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

中国移动 China Mobile

CAICT 中国信通院

5G 边缘计算安全白皮书

发布日期：2020 年 11 月

参与编写单位：

中国移动通信集团有限公司
中国信息通信研究院
中国电信集团公司
中国联通股份有限公司
北京邮电大学
中国南方电网有限责任公司
爱立信（中国）通信有限公司
上海诺基亚贝尔股份有限公司
华为技术有限公司
中兴通讯股份有限公司
三一重工股份有限公司
北京交通大学
双湃科技有限公司
北京奇虎科技有限公司
北京六方云科技有限公司
北京山石网科信息技术有限公司
北京神州绿盟科技有限公司
杭州安恒信息技术股份有限公司
东软集团股份有限公司
北京万维物联科技发展有限公司
长扬科技（北京）有限公司
北京信安世纪科技股份有限公司
郑州信大捷安信息技术股份有限公司
工业信息安全（四川）创新中心有限公司
江苏亨通工控安全研究院有限公司

编写组成员：

张　滨、袁　捷、魏　亮、张　峰、于　乐、田慧蓉、沈　彬、陶耀东、李江力、李祥军、林　欢、闫　霞、张弘扬、安宝宇、张国翊、曹　扬、袁　琦、程　渤、赵　帅、何国锋、张建宇、高　枫、董　悦、滕志猛、陆　伟、李　娜、刘秀龙、朱　兵、徐高峰、葛林娜、张雪菲、李鸿彬、张　屹、任　亮、魏立平、辛　毅、陈　凯、高　勇、汪义舟、刘尚麟、张　森、付　军、李剑锋、谷久宏、张洪宇、刘为华、胡晶晶、常　静、陈夏裕

PREFACE 前言

5G 边缘计算作为 5G 网络新型网络架构之一，通过将云计算能力和 IT 服务环境下沉到移动通信网络边缘，就近向用户提供服务，从而构建一个具备高性能、低时延与高带宽的电信级服务环境 [1]。

5G 边缘计算将核心网功能下沉到网络边缘，具备丰富的应用场景，带来新的安全挑战的同时，也加大了安全监管难度；与此同时，原有的安全防护方案并没有覆盖到边缘场景，包含 3GPP 等国际标准组织针对边缘计算的标准，都在同步研制和探讨中 [2-6]。本白皮书结合前期的实践经验，面向运营商和 5G 行业用户，提出了 5G 边缘计算安全防护策略，方便行业用户在开展 5G 边缘计算应用的同时，落实安全三同步（同步规划、建设、维护）方针，指导行业提升边缘计算的安全能力。

CONTENTS

目录

01 5G 边缘计算概述

1.1 5G 边缘计算介绍

5G 边缘计算（Multi-access Edge Computing，MEC）是指在靠近用户业务数据源头的一侧，提供近端边缘计算服务，满足行业在低时延、高带宽、安全与隐私保护等方面的基本需求，如：更接近用户位置的实时、安全处理数据等。

5G PPP 发布的白皮书《5G empowering vertical industries》[7] 指出，5G 通过边缘计算技术将应用部署到数据侧，而不是将所有数据发送到集中的数据中心，满足应用的实时性。白皮书认为，智慧工厂、智能电网、智能驾驶、健康医疗、娱乐和数字媒体是未来最具商业规模且排名靠前的边缘计算需求场景，极具典型性，并且运营商也在这些领域与行业客户紧密合作，基于用户需求，共同推动边缘计算的发展，为用户提供安全可靠的边缘计算业务。2019 年由边缘计算产业联盟（ECC）与工业互联网产业联盟（AII）联合发布的《边缘计算安全白皮书》[1] 中指出边缘计算具有资源约束、分布式、实时性等特征，所以边缘计算安全防护需考虑海量、异构、资源约束、分布式、实时性等特征，提出轻量级、针对性的边缘计算安全防护架构。

1.2 5G 边缘计算场景

综合不同业务对时延、成本和企业数据安全性的考量，下沉到汇聚机房和园区是主力部署方案，MEC 的部署场景可分为广域 MEC 和局域 MEC 两大类。

1.2.1 广域 MEC 场景

对于低时延业务，由于百公里传输引入的双向时延低于 1ms，基于广域 MEC 的 5G 公网已经能够为大量垂直行业提供 5G 网络服务。权衡应用对接、运维复杂度、设备和工程成本等多种因素，MEC 部署在安全可控的汇聚机房是当前运营商广域 MEC 的主力方案。

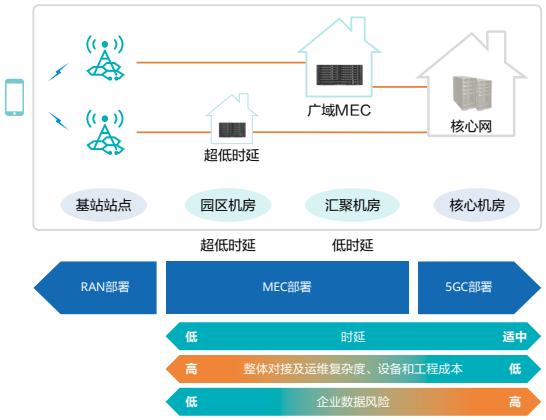

图 1-1 MEC 部署场景

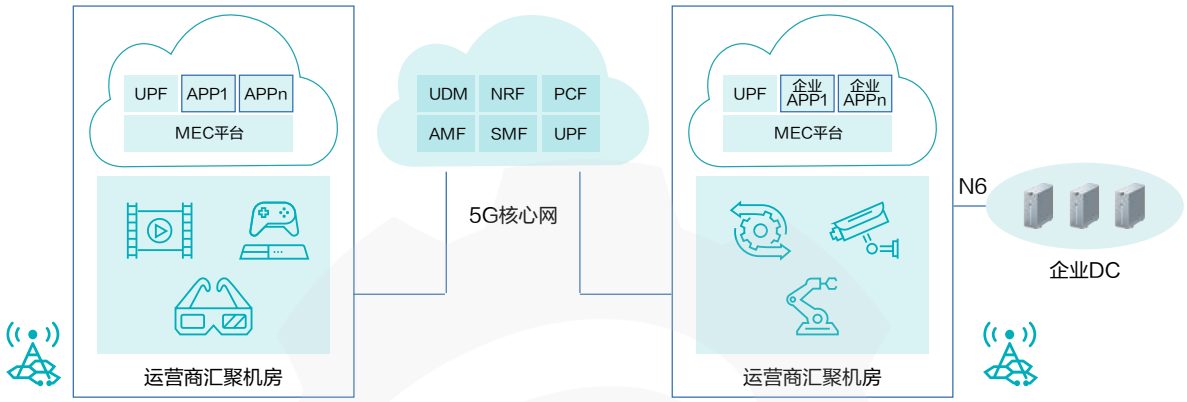

图 1-2 广域 MEC 场景

广域 MEC 的主要应用场景包括：大网 OTT 连接（Cloud VR/ 云游戏）、大网集团连接（公交广告 / 普通安防）、大网中的 URLLC 专网（电力等）、大网专线连接（企业专线）等，这些应用场景下，通过将 MEC 部署在汇聚机房，满足低时延的业务诉求。

1.2.2 局域 MEC 场景

对于安全与隐私保护高敏感的行业，可以选择将 MEC 部署在园区，以满足数据不出园的要求。

港口龙门吊的远程操控，钢铁厂的天车远程操控，以及大部分的制造、石化、教育、医疗等园区 / 厂区都是局域 MEC 的典型场景。局域 MEC 部署场景下，MEC 将满足 URLLC 超低时延业务；同时支持企业业务数据本地流量卸载（LBO），为园区客户提供本地网络管道。通过增强隔离和认证能力，防止公网非法访问企业内网，构建企业 5G 私网。

- 通过 DNN、切片等方案组成企业子网，只允许无线终端接入园区内网络；
- 通过机卡绑定、企业 AAA 二次鉴权等手段，只允许特定终端访问园区网络；
- 通过基站广播园区专用 PLMN ID+NID 或者 CAG ID，只允许企业终端接入园区专用网络。

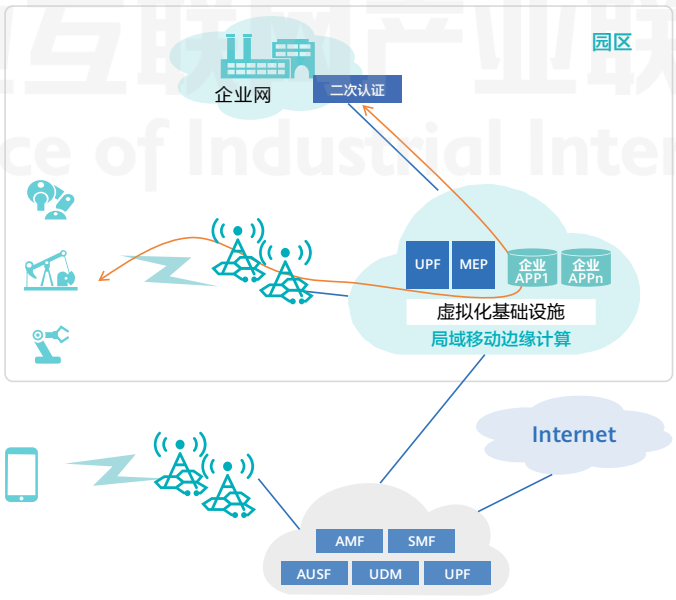

图 1-3 局域 MEC 场景

02
5G 边缘计算标准及政策

2.1 5G 边缘计算相关标准

MEC 标准是双规发展制，一方面 ETSI 着重定义 MEC 的平台、虚机和 API 管理等标准；另一方面 3GPP 着重定义 MEC 和其它 5G 核心网元的交互方式，因此 MEC 从架构上归属核心网。典型的，ETSI 规定了 UPF 网元的位置即为 MEC 在 5G 网络架构中的位置。

