接入、核心网、平台等各个环节，最终导致端到端时延较长，性能上无法满足对时延要求比较高的工业控制应用的要求。为了进一步降低端到端通信时延，可以将 5G 网络中 UPF 下沉到 MEC，通过将数据、应用、智能引入基站边缘侧，通过减少数据传输路由节点，将业务部署在边缘节点以降低端到端通信时延。

另外在网络传输方面，服务于工控的网络切片，对时延要求更高，传统分组设备对于客户业务报文采用逐跳转发策略，网络中每个节点设备都需要对数据包进行 MAC 层和 MPLS 层解析，这种解析耗费大量时间，单设备转发时延高达数十 us。为此，可以在 5G 网络中采用 FlexE 交叉技术来实现网络设备之间的信息传递，它实现基于物理层的用户业务流转发，用户报文在网络中间节点无须解析，业务流交叉过程近乎瞬间完成，实现单跳设备转发时延 1~10us。可有效解决时间报文的模拟、欺骗。

6.3 多重机制提供企业端到端数据安全保障

用户数据在传输过程中存在被窃听、篡改、泄露等安全威胁。为降低 5G 行业应用中数据安全风险，5G 提供了更强壮的数据安全保护方法。

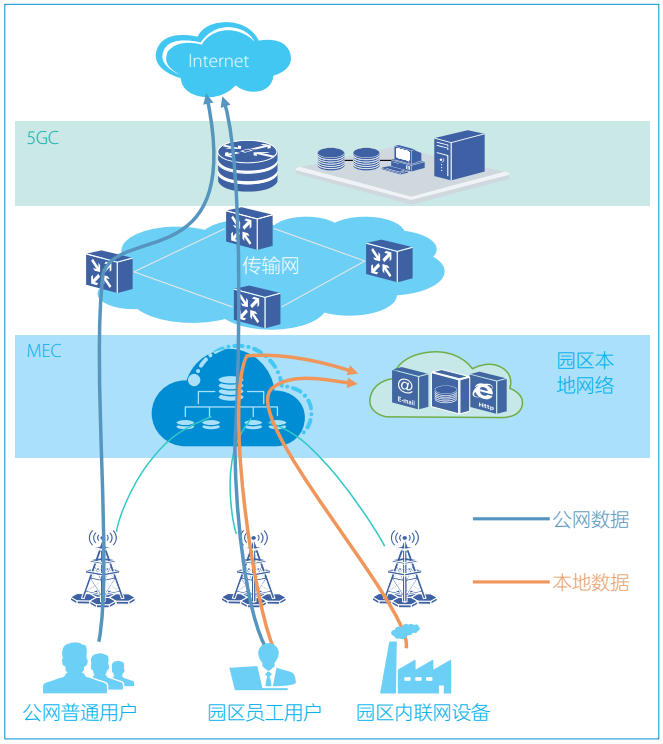


图 6-6 5G+ 工业园区数据安全

6.3.1 接入认证

在为安全等级高的工业系统提供定制化的服务过程中，采用切片二次认证机制，即在用户接入网络时所做认证之后为接入特定业务建立数据通道而进行的认证。在该认证过程中，使用了非运营商控制的信任状要求，即用户通过接入认证后并不能直接与业务系统建立连接，而是利用业务相关的信任状与用户终端进行认证，并在认证通过的情况下才允许 5G 网络为用户建立与业务系统间的通信链路，从而保证企业对安全策略自主可控。

6.3.2 访问控制

遵循最小权限授权原则，为不同用户分配不同的数据操作权限，未经授权不能访问用户信息，防止非法访问、越权访问等手段获取用户的数据。

为避免不可靠来源用户的接入，提供选择多种访问控制方式，系统不允许时间，来源，登录方式等各种访问控制条件不满足的用户登录系统建立会话。另外，对关键敏感数据采用 SHA256、AES256 等加密算法进行加密存储。

6.3.3 数据传输安全

在机密性保护的密码算法方面，采用 5G 网络的 AES（高级加密标准 Advanced Encryption Standard）、SNOW 3G（3GPP 流密码算法）、ZUC（祖冲之密码算法）等算法（这些算法采用 128 位密钥长度，被业界证明是安全的）

为保护数据在网络间传输，可采用 5G 新增的安全边缘保护代理功能。SEPP 在运营商之间建立 TLS 安全传输通道，对需要保护的信息进行机密性和完整性保护，有效防止数据在网间传输时被篡改或窃听。

提供工业互联网中的数据产生、处理、使用等环节的安全保护。首先，在数据产生和处理过程中，根据数据的敏感度进行分类，建立不同安全域间的加密传输链路，根据不同的安全级别采用差异化的数据安全技术。在数据使用过程中，对数据使用方进行授权和验证，保证数据使用的目的和范围符合安全策略，对重要业务数据的使用进行审计，最终为行业用户提供数据的机密性和完整性保护。

另外采用基于会话的加密机制，按需配置加密算法与密钥强度。采用数据加密、完整性校验保证数据在空口、UE 和 MEC 之间的安全传输，比如建立 IPSec/SSL VPN 隧道，预防数据被嗅探窃取、篡改等威胁，同时结合 UPF 分流技术及内部边界安全隔离，实现数据不出园区。

6.4 零信任架构增强海量终端的接入安全

随着 5G 网络的引入，UPF 下沉到工业园区，海量行业终端将接入工业互联网，相应的安全风险也在增加，一旦这些工业生产终端被入侵利用，将会产生非常严重的后果。

传统安全采用边界防护方式，即在网络边界验证终端身份，确定用户是否被信任。随着攻击方式和威胁多样化，传统网络接入安全架构凸显出很大的局限性，为此，5G+ 工业互联网安全架构引入基于零信任安全理念，启用新型身份验证管理模式，充分利用身份验证凭据、设备、网络、应用等多种资源的组合安全边界。