ETSI 2016 年 3 月发布了 ETSI GS MEC 003, 定义了移动边缘计算的框架和参考架构；后续还定义了 GS MEC 009、GS MEC 010-2、GS MEC 011、GS MEC 012 和 GS MEC 013 等标准，涵盖了应用生命周期管理，移动边缘应用支持，无线网络信息和位置等主题。

3GPP 在 5G 网络架构标准规范 TS 23.501（Release 15）中也对 5G 边缘计算定义了交互标准（support for Edge Computing）。目前 3GPP 的 Release 17 中对 MEC 增强以及 MEC 安全启动标准制订预计 2021 年 3 月后发布。

ITU 立项了 ITU-T X.5Gsec-netec“Security capabilities of network layer for 5G edge computing” 和 ITU-T X.5Gsec-ecs "Security Framework for 5G Edge Computing Services" 两项边缘计算安全国际标准项目。

中国通信行业标准 CCSA 在《5G 核心网边缘计算总体技术要求》也提出了 5G 边缘计算系统架构，如下图所示：

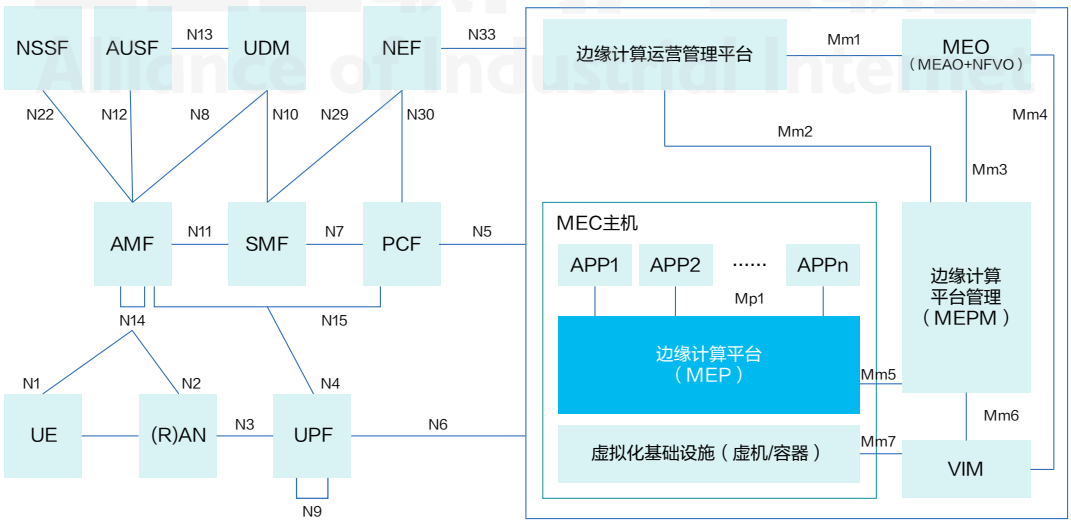

图 2-1 5G 边缘计算系统逻辑架构

CCSA 的 5G 边缘计算系统逻辑架构将 5G 的 UPF 作为边缘计算的数据面，边缘计算平台系统（MEP）为边缘应用提供运行环境并实现对边缘应用的管理。5G 边缘计算平台系统相对于 5G 核心网络是 AF+DN（应用功能 + 数据网络）的角色，与 UPF 之间为标准的 N6 接口连接。

此外，CCSA 正在研究《5G 边缘计算安全技术研究》与《5G 多接入边缘计算安全防护要求》。

2.2 5G 边缘计算安全边界定义

3GPP 标准上核心与非核心界面明确，即使 5G 核心网的部分功能（如 UPF）下沉，位置上接近应用，依然遵循 5G 核心网的配置分流策略，仍属于核心网。而且 5G MEC 和 RAN 接入网位于不同的安全等级中，两者之间必须部署安全网关或者防火墙，以确保 MEC 和 RAN 之间的接口安全；同时，两者的接口是 3GPP 标准定义的，MEC 和 RAN 可以来自不同的厂商，各厂家遵从 3GPP 和 ETSI 标准，根据 3GPP 标准定义接口实现解耦和互操作。

CCSA 的安全架构中规定 MEC 的安全边界：MEC 除支持 UPF 通用安全要求外，还要求“应部署在运营商可控、具有基本物理安全环境保障的机房，UPF 网元或者虚拟化 UPF 所在的基础设施应具备物理安全保护机制（如：防拆、防盗、防恶意断电、防篡改等，设备断电 / 重启、链路断开等问题发生后应触发告警）。”因此，相比 RAN 的广域部署模式，MEC 与 RAN 部署在不同的地理位置和安全区，所需要的保障安全等级是完全不同的。MEC 原则上部署在物理安全环境有保障的机房，如，园区和汇聚机房。因此与 RAN 的基站之间的安全边界是清晰的，不可模糊的。

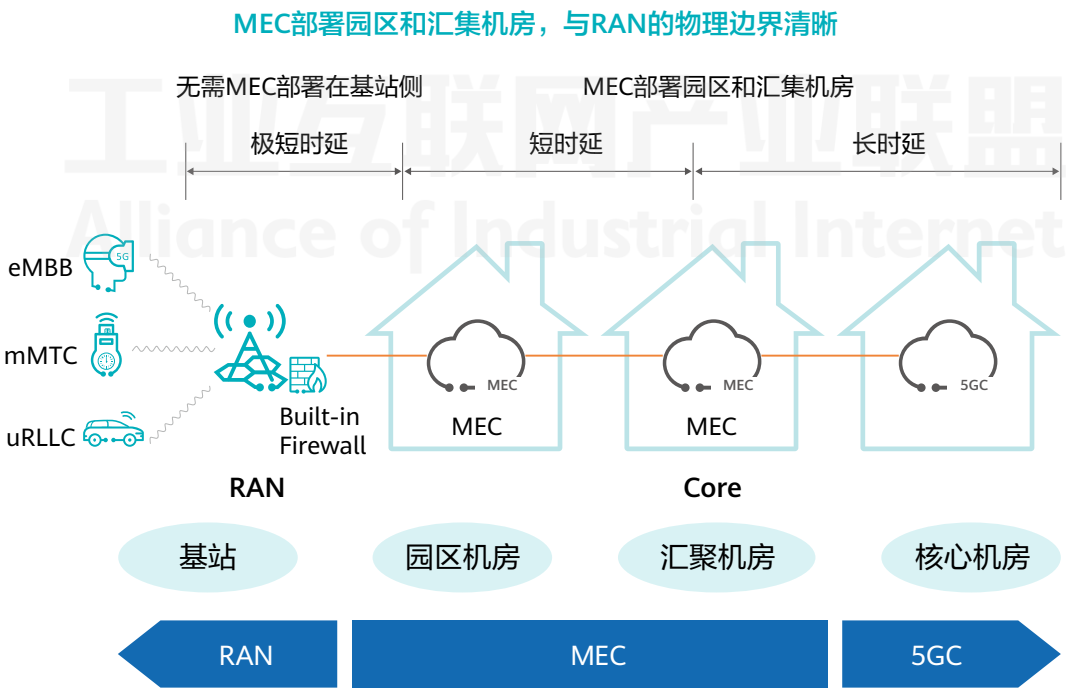

图 2-2 5G 边缘计算典型部署位置

03
5G 边缘计算安全威胁

一方面，MEC 节点的计算资源、通信资源、存储资源较为丰富，承载了多个企业的敏感数据存储、通信应用和计算服务，一旦攻击者控制了边缘节点，并利用边缘节点进行进一步的横向或纵向攻击，会严重破坏应用、通信、数据的保密性、可用性和完整性，会给用户和社会带来广泛的新型安全威胁。与此同时，MEC 节点常常部署在无人值守的机房，且安全生命周期里具备多重运营者和责任方，同时给物理安全防护以及安全运营管理带来了更多的挑战。

3.1 网络服务安全威胁

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。

3.2 硬件环境安全威胁

相比核心网中心机房完善的物理安全措施，边缘计算节点可能部署在无人值守机房或者客户机房，甚至人迹罕至的的地方，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。

3.3 虚拟化安全威胁

边缘计算基础设施中，容器或虚机是主要部署方式。攻击者可篡改容器或虚机镜像，利用 Host OS 或虚拟化软件漏洞攻击，针对容器或虚机的 DDoS 攻击，利用容器或虚机逃逸攻击主机或主机上的其他容器和虚机等威胁。

3.4 边缘计算平台安全威胁

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。

3.5 应用安全威胁

边缘计算节点连接海量的异构终端，承载多种行业的应用，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。

边缘计算平台上可能会部署多个第三方 APP，因此会存在 APP 之间的非法访问的安全威胁，以及第三方 APP 恶意消耗 MEC 系统资源造成系统服务不可用的安全威胁。

工业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 Dos 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。

3.6 能力开放安全威胁

MEC 为边缘计算提供了一个应用承载的平台。为了便于用户开发所需的应用，MEC 需要为用户提供一系列的开放 API，允许用户访问 MEC 相关的数据和功能。这些 API 为应用的开发和部署带来了便利，同时也成为了攻击者的目标。如果缺少有效的认证和鉴权手段，或者 API 的安全性没有得到充分的测试和验证，那么攻击者将有可能通过仿冒终端接入、漏洞攻击、侧信道攻击等手段，达到非法调用 API、非法访问或篡改用户数据等恶意攻击目的。

3.7 管理安全威胁

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。由于边缘计算节点分布式部署，对于运营商来说这将意味着有大量的边缘节点需要进行管理和运维。