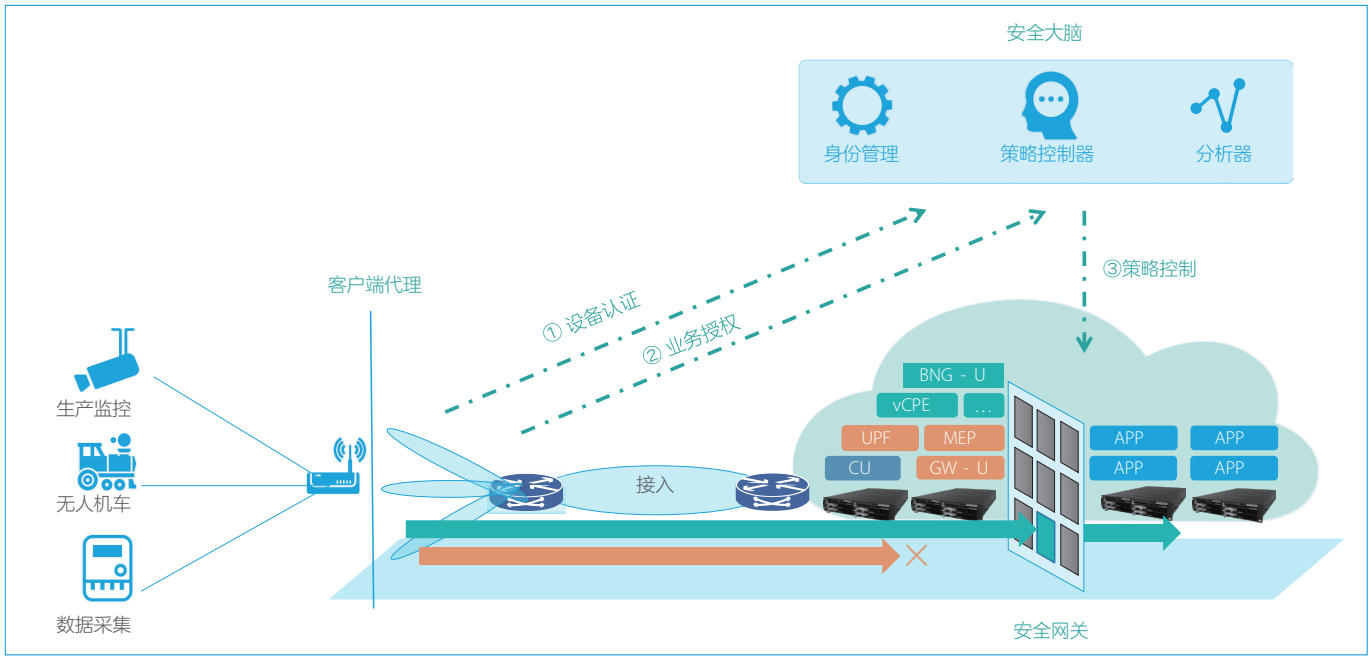


图 6-7 基于 5G 的工业零信任安全系统

零信任安全系统包括控制器、可信网关、分析器三大组件。控制器作为安全控制面的核心组件，为可信网关提供认证服务、动态业务授权和集中的策略管理能力。控制器对所有的访问请求进行权限判定，权限判定不再基于简单的静态规则，而是基于身份、权限、信任等级和安全策略等进行动态判定。

分析器为控制器提供信任等级评估，作为授权判定依据。分析器持续收集终端、可信网关、控制器的日志信息，结合身份库、权限库数据，基于大数据和人工智能技术，对身份进行持续画像，对访问行为进行持续分析，对信任进行持续评估，最终生成和维护信任库，为动态访问控制引擎提供决策依据。

可信网关作为用户面的网络准入节点，是确保业务安全访问的第一道关口，是动态访问控制能力的策略执行点。针对 5G 行业终端访问控制需求，通过控制器对访问主体进行认证，对访问主体的权限进行动态判定。只有认证通过、并且具有访问权限的访问请求才予以放行。

5G 工业互联网零信任安全架构下的终端安全接入不再以网络边界为限，无论是来自于企业网络之外的用户，还是来自于企业网络内部的用户，在建立连接前均需进行认证授权。5G 工业互联网零信任安全架构，使得原来的被动防御向主动防御的转变，从边界防御方式向内生安全转变，有力保障 5G 网络环境下海量行业终端的接入安全。

6.5 态势感知保障网络整体安全能力

5G 网络的应用，有力推动了有线工业控制向无线接入工控自动化的转型 ，云 VR/AR 技术的大量应用，工业可穿戴，远程操控的普及，在此过程中，传统工业系统势必与 5G 移动互联网产生大量信息和数据交互。这也给工业互联网行业安全防护提出了更高的挑战，原有的被动式防御已不可靠，无法有效防止有组织的规模性攻击，迫切需要新的安全技术。

5G 工业互联网态势感知技术，可以覆盖 5G 资产，包括 5GC 网元、切片、虚机、物理机、中间件等，并能将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，在大量的安全事件中寻找事件之间的因果关系，能够追踪攻击链定位威胁发生的源头，并分析可能的波及范围，能够根据资产价值及业务影响来确定处置方式与手段。另外，态势感知可以基于对网络攻击事件的深度挖掘，结合网络的基础设施情况和运行状态，就能够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和措施。其次，在工业互联网业务与 5G 移动互联网交互的关键路径上，对网络中的流量和各种日志信息进行持续地收集分析，对网络异常流量进行解析，包括攻击流量特征、威胁文件传输等。从而发现网络流量异常行为或者用户异常行为，主动对未知威胁提前干预。

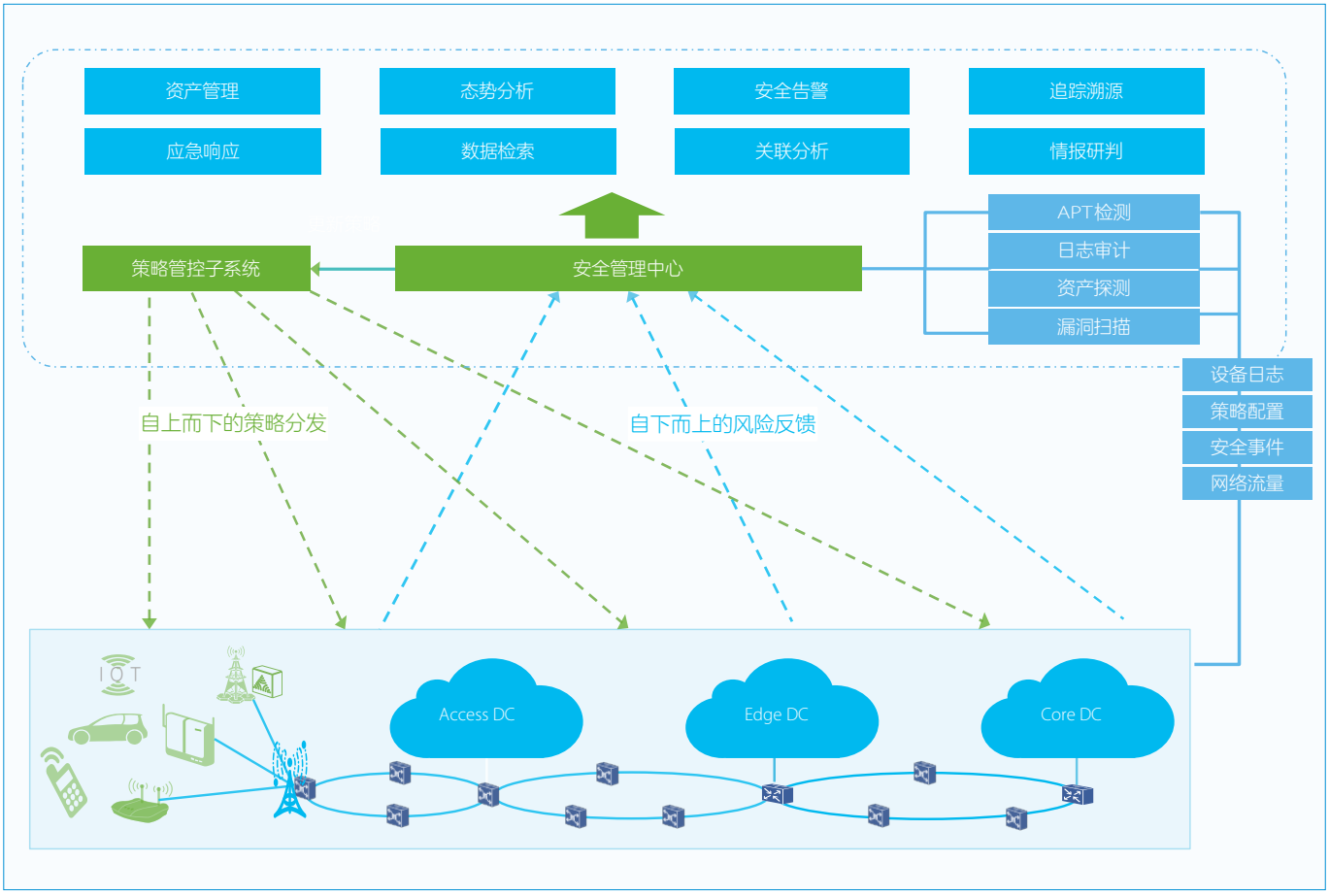


图 6-8 5G+ 工业安全态势感知系统

07

5G+ 工业互联网
安全应用案例

7.1 5G+ 智能电网网络安全解决方案

• 应用简介

2019 年，福建国网电力联合福建移动、中兴开展合作，整合三方基础资源及技术能力，探索电力行业内 5G 网络新型组网模式、边缘计算深化应用，同时验证 5G 网络在各类环境下对电力控制类业务端到端的时延、速率等性能指标及业务功能性指标，探索针对电力业务的 5G 网络专网部署最优方案。

项目搭建了国网电力全国首个 5G 电力生产网，完成配网自动化终端、营销用电信息采集以及机器人巡检三项业务的网络调测，实测 5G 网络环境下，平均时延为 8ms。测试成效得到了国网总部的高度认可，并最终入选国网总部 5G 最佳实践案例，并在电力总部两会期间向全国宣传展示。

• 安全需求

5G 智能电网主要面临的主要网络安全风险可分为外部威胁和内部威胁，外部威胁主要包括 MEC 节点靠近网络的边缘，外部环境可信度降低，管理控制能力减弱，使得 MEC 平台和 MEC 应用处于相对不安全的物理环境，更容易遭受非授权访问、敏感数据泄露、DDoS 攻击、设备物理攻击等威胁；内部威胁包括营商网络功能与不可信任的第三方应用共平台部署，进一步导致网络边界模糊、虚拟机逃逸、镜像篡改、数据窃取与篡改等诸多安全问题。

• 安全方案

为应对 5G 引入后带来的安全威胁，智能电网 5G 网络安全建设以我国相关安全政策、标准、规范为指导原则，以纵深防御思想为核心，使用先进设计理念，采取专业安全设备，形成完善的综合网络安全防护体系。