为了节省人力，边缘节点依赖远程运维，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。

3.8 数据安全威胁

5G 边缘计算平台可收集、存储与其连接设备的数据，包括应用数据、用户数据等。5G 边缘计算的数据面临的安全风险包括数据损毁风险、数据泄露风险。

因 5G MEP 平台设备毁坏、设备遭受攻击、重要数据未备份、未具备数据恢复机制等造成的数据损毁等安全风险。

5G MEP 平台业务开展过程中可获得和处理用户敏感隐私数据，因未实施数据分级分类管理，未部署敏感数据加密、脱敏手段，或开展不合规的数据开放共享等，可能导致数据泄露等安全风险。

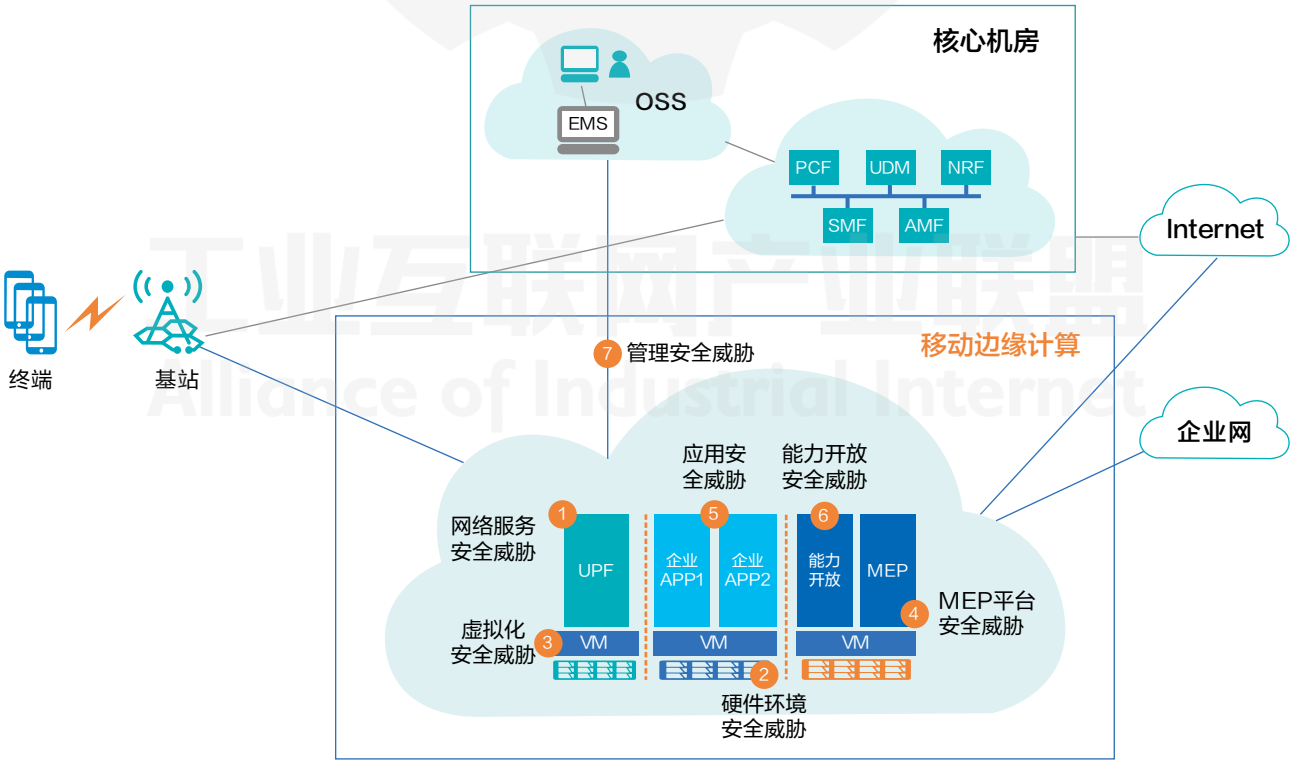

图 3-1 MEC 的安全风险

04

5G 边缘计算安全防护

4.1 5G 边缘计算安全防护架构

由于行业的需求差异，UPF、边缘计算平台存在不同的部署方式：

» 对于广域 MEC 场景，行业用户无特殊的边缘计算节点的部署位置需求，UPF 和边缘计算平台可部署在安全可控的运营商汇聚机房，为用户提供服务。

» 对于局域 MEC 场景，行业用户数据的敏感程度高，用户会要求运营商的 UPF 和边缘计算平台均部署在用户可控的园区，实现敏感数据不出园区。

无论对于广域 MEC 还是局域 MEC 场景，行业用户除了使用 MEP 平台之外，还可能要求边缘侧 UPF 负责行业用户的业务数据流量转发。不同的部署方式，导致运营商网络的暴露面不同，所以，应针对不同的部署方式及业务需求考虑边缘计算的安全要求，设计相应的安全解决方案，在保证运营商网络安全的同时，为行业用户提供安全的运行环境以及安全服务。

5G 边缘计算安全体系包括基础设施安全（硬件安全和虚拟化安全）、网络安全、边缘计算平台安全、应用安全、能力开放安全和管理安全，如下图 5-1 所示。

图 4-1 5G 边缘计算安全防护架构

4.2 5G 边缘计算安全防护要求

4.2.1 网络服务安全

4.2.1.1 组网安全要求

在 5G 边缘云计算平台中除了要部署 UPF 和 MEP 之外，还要考虑在 MEC 上部署第三方 APP，其基本组网安全要求如下：

» 三平面隔离：服务器和交换机等，应支持管理、业务和存储三平面物理 / 逻辑隔离。对于业务安全要求级别高并且资源充足的场景，应支持三平面物理隔离；对于业务安全要求不高的场景，可支持三平面逻辑隔离。

» 安全域划分：UPF 和通过 MP2 接口与 UPF 通信的 MEP 应部署在可信域内，和自有 APP、第三方 APP 处于不同安全域，根据业务需求实施物理 / 逻辑隔离。

» INTERNET 安全访问：对于有 INTERNET 访问需求的场景，应根据业务访问需求设置 DMZ 区（如 IP 地址暴露在 INTERNET 的 portal 等部署在 DMZ 区），并在边界部署抗 DDoS 攻击、入侵检测、访问控制、WEB 流量检测等安全能力，实现边界安全防护。

» UPF 流量隔离：UPF 应支持设置白名单，针对 N4、N6、N9 接口分别设置专门的 VRF；UPF 的 N6 接口流量应有防火墙进行安全控制。

5G 边缘计算的组网安全与 UPF 的位置、MEP 的位置以及 APP 的部署紧密相关，还需要根据不同的部署方式进行分析：

» 广域 MEC 场景：UPF 和 MEP 部署在运营商汇聚机房，在运营商边缘云部署 UPF 和 MEP，行业用户的 APP 到部署运营商的边缘 MEP，其组网要求实现三平面隔离、安全域划分、INTERNET 安全访问和 UPF 流量隔离等 4 个基本的安全隔离要求。

» 局域 MEC 场景：UPF 和 MEP 均部署在园区，其组网要求除了包括以上 4 个基本安全要求之外，在安全域划分方面，还需要园区 UPF 和通过 MP2 接口与 UPF 通信的 MEP 应与 APP 之间应进行安全隔离，以及 APP 与 APP 之间应进行隔离（如划分 VLAN）。在 UPF 流量隔离方面：除了 (1) 部署场景的要求，还应在 UPF 的 N4 口设置安全访问控制措施，对 UPF 和 SMF 的流量进行安全控制。

MEC 还包括专网业务场景，即 UPF 仅做转发，并且部署在运营商汇聚机房或者园区机房，同样需要实现上述 4 个安全要求。

4.2.1.2 UPF 安全要求

核心网功能 随着 UPF 下沉到 5G 网络边缘，增加了核心网的安全风险。因此，部署在 5G 网络边缘的 UPF 应具备电信级安全防御能力。UPF 需要遵从 3GPP 安全标准和行业安全规范，获得 NESAS/SCAS 等安全认证和国内行业安全认证。部署在边缘的 UPF 应具备与主流核心网设备的互操作性和接口兼容性。UPF 安全要求主要包括网络安全和业务安全。

1. UPF 网络安全要求如下：

(1) 支持网络不同安全域隔离功能

UPF 支持对网络管理域、核心网络域、无线接入域等进行 VLAN 划分隔离。UPF 的数据面与信令面、管理面能够互相隔离，避免互相影响。

(2) 支持内置接口安全功能

位于园区客户机房的 UPF 应支持内置接口安全功能，如支持 IPSec 协议，实现与核心网网络功能之间的 N3/N6/N4/N9/N19 接口建立 IPSec 安全通道，保护传输的数据安全。

(3) 支持信令数据流量控制

UPF 应对收发自 SMF 的信令流量进行限速，防止发生信令 DDoS 攻击。

2. UPF 的业务安全要求如下：

(1) 支持防移动终端发起的 DoS 等攻击行为

UPF 须支持对终端发起 DoS 攻击的防范，支持根据配置的包过滤规则（访问控制列表）对终端数据报文进行过滤。

(2) 协议控制功能

UPF 应具有协议控制功能，可以选择允许 / 不允许哪些协议的 IP 报文进入 5GC 网络，以保证 5GC 网络的安全。该功能也可以通过如防火墙来实现。

(3) 移动终端地址伪造检测

对会话中的上下行流量的终端用户地址进行匹配，如果会话中报文的终端地址不是该会话对应的终端用户地址，UPF 需要丢弃该报文。

(4) 同一个 UPF 下的终端互访策略

对于终端用户之间的互访，UPF 可以根据运营商策略进行配置，是否允许其互访。UPF 还应支持把终端互访报文重定向到外部的网关，由网关设备来决定是禁止还是允许终端互访。

(5) UPF 流量控制

UPF 应对来自 UE 或者 APP 的异常流量进行限速，防止发生 DDoS 攻击。

(6) 内置安全功能

内置虚拟防火墙功能，实现安全控制（如 UPF 拒绝转发边缘计算应用发送给核心网网络功能的报文）等。

(7) 支持海量终端异常流量检测

UPF和核心网控制面需要对海量终端异常行为进行检测，一方面识别并及时阻断恶意终端的攻击行为，保护网络可用性和安全性；另一方面，识别被攻击者恶意劫持的合法终端，为合法终端提供安全检测和攻击防御的能力。

UPF 对终端异常行为可以采取以下安全措施：

» 通过信令和数据流量的大数据分析来实现终端异常流量检测、异常信令过滤和信令过载控制；

» 针对合法终端被恶意劫持利用的攻击场景：可以通过对终端的数据流量特征解析和信令行为画像，发现恶意流量及异常信令行为的终端设备，从而有针对性地实施限制和管理。

» 核心网控制面可以针对终端信令进行安全检测，结合话统 / CHR 等数据，利用 AI 算法等技术，对信令 DDoS 攻击特征进行分析，从而定位引发 DDoS 的恶意终端。
» UPF 支持终端微分段和微隔离保护，防止其访问未经授权的资源，并隔离行为异常的设备或应用程序。

4.2.2 硬件环境安全

硬件环境安全包括物理环境安全、资产管理要求和设备硬件安全：

(1) 物理环境安全要求：
» 边缘计算系统机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员，机柜应具备电子防拆封功能，应记录、审计打开、关闭机柜的行为。边缘计算设备应是可信设备，应防止非法设备接入系统。

(2) 资产管理要求：
基础设施应具备资产管理能力，包括：
» 应支持物理资产的管理能力，物理资产的发现（纳管）、删除、变更及呈现。基础设施应支持宿主机的自动发现，对于交换机、路由器及安全设备应支持自动发现或手动添加资产库的能力。

» 应具备资产指纹管理能力。资产指纹管理功能支持采集分析、记录并展示以下四种指纹信息：端口（监听端口）、软件（软件资产）、进程（运行进程）、账户（账户资产）。资产功能支持设置监听端口、软件资产、运行进程和账户资产数据的采集刷新频率。能根据所设置的频率定期采集资产指纹。

(3) 设备硬件安全
MEC 服务器基于 TPM 硬件可信根启动和安全运行，确保启动链安全，防止被植入后门。在可信启动时，通过远程证明可以验证软件是否安全可信。MEC 服务器在启动阶段逐层度量计算 Hash 值，将 TPM 记录的度量值与远程证明服务器上预置的软件参考基准值进行比对（本地篡改无法影响远程服务器），确保软件合法运行。

4.2.3 虚拟化安全

宿主机安全技术要求

宿主机应禁用 USB、串口及无线接入等不必要的设备，应禁止安装不必要的系统组件，禁止启用不必要的应用程序或服务，如邮件代理、图形桌面、telnet、编译工具等，以减少被攻击的途径。

应根据用户身份对主机资源访问请求加以控制，防止对操作系统进行越权、提权操作，防止主机操作系统数据泄漏。

主机操作系统应进行安全加固，并为不同身份的管理员分配不同的用户名，不同身份的管理权限不同，应禁止多个管理员共用一个帐户。主机操作系统应设置合理的口令策略，口令复杂度、口令长度、口令期限等符合安全性要求，口令应加密保存。应配置操作系统级强制访问控制（MAC）策略。应禁止利用宿主机的超级管理员账号远程登录，应对登录宿主机的 IP 进行限制。

应启用安全协议对宿主机进行远程登录，禁用 telnet、ftp 等非安全协议对主机访问。应具备登录失败处理能力，设置登录超时策略、连续多次输入错误口令的处理策略、单点登录策略。

宿主机系统应为所有操作系统级访问控制配置日志记录，并应支持对日志的访问进行控制，只有授权的用户才能够访问。

镜像安全

虚拟机镜像、容器镜像、快照等需进行安全存储，防止非授权访问；基础设施应确保镜像的完整性和机密性，虚拟层应支持镜像的完整性校验，包括支持 SHA256、SM3 等摘要算法和签名算法来校验虚拟机镜像的完整性。应使用业界通用的标准密码技术或其他技术手段保护上传镜像，基础设施应能支持使用被保护的镜像来创建虚拟机和容器。

上传镜像时，约束镜像必须上传到固定的路径，避免用户在上传镜像时随意访问整个系统的任意目录。使用命令行上传镜像时，禁止用户通过 "../" 的方式任意切换目录。使用界面上传镜像时，禁止通过浏览窗口任意切换到其他目录。同时，应禁止 at、cron 命令，避免预埋非安全操作。

镜像发布需要通过漏洞扫描检查，至少保证无 CVE、CNVD、CNNVD 等权威漏洞库收录公开的“高危”或“超危”安全漏洞。

虚拟化安全

为了避免虚拟机之间的数据窃取或恶意攻击，保证虚拟机的资源使用不受周边虚拟机的影响，Hypervisor 要能够实现同一物理机上不同虚拟机之间的资源隔离，包括:

» vCPU 调度安全隔离
» 存储资源安全隔离
» 内部网络的隔离

终端用户使用虚拟机时，仅能访问属于自己的虚拟机的资源（如硬件、软件和数据），不能访问其他虚拟机的资源，保证虚拟机隔离安全，虚拟机应无法探测其他虚拟机的存在。

Hypervisor 应进行安全加固，其安全管理和安全配置应采取服务最小原则，禁用不必要的服务。

如果硬件支持 IOMMU（input/output memory management unit）功能，Hypervisor 应该支持该配置项以更好的管理 VM 对 DMA（Direct Memory Access）的访问。

应支持设置 VM 的操作权限及每个 VM 使用资源的限制，如最小 / 大的 vCPU，内存等，并能够正确监控资源的使用情况。

Hypervisor 可支持多角色定义，并支持给不同角色赋予不同权限以执行不同级别的操作。

对于虚拟化应用，迁移应用时，如安全组等访问控制策略随应用迁移。

为了防止虚拟机逃逸，通过虚拟机隔离提升虚拟化安全：对于部署在虚拟化边缘环境中的 VM，可以加强 VM 之间的隔离，对不安全的设备进行严格隔离，防止用户流量流入到恶意 VM 中。另外，可以实时监测 VM 的运行情况，有效发掘恶意 VM 行为，避免恶意 VM 迁移对其他边缘数据中心造成感染。

容器安全

容器安全应覆盖整个容器的生命周期，可以从开发、部署、运行三个阶段来进行安全防护。

开发阶段应要求开发者对 base 容器镜像以及中间过程镜像进行漏洞扫描检查，同时对第三方甚至自有应用 / 代码进行安全检查。部署阶段应由 MEP 平台对镜像仓库进行安全监管，对上传的第三方 / 自有容器镜像进行漏洞扫描，控制有高危漏洞的容器镜像的运行使用。运行阶段首先应支持容器实例跟宿主机之间的内核隔离；其次应支持容器环境内部使用防火墙机制防止容器之间的非法访问，例如可以使用容器自带的 NetworkPolicy 网络防火墙能力对容器实例之间的网络互访进行控制；再者需支持进程监控或流量监控对运行时容器实例的非法 / 恶意行为监控；最后需要考虑在平台层面部署 API 安全网关来对容器管理平台的 API 调用进行安全监管。

支持基于主机的容器行为感知能力，支持容器逃逸等恶意行为检测。

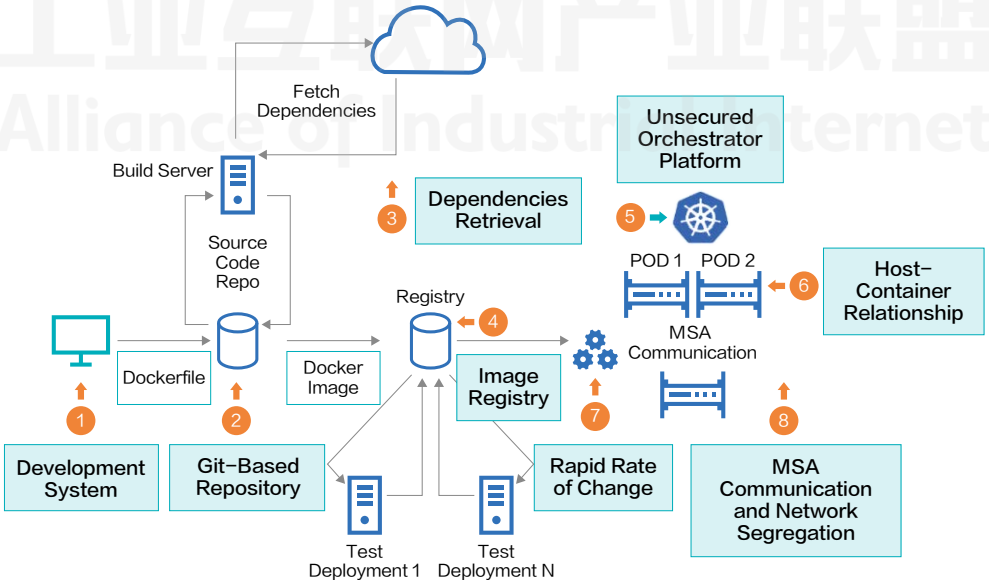

图 4-2 Gartner 的容器全生命周期攻击面分析

4.2.4 边缘计算平台安全

4.2.4.1 边缘计算平台系统安全

MEP（MEC Platform，边缘计算平台），不仅提供边缘计算应用的注册、通知，而且为应用提供 DNS 的请求查询功能、路由选择功能，本地网络的 NAT 功能，同时可以基于移动用户标识的控制管理能力，满足业务分流后的用户访问控制。MEP 还提供服务注册功能，将 MEP 平台的服务能够被其他服务和应用发现，也可以通过 API 接口的方式对外开放 MEP 的能力。