从逻辑结构上将 5G 智能电网进行安全区划分，同时考虑到边缘数据中心内部有不同的应用区，依照功能属性对其进行安全域划分。

5G+ 智能电网的安全域主要分为：5G 接入区、5G 边缘计算区 、5G 核心网区 、电网业务区、安全运维区。

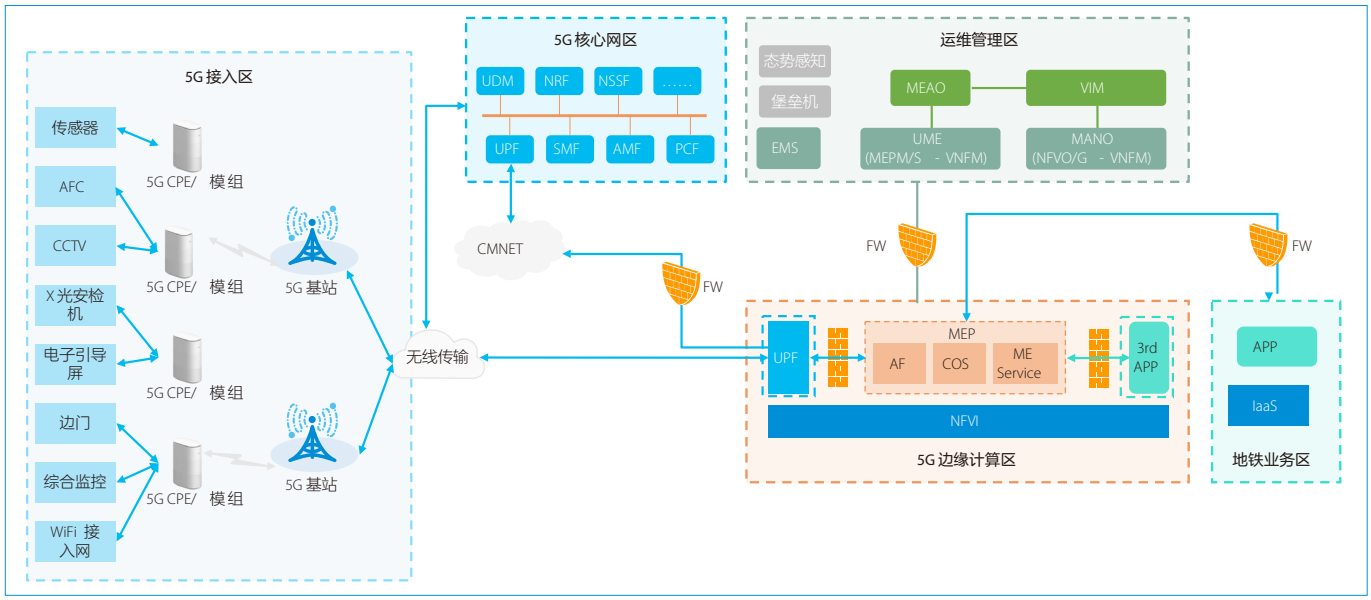


图 7-1 5G+ 智能电网安全拓扑图

❶终端（CPE/ 模组）安全防护

电力终端主要有配电自动化终端、智能电表、无人机、巡检机器人、高清摄像头等品类，从形态上则分为 CPE 和嵌入式通信模块。无论基于哪种品类、哪种形态，5G 模组作为提供通信连接的核心产品，都是非常重要的组成部分，也是电力 5G 专网得以运营的关键。

为了做好终端安全防护，首先引入 eSIM 技术并配合 5G 模组，固定嵌入到终端设备上，提供移动网络接入鉴权和用户身份认证的安全服务，然后再给终端配置 EDR，保证终端的安全性。

通过上述措施可以有力保证 CPE 与 RAN 在接入层（AS）和非接入层（NAS）两层安全体系保障传输安全，从而有效抵抗假冒终端、伪基站、信令/数据窃听、信令/数据篡改/重放等攻击。

❷电力切片安全隔离

区别于传统物理专网的私有性与封闭性，电力 5G 网络切片是建立在共享资源之上的虚拟化专用网络，需要根据具体的业务场景提供网络切片之间端到端安全隔离机制。根据电力不同 5G+ 业务的网络性能需求，可分为如下四种切片类别：

切片名称	切片类别	承载电力业务类别	带宽需求	时延	可用性	隔离要求
生产控制切片	广域专网	生产控制类业务： 如 PML、差动保护等	2Mbps	15ms	99.99%	生产区
生产非控制切片	广域专网	生产非控制类业务： 如变电设备监测、港口岸电监测等	2Mbps	100ms	99.90%	生产区
管理切片	广域专网	智输电线路无人机巡检、 隧道巡检和消防机器人等	100Mbps	100ms	99.90%	管理区
局域专网切片	局域专网	电网需本地闭环业务： 如变电站、电厂、园区等	8M~100Mbps	200ms	99.90%	管理区 +MEC 实现业务本地闭环

图 7-2 5G+ 智能电网切片分类

为保障这些网络切片的，采用四种不同的切片安全隔离机制，实现空口、终端和 MEC 之间加密传输，提供数据源认证、数据完整性和数据机密性等保护措施，防止数据在传输过程中被篡改、拦截或窃听。