根据边缘计算架构，MEP 本身是基于虚拟化基础设施部署，需要虚拟化基础设施提供安全保障：应对 Host OS、虚拟化软件、Guest OS 进行安全加固，并提供 MEP 内部虚拟网络隔离和数据安全机制。MEP 对外提供应用的发现、通知的接口，应保证接口安全、API 调用安全。对 MEP 的访问需要进行认证和授权，防止恶意的应用对 MEP 的非授权访问。同时为防止 MEP 与 APP 等之间的通信数据被拦截、篡改，MEP 与 APP 等之间的数据传输应启用机密性、完整性、防重放保护。并且，MEP 应支持防 (D)DoS 攻击，MEP 的敏感数据应启用安全保护，防止非授权访问和篡改等。

边缘计算系统中的标准接口应支持通信双方之间的相互认证，并在认证成功后，使用安全的传输协议保护通信内容的机密性和完整性。

边缘计算系统应使用安全的标准通信协议，如 SSHv2，TLS v1.2 及以上版本，SNMP v3 等，禁止使用 telnet，FTP，SSHv1 等。

4.2.4.2 边缘服务授权

移动网络运营商需要对 UE 使用边缘计算服务进行授权，只有具备合法授权的用户才能使用对应的边缘计算服务。对于非运营商部署场景，5G 边缘计算服务提供商也应该采取类似的授权机制保证边缘计算服务不被非法访问。例如，当用户访问边缘应用时，核心网需要获取用户签约数据，若用户未签约则拒绝用户的访问，或者核心网与用户所访问的应用交互获取用户授权信息，只有用户具备合法的授权才允许用户访问 5G 边缘计算服务。

4.2.4.3 应用切换过程中的服务认证和授权

因为 UE 位置移动，或者是负载均衡等因素，边缘应用服务器会发生切换。需要考虑将必要的上下文安全地从源边缘应用服务器传递到其他服务器（边缘应用服务器或云应用服务器）以保证用户服务连续性。常见的切换触发有四种触发方式：EAS（边缘应用服务器）发起、EES（边缘使能服务器）发起、UE 侧应用客户端发起以及 UE 侧使能客户端发起。以 EAS 发起的为例，应用上下文通过源和目标 EES 传递到目标应用服务器，从而使的目标应用服务器可以对 UE 进行认证和鉴权，保证应用切换过程中 UE 的业务连续性。

4.2.4.4 用户接入安全

用户接入安全是指对接入到运营商核心网络、边缘计算节点的终端进行身份识别，并根据事先确定的策略确定是否允许接入的过程。边缘计算节点面临海量异构终端接入，这些终端采用多样化的通信协议，且计算能力、架构都存在很大的差异性，如在工业边缘计算、企业和 IoT 边缘计算场景下，传感器与边缘计算节点之间众多不安全的通信协议（如 Zigbee、蓝牙等），缺少加密、认证等安全措施，易于被窃听和篡改，因此，应根据安全策略允许特定的设备接入网络、拒绝非法设备的接入。

此外，对于接入关键核心业务的终端，应考虑基于零信任理念进行动态持续的安全与信任评估，一旦发现安全与信任异常，应采取合适的管控。

4.2.5 应用安全

MEC 的应用可以分为运营商网元、运营商自己的增值业务、第三方垂直行业的业务等多种不同的业务类型，不同类型业务的安全要求和安全能力都不同，尤其是第三方垂直行业的应用，会给 MEC 环境引入比较大的安全风险，因此不同业务类型应用之间的隔离和之间互访过程中的安全监控是非常必要的。同时需要对 APP 做全生命周期的安全管理。

MEC 应用以虚拟化网络功能的方式部署在 NFV 基础设施上，当 MEC 应用以虚拟机或容器部署时，相应的虚拟化基础设施应支持 MEC 应用使用的虚拟 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进行隔离、APP 镜像和镜像仓库具有完整性和机密性、访问控制保护等，可参考虚拟层安全要求和容器安全要求。

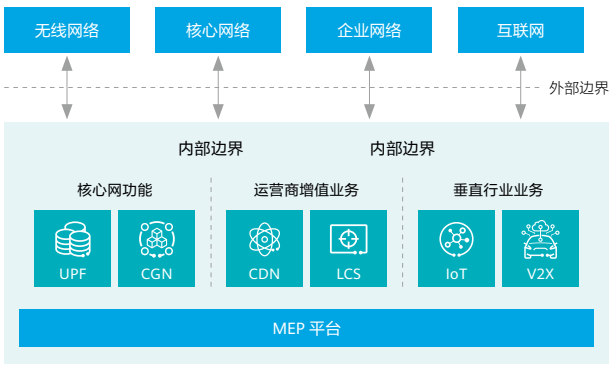

图 4-3 MEC 应用安全

4.2.6 能力开放安全

MEC 中边缘应用需要调用运营商网络的能力，如用户位置、QoS 等信息，实现业务价值。为了更好的为边缘应用提供服务，运营商网络支持网络能力向边缘应用开放。网络能力开放带来好处的同时也引入了新的安全威胁，应对 API 进行安全的管理、发布和开放。对作为 API 调用方的边缘应用进行认证和授权，从而保证边缘网络能力开放的安全性。目前，关于能力开放基于 3GPP SA2 组定义的 3GPP TS 23.222 [5] 为 API 服务调用定义的公共 API 框架（CAPIF）的关系模型，如下图 4-4 所示：

其中 CAPIF 提供者提供 CAPIF 核心功能，负责处理 API 调用者的请求和授权，并管理 API 提供者的服务 API 集合。

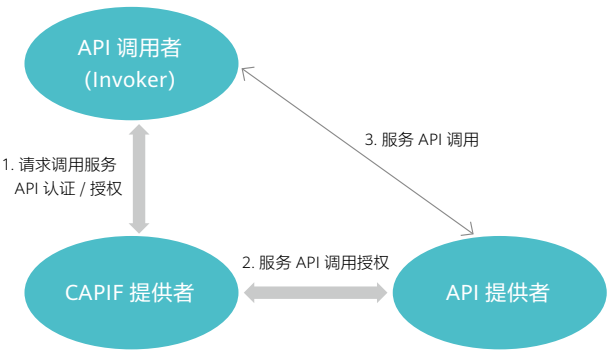

图 4-4 公共 API 框架（CAPIF）的关系模型

4.2.6.1 CAPIF 架构适配

针对 CAPIF 的部署方式不同，典型的映射有两种方式，一种是分布式，一种是集中式。对于分布式的映射，除了 PLMN 网络部署的 CAPIF core function，每个边缘数据网络部署有独立的 CAPIF core function，负责对应数据网络中 API 调用者的服务调用；对于集中式的映射，边缘数据网络的服务调用由 PLMN 中的 CAPIF core function 进行管理，不再单独部署分布式核心功能。

有了上述映射关系之后，MEC 场景下边缘计算服务器之间进行 API 调用，或者边缘计算服务器调用 3GPP 网络开放的北向 API 均可以复用 33.122 所定义的安全机制。

4.2.6.2 用户授权的能力开放

边缘应用服务器需要调用运营商网络的能力开放，其中涉及 UE 的敏感信息，如位置信息。这些信息需要获取用户同意，且用户需要完全掌握哪些应用可以以什么频率获取用户或用户设备的指定信息。例如，当核心网收到边缘应用的用户位置请求时，可以通过信令面向用户发送位置请求，在获取用户同意后，核心网才会将获取的用户位置信息返回给相应的边缘应用。

4.2.7 管理安全

边缘计算的特点是边缘节点规模小、数量多，安全的运行和管理需要考虑边缘侧资源受限，云边协同和安全功能编排与自动化响应等技术手段来保障边缘计算平台安全的服务化、智能化、协同化。

安全管理具体描述如下：

4.2.7.1 安全事件管理

实现 MEC 系统中安全事件可追溯，提高告警日志利用率，对安全事件进行预警。安全事件管理通过收集物理安全设备、虚拟安全设备、应用层安全设备相关告警日志，上报至态势感知系统进行分析，进行安全预警；同时将告警信息进行归档，方便后续日志追溯。

4.2.7.2 用户行为管理

实现人员操作行为可追溯，预警人为操作所产生的风险。针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程。通过统一接入门户对宿主机、虚拟机、云管理平台、MEC 管理平

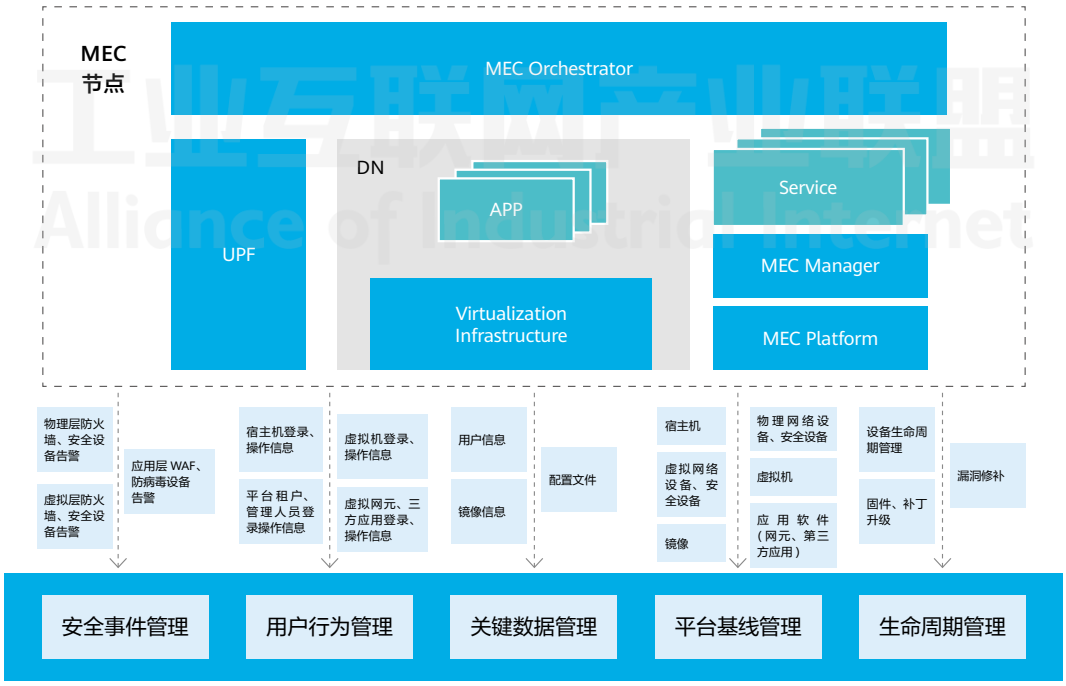

图 4-5 管理安全框架

台以及虚拟网元、第三方应用的用户进行统一管理。记录其登录登出以及相关的命令操作，通过 UEBA 技术绘制用户行为肖像并生成相应安全策略。当用户出现异常操作时，发生告警并阻止相关操作。