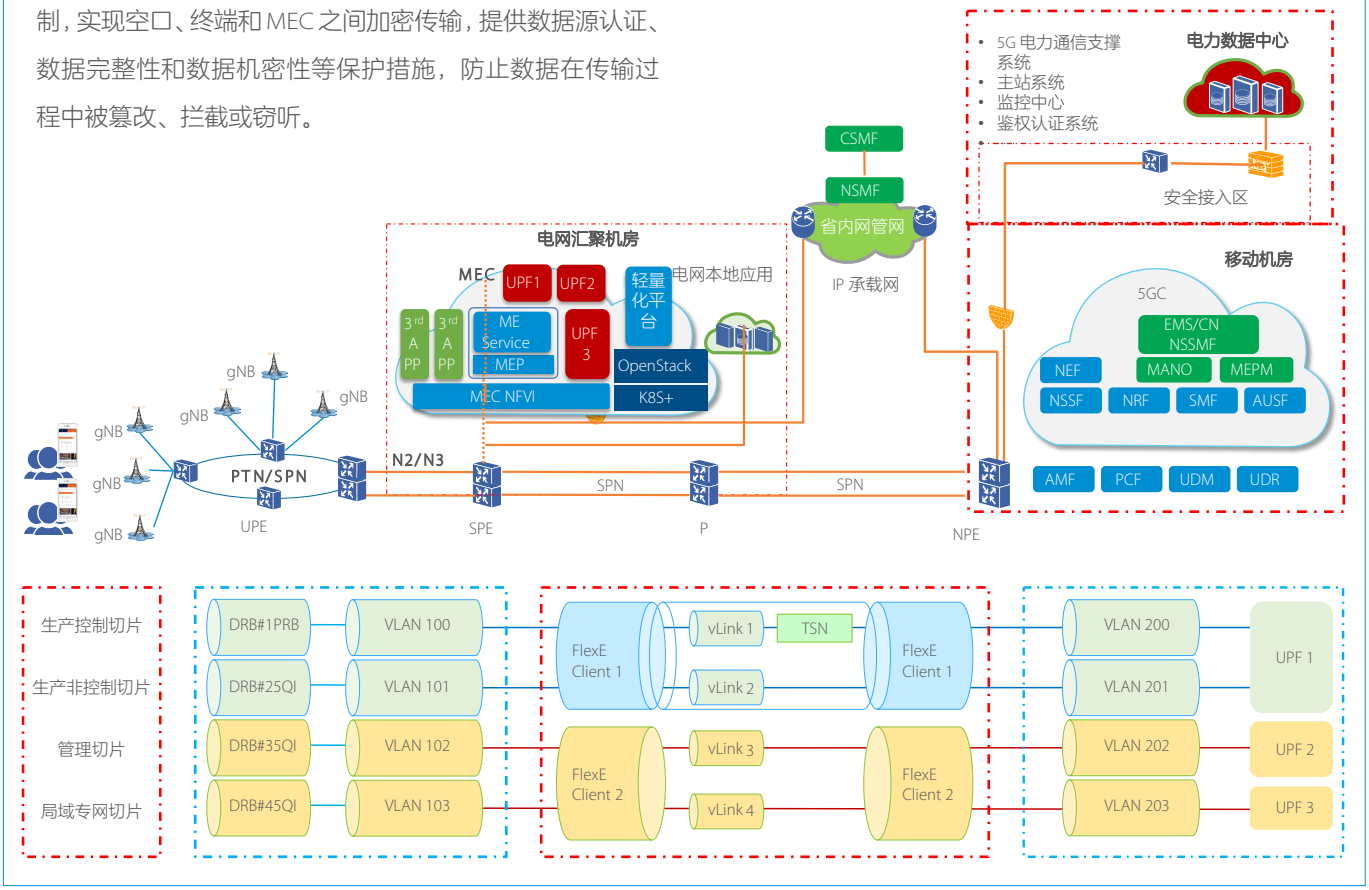


图 7-3 5G+ 智能电网切片安全隔离

❸ 5G 行业资产安全管理系统

5G 行业资产管理系统通过以下功能来实现对 5G+ 智能电网的资产安全管理。

- **数据采集**：采集电信业务网络中的安全数据以支持上层的安全分析，安全数据包括资产信息（资产如切片、网元、虚机、物理机、服务、端口等）、资产日志、信令 & 用户面流量及网络中配套的其它安全设备日志。
- **资产安全态势感知**：对采集到的网络资产进行层级关联，形成资产拓扑关系图，从资产维度体现资产存在的安全威胁（漏洞、安全事件、风险等），并对资产进行风险评估，通过资产关联关系对威胁进行定位，并结合 5G 网络业务进行资产安全态势评估。
- **漏洞管理**：提供漏洞管理功能对网络中存在的漏洞及漏洞位置进行一览、诊断和处置。
- **高级威胁检测**：支持已知、未知威胁检测。通过丰富的规则库对现存已知的安全威胁进行检测，采用机器学习技术对潜在的安全威胁进行发现。
- **日志 / 流量安全检测**：基于原始流量和海量日志数据，通过规则引擎、AI 检测引擎、关联分析引擎发现已知、未知安全事件。
- **5G 威胁检测**：建立特定的基线分析模型，检测移动网络特有的安全威胁，例如信令风暴、网元异常访问、漫游信令异常等。

- **威胁告警**：威胁事件告警展示，直接查询威胁事件发生时间、威胁等级、事件详情等信息，并在仪表盘进行 topN 威胁事件推荐。产品可通过邮件、短信等方式提醒管理员关注特定的安全事件。
- **溯源取证**：保存采集的原始流量和日志信息用于威胁溯源取证。原始采集数据至少保存 6 个月。

可视化与报表：提供作战大屏、仪表盘对网络中存在的威胁和风险情况进行直观感知；提供系统分析结果报告导出及用户定制化统计报表功能。

编排响应：采用 SOAR 技术进行自动化响应剧本编排，联动网络中的其它安防设备（如 EDR、NDR、防火墙等）进行响应阻断。

❹ 实施效果

通过在 CPE 上引入 eSIM 技术并配合 5G 模组，提供移动网络接入鉴权和用户身份认证的安全服务，保证终端的安全性的同时，不影响业务性能和网络延时，有力保障了终端可靠安全接入。

根据电力网络差异化的 5G 业务场景安全需求，采用切片技术进行安全隔离，并对切片隔离情况进行安全验证，满足了电力业务安全定制化需求。

对 5G 通信系统不同层级资产存在的漏洞、脆弱性、异常行为进行监测，结合各个维度的安全问题进行资产风险评估，更直观了解业务网络中存在的风险点、风险位置、严重程度及波及范围，实现 5G 整体安全态势感知可管可控。