4.2.7.3 关键数据管理

实现关键数据流转路径可追溯，防止数据泄露。对用户信息、配置信息、镜像信息、软件包等关键数据的流转进行记录，形成数据流转路径。当发生数据泄露事件时，为事件追溯提供证据。

4.2.7.4 平台基线管理

保证 MEP 平台的可靠性和安全防护能力。通过对宿主机、虚拟机、物理网络设备、虚拟网络设备、镜像、应用软件包（网元、第三方应用）进行基线核查，确保平台本身以及上层应用的安全性，减少安全风险，提高安全防护水平。

4.2.7.5 生命周期管理

对接入到 MEC 的设备进行生命周期管理，定期远程更新所有边缘设备和节点，维护管理补丁升级和固件升级，及时修补漏洞。如果不能及时更新最新的补丁或升级边缘设备或终端传感器固件，随着每天发生新的复杂的攻击，会带来很大的风险。设备商应该具备可持续的漏洞系统治理与应急响应能力，包括：

» 建立针对安全漏洞事件端到端的治理、响应与支撑组织。
» 建立全面的漏洞感知渠道与分析体系，确保快速精准追溯。
» 定义符合行业惯例和客户需要的漏洞修补基线，支持快速修补与部署。
» 提供及时、公开、透明的安全漏洞披露策略与渠道，确保客户具备同等知情权，支撑下游客户决策处置。
» 构建工程体系能力，确保过程可视可追溯，漏洞敏感信息安全受控。
» 建立针对组织、员工的培养体系。

4.2.7.6 构建态势感知能力

通过统一的安全态势感知、协同防御能力建设，实现边云协同态势感知。应用于中心云入侵检测技术也可以应用于边缘节点，对恶意软件、恶意攻击等行为进行检测。此外，对于边缘分布式的特点，可以通过相应的分布式边缘入侵检测技术来进行识别，在中心云管理面进行安全态势感知呈现。

相比中心侧，边缘场景由于其部署位置更下沉，提供开放能力，且可用资源更受限等特点，无法部署重量级的防御能力，边缘场景将面临更大的安全威胁。为了解决这个问题，利用“白名单 / 规则 /AI 算法”等技术，结合边缘网元自身的业务特点，构建边缘场景内置的轻量化安全态势感知能力，实现威胁检测的高性能和高检出率。

凭借边缘场景内置的轻量化安全态势感知能力，能够实现设备接入前的安全配置核查，系统加固，以减少系统自身的脆弱点；能够实现平台运行时的实时入侵检测 / 定时配置核查加固，及时发现网络被攻击 / 系统配置被篡改的异常行为，快速响应，降低不良影响。

MEC 的编排管理系统架构与 NFV 的编排和管理系统类似。从 ETSI MEC 系统参考架构（图 3-1）中可以看出，MEC 的编排管理系统包括 MEO、MEPM 两部分，南向接口面向 VIM 和 MEP，北向接口面向运营商的 OSS 系统。OSS、MEO、MEPM 之间的接口都属于 API 调用，并不直接面向用户和互联网，除应做好严格的访问控制外，还可部署 API 网关对 API 的调用进行安全管控。

边缘计算系统的管理维护接口应支持对接入者的身份认证，并在身份认证成功后，使用安全的传输协议保护通信内容的机密性和完整性。

4.2.8 数据安全

在边缘计算环境下，由于边缘计算服务模式的复杂性、实时性，数据的多源异构性、感知性以及终端资源受限特性，传统环境下的数据安全和隐私保护机制不再适用于边缘设备产生的海量数据防护，亟待新的边缘数据安全治理理念，提供轻量级数据加密、数据安全存储、敏感数据处理和敏感数据监测等关键技术能力，保障数据的产生、采集、流转、存储、处理、使用、分享、销毁等环节的全生命周期安全，涵盖对数据完整性、保密性和可用性。

广域 MEC 和局域 MEC 场景下，数据在边缘节点存储以及在复杂异构的边缘网络环境中传输的安全性需要得到保障。对于存储的大量数据，需要识别出保障业务运行的重要数据并进行安全备份和恢复，避免因数据损毁导致正常业务无法进行。此外，应提供异地备份功能，可通过通信网络将重要数据备份到异地，支持备份数据一致性检验、备份位置查询等功能。

面对边缘计算用户隐私数据泄露的安全风险，除了可以采用轻量级加密、隐私保护数据聚合、基于差分隐私的数据保护、联合机器学习隐私保护等技术手段外，在进行数据信息的路由转发时，还可以根据数据信息的类型进行分类管理。将涉及用户隐私的数据信息加以标识，在每个 MEC 节点的数据入口通过防火墙进行隔离，按照最小化原则关掉所有不必要的服务及端口，对于增加标识的重要数据进行完整性、机密性及防复制的保护。另外，针对开放 API 接口的隐私数据泄露问题，可以将云计算服务中心的入侵检测技术应用于 MEC 节点，对 API 接口的使用者进行检测，防止攻击者获取用户的隐私数据信息；针对 MEC 节点部署分散的问题，可以采用分布式入侵检测技术，通过多个 MEC 节点之间进行协作，以自组织的方式实现对恶意攻击的检测 [3]。

数据脱敏要求对用户数据中的隐私（含：身份信息、位置信息和私密数据等关联到个人的数据）和身份（含：用户所知、用户拥有（如智能卡）、用户具有（如生物特征等））进行保护，以加密（含：对称加密、非对称加密等）或脱敏（含：匿名或假名等）等主流数据安全技术，并且加强存储以防数据丢失，保障用户数据的机密性和完整性。边缘计算应支持对接入设备使用用户准入机制，同时支持 VPN 的安全接入隧道，并对用户的数据加密，来确保安全的接入设备。尤其在企业园区的应用场景中，可将用户的接入授权与企业内部的授权服务器对接，实现用户接入授权。

05 5G 边缘计算安全案例

5.1 智能电网

5.1.1 智能电网概述

广域 MEC 场景可以不限定地理区域，通常可基于运营商的端到端公网资源，通过网络切片等方式实现不同行业不同业务的安全承载，主要应用场景包括交通、电力、车联网以及跨域经营的特大型企业等。

以智能电网为例，MEC 的部署方式，在满足业务时延和隔离的基础上，主要考虑与电力业务的流向进行匹配，避免流量迂回。根据电网业务特点匹配，采取省、地、区三级部署方式（即汇聚及汇聚以上部署），其中省、地作为规模推广方式。因此，智能电网是广域 MEC 安全典型场景。

省级：主要针对省集中业务（主站在分子公司），UPF 在省公司层面部署，卸载省集中的业务流量，如计量、公车监控等。

地级：主要针对地市终结业务（主站在地市局），UPF 地市集中部署，卸载本市流量，如配网自动化三遥、配网差动保护、精准负控、PMU、配变监测、智能配电房、输电线路在线监测、充电桩等。

区县级（暂不作规模推广）：特大型城市、变电站 / 换流站、抽水蓄能电厂等大型封闭区域。主要针对变电站高要求场景，既要保障安全性，又有本地卸载逐级分流监控的需求，可采用 UPF+MEC 按需下沉至变电站或区县级：如变电站巡检机器人、状态检测、视频监控等。

5.1.2 智能电网安全

电网安全是涉及国计民生的大事，因此智能电网作为广域 MEC 的典型场景，对安全有严格的要求。电网安全隔离需求主要依据来源是《电力监控系统安全防护规定》（国家发改委 2014 年第 14 号）、《国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》（国能安全 [2015]36 号文）。根据国能安全 [2015]36 号文，电力业务的安全总体原则为安全分区、网络专用、横向隔离、纵向认证。

5.1.2.1 安全分区

电网业务主要分为生产控制大区、管理信息大区两大类。

1、对于生产控制大区，包含了生产控制和生产非控制两大类业务。其中生产控制类包括配网自动化实现配网差动保护、配网广域同步向量测量 PMU 和配网自动化三遥业务等。生产非控制类主要是计量业务，实现电能 / 电压质量监测、工厂 / 园区 / 楼宇智慧用电等。

生产控制大区业务的共性特征在于点多面广，需要全程全域全覆盖，属于广域场景，要求 5G 网络提供高安全隔离、低时延、高频转发、高精授时等能力，用户面 UPF 接入电力生产控制大区的专用 MEC。