7.2 5G+ 智慧地铁网络安全应用解决方案

❶ 应用简介

广东移动携手中兴通讯、广州地铁等单位，基于 5G SA 网，集中应用了网络切片、边缘计算、室内高精度定位等最前沿的 5G 关键技术，建设了广州塔智慧地铁示范站行业专网，率先实现了全球首个无线 PRB（Physical Resource Block）硬隔离切片方案，实现敏感数据不出地铁、超低时延及超高带宽，承载了人脸识别闸机、智慧安检、站内高精度定位、智能客服中心、站内高清视频监控等地铁站厅业务，打造了地铁行业专网业务应用模式。

❷ 安全需求

5G 网络的引入，打破了原有相对封闭的网络环境，地铁业务及管理数据与运营商的网络数据汇聚在 MEC 上，基于数据安全的考虑，要求数据不出园区。通过网络切片安全隔离、边缘计算（MEC）安全防护、端到端数据安全保护来保障广州地铁 5G+ 智慧地铁项目安全运行。

5G 网络切片为 5G+ 智慧地铁不同业务提供差异化安全服务，不同的网络切片承载不同的 5G+ 智慧地铁业务，实现不同类型业务之间的逻辑隔离，满足控制业务端到端超低延时和高可靠性要求。

MEC 将承载重要地铁业务数据流量，同时作为边缘云还会承担相关的地铁业务以及开放网络能力，例如室内高精度定位业务，所以同样面临传统的各类网络安全问题，考虑性能、成本、部署灵活性要求等多种因素，还需要综合增强 MEC 的安全防护能力，包括物理环境、网络、系统及平台、业务与应用等安全防护。

5G+ 智慧地铁数据将从传统的少量、单一、单向数据逐步发展为大量、多维、双向数据，5G+ 智慧地铁用户多样化、设备多样化、业务多样化、平台多样化的网络发展趋势，使得地铁业务数据在用户、设备、业务、平台之间持续流动，导致传统网络安全边界模糊，其遭到攻击影响到数据的安全性的风险增加。

❸ 安全方案

为满足上述的安全需求，通过基于业务优先调度、多层次网络切片隔离安全、多元化边缘计算（MEC）安全、端到端数据安全保护，实现敏感数据不出地铁、超低时延及超高带宽，实现地铁信息高速传输、互联互通、智能应用，提升智能调度成效，为市民提供高效便捷的信息交互和乘车体验，有效提升广州地铁服务管理水平。

●PRB 硬隔离切片方案

5G SA 环境的无线 PRB 硬隔离切片方案，解决方案涵盖了 5G 商用终端、5G 基站、承载及 5G 核心网，构建了端到端的 5G 地铁切片，标志着 5G 切片专网技术正式在地铁领域展开应用。

终端层面，普通切片和地铁切片采用不同的用户终端，根据接入控制各自接入到相应的切片中进行物理隔离；无线层面，采用 PRB 硬隔离为地铁切片预留了相关空口资源，实现地铁业务优先保障；传输层面，通过 VPN 方式对两种切片进行逻辑隔离；核心网层面，将各个子切片端到端拉通，普通切片和地铁切片采用 UPF 独享，实现用户数据隔离；应用层面，地铁用户专线接入地铁数据中心，实现物理隔离。

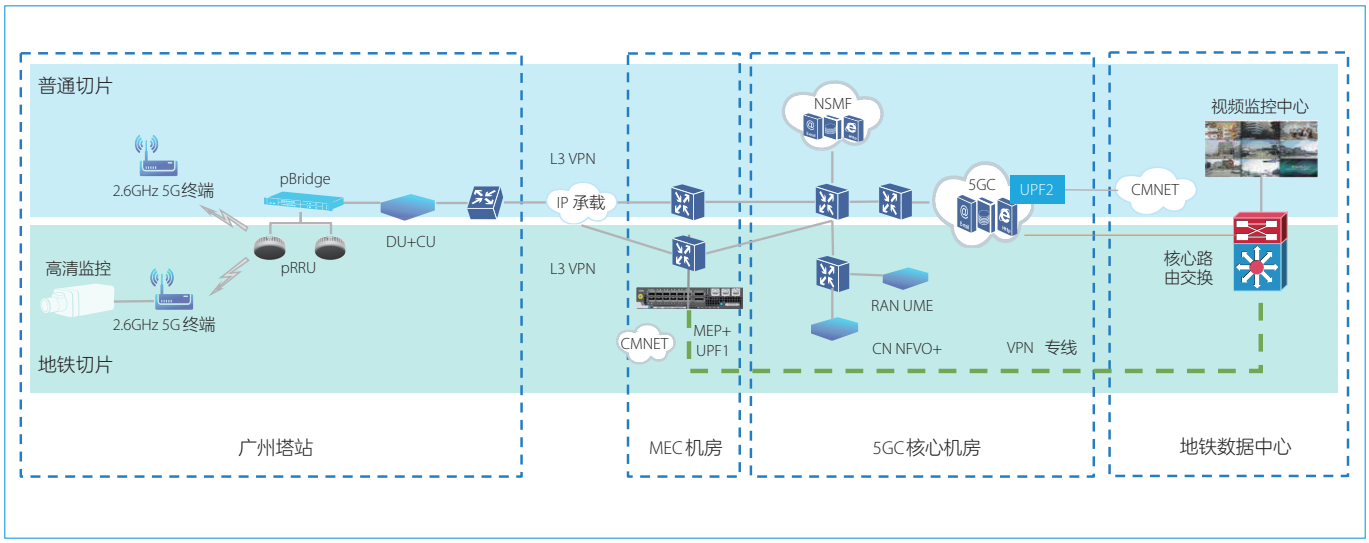


图 7-4 PRB 硬隔离切片

●MEC 本地分流实现数据不出地铁

MEC 本地分流实现数据不出地铁，保证数据端到端安全主要有三个方面，第一是接入认证，包括主认证和切片二次认证，保证用户合法接入，同时双向认证保证用户和网络之间的相互可信；第二是数据访问控制，防止接入用户的非授权访问网络切片；第三是地铁数据走 VPN 专线不出虚拟专网，不出地铁，针对地铁高价值资产数据，在空口、UE 和 MEC 之间使用 IPSec/TLS 等安全传输方式，对需要保护的信息进行机密性和完整性保护，同时 MEC 内部边界做安全隔离。

❹ 实施效果

基于 5G 的 MEC 技术，采用了多元化的安全防护，实现乘客的精准定位，从而实现客流分布、客流预测和客流引导等多种业务，基于 5G 的网络切片技术，通过预留一定比例的 PRB 资源，保障地铁专网的最小带宽和最大可调用带宽，实现地铁专网和公网的安全隔离，从而保障地铁安全稳定。端到端数据安全保护，保证地铁业务数据分类分级加密传输存储，不出地铁园区。整体方案提高了系统的响应性能、运作能力和安全性，进一步支撑轨道交通数字化转型的发展。

08

未来展望

随着“中国制造 2025”、“工业 4.0”、“新基建”等战略概念的提出，新一轮科技革命和产业变革浪潮席卷而来，工业转型升级的新机遇已然到来。制造业要从基于要素的低成本战略转向基于创新的差异化战略，才能推进产业转型升级，为此工业系统需要吸纳各种先进技术，特别是与 5G 进行深度的融合，充分利用 5G 的大带宽、低时延、广覆盖的网络特性来提升整个工业系统的信息化水平。

在 5G 与工业互联网融合的过程中必然会带来安全问题，目前的 5G 工业互联网安全防护发展尚处起步阶段。随着 5G 融入工业互联网的广度和深度持续增强，有必要引入新的安全理念、安全技术，不断完善 5G 工业互联网安全防护体系，以支撑工业数字化转型升级行稳致远。为抵御不断演变的高级威胁，未来对于 5G 工业互联网安全防护的思维模式需要从传统的事件响应式向持续智能响应式转变，通过引入主动式、智能化的威胁检测与安全防护技术，构建全面的预测、基础防护、响应和恢复能力，同时利用机器学习、深度学习等人工智能技术分析处理安全大数据，从而不断改善安全防御体系。

5G 与工控系统的深度融合是工业互联网提质增效的关键，而要调和 5G 网络的开放性与工控协议的私密性，特别是解决工控协议安全性较弱的问题，就必须要引入内生安全防御的理念，即提升工业互联网自身在安全设计方面的完备性，提高工业互联网自身的免疫力。5G 的引入使得工业网络带宽与计算设备处理性能得到很大提升，为更多安全机制引入工业互联网的安全防护提供了可能。首先要加强 MEC 平台 IaaS 层、PaaS 层及 Sass 层的安全接入与安全加固，然后对于安全保障机制欠缺的各类工控通信协议，需要加入数据加密、身份验证、访问控制、完整性验证等机制提升其安全性，并逐步取代现有通信协议。

另外，5G 网络的开放性，将加速推动工业互联网跨部门、跨行业、跨平台信息共享和联动处置机制建立。受限于资源及技术等多方面因素，任何一个企业都很难进行单独的防御，为此，基于 5G 网络的工业互联网企业，需要与移动运营商、设备提供商、安全服务商、监管机构等建立协同机制，共同应对来自 5G、工业等跨领域、跨行业的安全挑战。而 5G 工业互联网的安全能力，将成为一种可定制的服务，工业互联网企业可以根据自己的实际需求灵活定制。

09

附录 1（术语表）

中文名称	英文名称	定义
5G	5th generation mobile networks	最新一代蜂窝移动通信技术，也是继 4G（LTE-A、WiMax）、3G（UMTS、LTE）和 2G（GSM）系统之后的延伸。5G 的性能目标是高数据速率、减少延迟、节省能源、降低成本、提高系统容量和大规模设备连接。
工业互联网	Industrial Internet	工业互联网是满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。
5QI	5QI	5QI 是一个标量，用于索引一个 5G QoS 特性，3GPP TS23.501 Table 5.7.4-1 有标准化的 5QI 映射关系。
工业控制系统	Industrial control system	工业控制系统（ICS）是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC），现已广泛应用在工业部门和关键基础设施中。
云计算	Cloud Computing	云计算通常简称为“云”。通过互联网，“按使用量付费”的方式提供随需应变的计算资源（从应用到数据中心）。其部署方式包括公有云、私有云和混合云。
边缘计算	Edge Computing	在靠近物或数据源头的网络边缘侧，融合联接、计算、存储、应用核心能力的开放平台，就近提供边缘智能服务，满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。
网络切片	Network Slice	网络切片是一种按需组网的方式，可以让运营商在统一的基础设施上分离出多个虚拟的端到端网络，每个网络切片从无线接入网承载网再到核心网上进行逻辑隔离，以适配各种各样类型的应用。