2、对于管理信息大区，包含了管理区视频类和局域专网两大类业务。

» 管理区视频类包括利用机器人和无人机进行变电站和线路巡检、摄像头监控等，属于广域场景，要求用户面 UPF 接入电力管理信息大区专用 MEC。

» 局域专网类实现智慧园区、智能变电站等局域场景电力业务，其特征在于特定区域有限覆盖，属于典型的局域专网场景，要求 5G 网络提供上行大带宽、数据本地化处理等能力，其用户面 UPF 接入电力管理信息大区专用 MEC；后续根据业务需求，推荐用户面进一步下沉在电力园区部署小型化 MEC，进一步满足数据不出场站的安全需求。

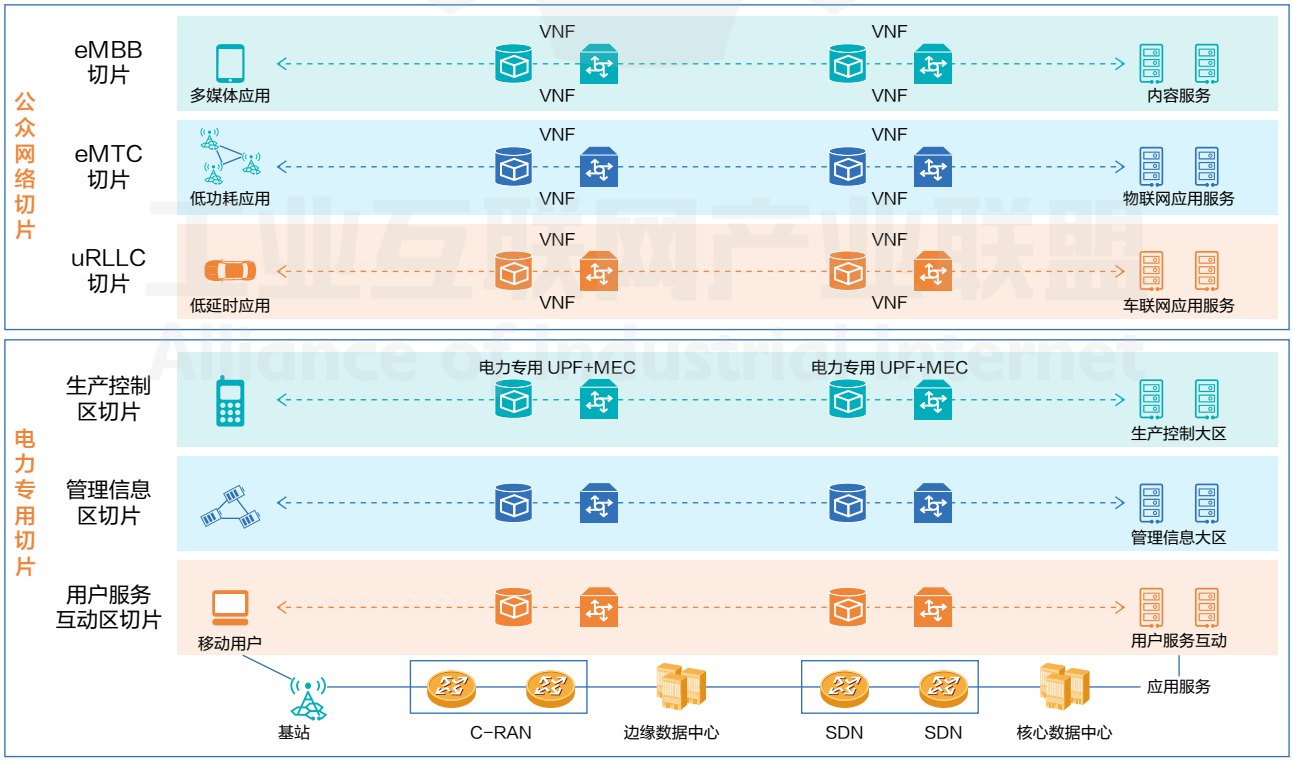

图 5-1 5G 电力虚拟专网总体框架

5.1.2.2 网络专用

» 生产控制大区业务需与其他业务进行物理隔离。对于个别生产控制大区业务，在使用无线公网、无线通信网络及处于非可控状态下的网络设备和终端进行通信，其安全防护水平低于生产控制大区内的其他系统时，应设立安全接入区，并采用安全隔离、访问控制、认证及加密等措施。典型业务如配网自动化、负荷管控管理系统、分布式能源调控系统。

» 各大区内部不同业务之间需进行逻辑隔离：可以采用 MPLS-VPN 技术、安全隧道技术、PVC 技术、静态路由等构造子网，进行逻辑隔离。

5.1.2.3 横向隔离

横向隔离主要体现在不同分区主站系统之间的隔离。

» 生产控制大区与管理信息大区之间：必须设置国家指定部门检测认证的电力横向单向安全隔离装置，隔离强度应当接近或达到物理隔离。

» 生产控制大区内部：不同业务之间采用具有访问控制功能的网络设备、防火墙等实现逻辑隔离。

» 安全接入区域生产控制大区相连时，应采用电力专用横向单向安全隔离装置进行集中互联。

传统网络承载电力业务时，包括电力专网和公网两大类，专网的物理层主要通过不同波长、时隙、物理纤芯等资源实现物理隔离，逻辑层主要通过 VLAN、VPN 等手段实现逻辑隔离。对于公网，生产控制类业务需接入安全接入区，管理信息类需接入防火墙。

5G 与传统网络承载电力业务的整体差异

	传统网络		5G	
	生产	管理	生产	管理
专网物理层	采用不同波长、分时、物理纤芯等		切片（空口时、频、空正交、传输引入时分，核心网独立服务器）	
专网逻辑层	采用 VLAN、VPN 等		切片（VLAN、IP 隧道、虚拟机）	
公网	安全接入区	防火墙	安全接入区	防火墙

图 5-2 5G 与传统网络承载的区别

相比较传统网络，采用 5G 公网承载电力业务时，引入了全新的端到端网络切片隔离方案。通过 MEC+ 切片，5G 在技术上具备了为业务提供端到端物理隔离和逻辑隔离的能力。在物理隔离层面，无线空口侧采用时、频、空域正交资源块 RB 传输数据，传送网侧引入了基于 FlexE 技术的硬隔离方式，使得传送网具备类似于 TDM 独占时隙，业务可实现基于时分的网络切割，不同 FlexE 切片之间业务互不影响，核心网侧利用网络功能虚拟化方式为电网分配独立的物理服务器资源。上述从无线空口 -> 基站 -> 传送网 -> 核心网的端到端切片技术，为电力行业在物理资源层面上隔离出了一张“无线专网”，满足电网业务的安全性、可靠性需求。在逻辑隔离层面，5G 网络切片仍然采用 VLAN、IP 隧道、VPN 虚拟机等方式进行业务逻辑隔离。

5.1.2.4 纵向认证

根据 5G 的通信机制，电网业务在开卡时，预先分配好 DNN（类比公网 APN）、网络切片标识（NSSAI）等属性，业务上线时，终端首先附着 5G 网络，在附着的过程中，完成 5G AKA 主鉴权，核心网将根据事先分配的 DNN、NSSAI 等签约属性，分配对应的 SMF 和 UPF，建立 PDU 会话连接。5G 通信机制要求用户数据必须先经过 UPF 再进行转发，从而实现了从终端至基站至 UPF 的传输隧道，且不暴露在公网上，保障了用户通信数据安全。

但是对于重点防护的调度中心、发电厂、变电站，由于其数据的高度敏感性，应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关及相关设施，实现双向身份认证、数据加密和访问控制。纵向加密认证装置为广域网通信提供认证与加密功能，实现数据传输的机密性、完整性保护，同时具有安全过滤功能。加密认证网关除具有加密认证装置的全部功能外，还应实现电力系统数据通信应用层协议及报文的处理。

5.2 智慧工厂

5.2.1 智慧工厂概述

智慧工厂是局域 MEC 典型场景，局域 MEC 场景一般适用于业务限定在特定地理区域，为基于特定区域的 5G 网络实现业务闭环，保障行业核心业务数据不出园区的需求，主要应用场景包括制造、钢铁、石化、港口、教育、医疗等园区 / 厂区型企业。以制造行业为例，传统制造工厂里面主要通过有线网络、WiFi、4G 以及近距离无线等几种技术实现联网，都存在一定的弊端，有线网络部署周期较长、部署难度较大，WiFi 稳定性不够、易受干扰，4G 的带宽不足、时延偏大，蓝牙、RFID 等近距离无线技术传输数据量太小、距离受限，迫切需要一种具备综合优势的网络技术。

5G 网络具有大带宽、低时延的特性，稳定可靠，智慧工厂生产制造过程中的需求与 5G 技术较契合。本案例是在智慧工厂实现基于 5G 的业务应用，包括在产品设备试验制造过程中的远程监控、可视化及远程指导和理化检验高速协同。整体项目涵盖设备的零部件材料检验、组件装配AR辅助、设备试车过程中的状态问题监控分析、试车过程中发现问题后的远程 AR 维护指导，初步实现设备试验制造的全流程管理，解决企业安全生产，提高研究和生产效率。

为满足上述场景的业务需求，本案例网络由以下几个部分组成：5G 终端，5G 基站、5G 承载网和 5G 核心网。同时通过部署 MEC 本地分流的方式实现了用户对本地网络资源低时延、高带宽的接入访问，并实现数据不出厂区。本案例设备均遵从国际 3GPP 协议规范，并满足 99.999% 以上的电信级可靠性。