中文名称	英文名称	定义
网络安全	Cyber Security	通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。
身份验证	Authentication	身份验证又称“验证”、“鉴权”，是指通过一定的手段，完成对用户身份的确认。身份验证的方法有很多，基本上可分为：基于共享密钥的身份验证、基于生物学特征的身份验证和基于公开密钥加密算法的身份验证。
访问控制	Access Control	访问控制是给出一套方法，将系统中的所有功能标识出来，组织起来，托管起来，将所有的数据组织起来标识出来托管起来， 然后提供一个简单的唯一的接口，这个接口的一端是应用系统一端是权限引擎。权限引擎所回答的只是：谁是否对某资源具有实施 某个动作（运动、计算）的权限。返回的结果只有：有、没有、权限引擎异常了。
嵌入式操作系统	Embedded Operating System	嵌入式操作系统是一种用途广泛的系统软件，通常包括与硬件相关的底层驱动软件、系统内核、设备驱动接口、通信协议、图形界面、标准化浏览器等。
零信任	Zero Trust	零信任既不是技术也不是产品，而是一种安全理念。根据 NIST《零信任架构标准》中的定义：零信任（Zero Trust，ZT）提供了一系列概念和思想，在假定网络环境已经被攻陷的前提下，当执行信息系统和服务中的每次访问请求时，降低其决策准确度的不确定性。零信任架构（ZTA）则是一种企业网络安全的规划，它基于零信任理念，围绕其组件关系、工作流规划与访问策略构建而成。
内生安全	SECURITY BUILT-IN DNA	指面对不断变化的网络威胁，网络安全进化到了“内生安全”时代，需要依靠聚合，从信息化系统内不断生长出自适应、自主和自成长的安全能力。
主动防御	Active Defense	是指网络能够在主动或者被动触发条件下执行各种硬件变体及相应的软件变体的一种防御方式。
态势感知	Situation Awareness	态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。
大数据	Big Data	指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产。

10 附录 2（缩略语表）

缩略语	英文名称	中文名称
3GPP	Third Generation Partnership Project	第三代合作伙伴计划
5GC	5G Core network	5G 核心网
AR	Augmented Reality	增强现实
VR	Virtual Reality	虚拟现实
eMBB	Enhance Mobile Broadband	增强型移动互联网
uRLLC	Ultra Reliable & Low Latency Communication	超高可靠性与超低时延通信
mMTC	Massive Machine Type Communication	海量物联网通信
3D	3 Dimensions	三维空间
E2E	End to End	端到端
TSN	Time Sensitive Network	时间敏感网络
MEC	Multi-access Edge Computing	多接入边缘计算
NFV	Network Function Virtualization	网络功能虚拟化
SDN	Software Defined Network	软件定义网络
NF	Network Function	网络功能
DN	Data Network	数据网络
IT	Information Technology	信息技术
UPF	User Plane Function	用户面功能
API	Application Programming Interface	应用程序编程接口
ITU	International Telecommunication Union	国际电信联盟
FW	Fire Wall	防火墙

缩略语	英文名称	中文名称
VPN	Virtual Private Network	虚拟专用网络
WAF	Web Application Firewall	网站应用级入侵防御系统
IDS	Intrusion Detection Systems	入侵检测系统
FlexE	Flex Ethernet	灵活以太网
SLA	Service Level Agreement	服务等级协议
RAN	Radio Access Network	无线接入网络
PRB	Physical Resource Block	物理资源块
DRB	Data Radio Bearer	数据承载
QoS	Quality of Service	服务质量
VLAN	Virtual Local Area Network	虚拟局域网
PHY	Physical	端口物理层
MAC	Medium Access Control	数据链路层
AMF	Access and Mobility Management Function	接入及移动性管理功能
SMF	Session Management Function	会话管理功能
AUSF	Authentication Server Function	鉴权服务器功能
UDM	Unified Data Management	统一数据管理
UDR	Unified Data Repository	统一数据存储
PCF	Policy Control function	策略控制功能
NRF	NF Repository Function	网络存储功能
NSSF	Network Slice Selection Function	网络切片选择功能
DNN	Data Network Name	数据网络名称
AES	Advanced Encryption Standard	高级加密标准
SEPP	Security Edge Protection Proxies	安全边缘保护代理功能
TLS	Transport Layer Security	传输层安全
UE	User Equipment	用户设备
IPSec	Internet Protocol Security	网际协议安全
SSL	Secure Sockets Layer	安全套接层
APT	Advanced Persistent Threat	高级持续性威胁
IaaS	Infrastructure as a Service	基础设施即服务
PaaS	Platform as a Service	平台即服务
SaaS	Software as a Service	软件即服务

11 附录 3（参考文献）

[1] 3GPP TS 33.501. Security Architecture and Procedures for 5G System[S], 3GPP.

[2] 5G-ENSURE_D2.7 Security Architecture[R], 5GPPP.

[3] ETSI GS MEC-002. MEC Technical Requirements[S], ETSI.

[4] IMT-2020 5G Network Security Requirement & Architecture[R], IMT-2020.

[5] GTI 5G Network Security Consideration[R], GTI

[6] ZHAO Fuchuan, WEN Jianzhong. Slicing Packet Network Infrastructure and Key Technologies for 5G Mobile Backaul[J], ZTE TECHNOLOGY,2018.8.

[7] Recommendation ITU-T X.rdmase: Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment[R], ITU-T.

[8] 5G Security White Paper: Security Makes 5G Go Further[R],GSMA

[9] 5G 信息安全白皮书 [R], 未来移动通信论坛

[10] AII- 工业互联网安全总体要求 , 工业互联网产业联盟

[11] AII- 工业互联网平台安全防护要求 , 工业互联网产业联盟

[12] AII- 工业互联网典型安全解决方案案例汇编（2019），工业互联网产业联盟

[13] Zero Trust Architecture:NIST,Draft Special Publication (SP) 800-207November 22, 2019.

[14] 尤肖虎 , 潘志文 , 高西奇 , 等 . 5G 移动通信发展趋势与若干关键技术 [J], 中国科学 : 信息科学

[15] 5G 网络安全需求与架构白皮书 [R],IMT-2020

[16] 基于 SDN/NFV 的电信网安全技术白皮书 [R],SDN/NFV 产业联盟