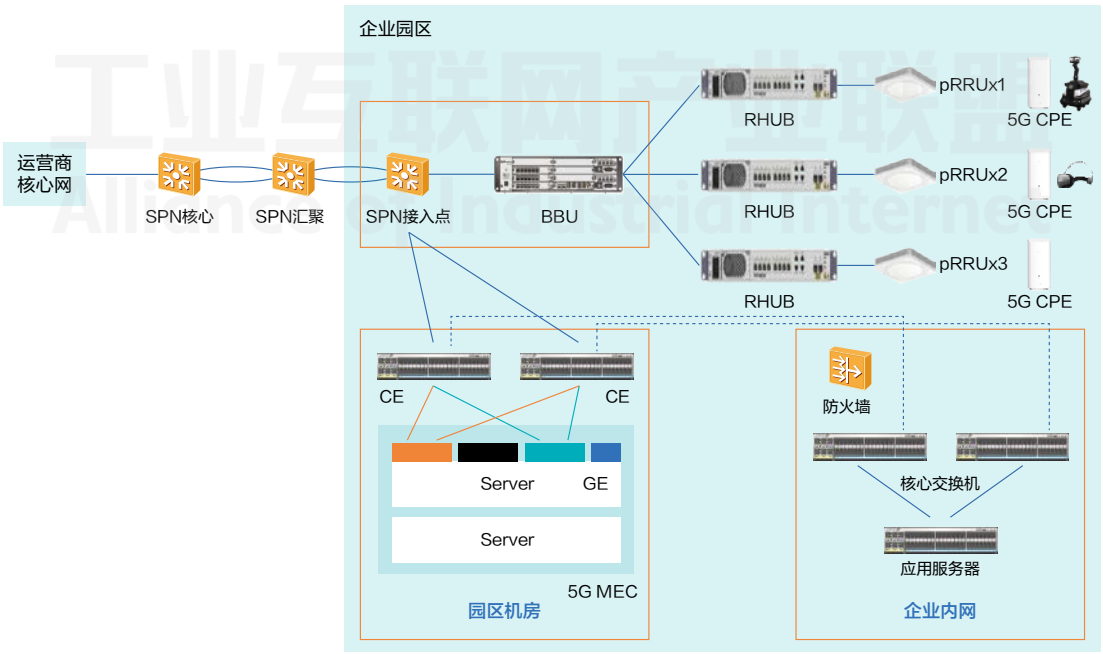

图 5-3 智慧工厂 MEC 网络架构图

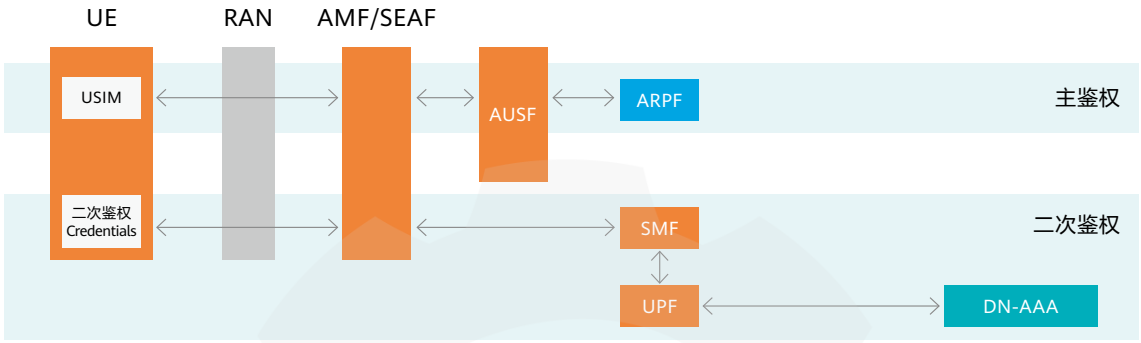

图 5-4 用户鉴权图

5.2.2 智慧工厂安全

本案例整体设计以等保三级安全要求为基础，结合工厂数据不出园核心诉求，从终端接入安全、通信网络机密性和完整性保护、企业网络边界隔离、安全管理和审计方面，提供智慧工厂 5G 网络安全方案。

5.2.2.1 终端接入安全

插有 SIM 卡的 CPE 终端首先向 5G 网络发起注册流程，通过 5G 基站和 5G 承载网向 5G 核心网控制面发起注册鉴权流程。该鉴权流程对用户的 SIM 卡身份合法性进行认证（5G AKA 双向鉴权标准），防止非法用户接入 5G 网络。

SIM 卡的鉴权能力由运营商提供，企业为了自行对行业终端进行认证和管理，可部署企业 AAA 服务对终端设备二次鉴权，确保合法用户及合法终端才能访问相应的园区网络。

以一个员工进入园区上班为例，主鉴权相当于要出示员工的身份证，证明员工可以进入企业园区，二次鉴权则要出示员工的企业工卡，同时还要做到人证合一，甚至还可以进一步证明员工具备进入园区的某个区域的权利。

5.2.2.2 通信网络机密性和完整性保护

1、通过 5G 空口安全和传输安全机制，实现 5G 网络端到端分段机密性和完整性保护。

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

机密性：5G 网络通过对空口信令和用户数据开启加密保护（其中用户的鉴权信息通过信令数据交互），将用户数据转换为密文数据，保证数据不被泄露，并且支持 128 位加密算法。

完整性：5G 网络支持信令消息和用户面数据提供完整性保护，5G 终端和 5G 基站通过完整性算法，确保信令消息和用户面数据不被非法篡改。

» 传输安全是指基站到 UPF 及 UPF 到企业内网的机密性和完整性。运营商及企业可以部署 IPSec 实现传输网络的机密性和完整性保护。

2、企业自主部署终端和边界安全网关的安全能力，实现应用层的通信链路安全。

» 创建本地透传的专用隧道。在保障 5G 网络端到端分段机密性和完整性保护的基础上，5G 终端还要完成 DNN（Data Network Name）签约，核心网控制面根据用户签约的 DNN 选择对应的用户面网元 UPF，UPF 和基站建立承载该用户的上下行专用隧道，确保终端用户数据只在园区 5G 基站、园区 UPF 和园区内部网络之间流转，形成一个本地透传的专用管道，达到数据不出园区的目的。

» 应用层端到端加密和完整性机制。本案例提供的工业级 CPE 支持 IPSEC 加密能力，后续还可通过支持 IPSec 的 5G 模组，结合企业内部网络边界部署的安全网关（防火墙内置安全网关），实现用户终端和安全网关之间的 IPSec 加密和完整性保护，该端到端安全通信链路不依赖于运营商 5G 网络的安全能力。

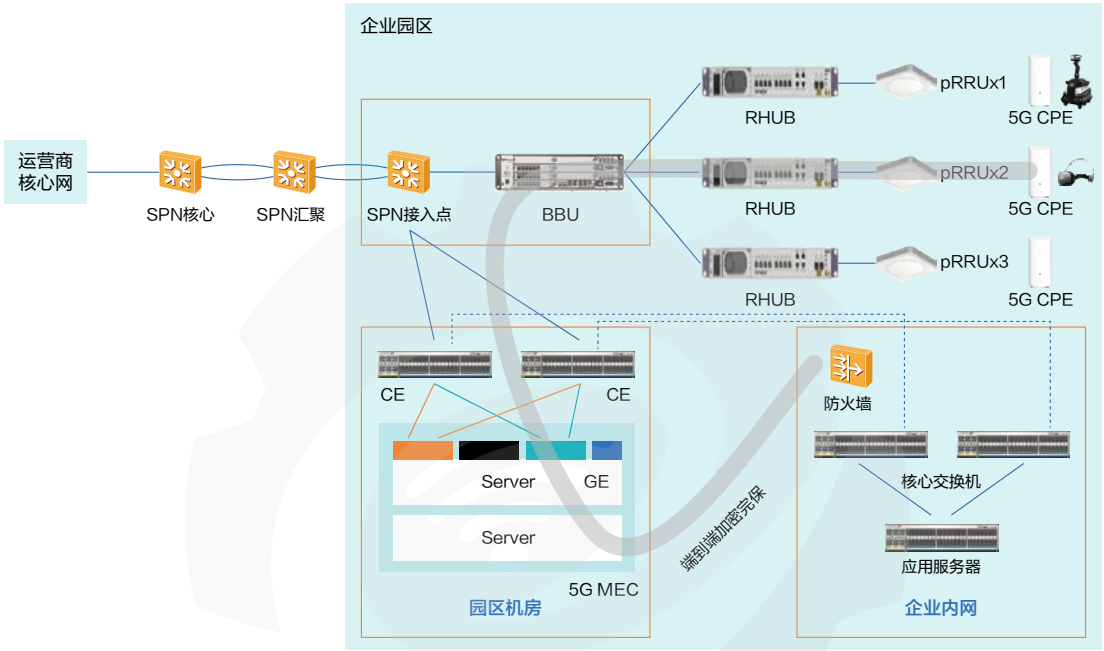

图 5-5 端到端加密完保

5.2.2.3 企业网络边界隔离

5G 网络和企业安全边界隔离：在 UPF 接入到企业内部网络的核心交换机之间部署防火墙，确保两个网络边界隔离安全。防火墙提供精细化访问控制策略缩小攻击面，并支持流量行为分析能力，及恶意软件检测能力。

防火墙安全策略采用最小授权方式，入防火墙的流量进入 Untrust 域，安全策略基于协议配置，只容许 IKE 和 IPSec 流量通过。出防火墙的流量从 Trust 域转发，目的地址为制定的 5G 终端连接服务器 IP+Port。这样可以确保攻击面最小，访问权限精细化防御。

防火墙配置更改，安全策略阻断，异常流量阻断等都会生成日志（Syslog 形式），并且发送给安全管理中心日志服务呈现，作为合规和审计的数据。

防火墙提供既有只读权限的 UI 接口，可以读取配置、查看历史丢包记录，进行初级安全故障处理。

5.2.2.4 安全管理和审计

通过已经部署在安全管理中心的日志审计系统，可以集中采集边界防火墙中的系统安全事件、用户访问记录、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，实现对信息系统日志的全面审计，同时可以帮助管理员进行故障快速定位，并提供客观依据进行追查和恢复。

06 未来展望

边缘计算是计算能力在网络支持下向边缘侧延伸的新形态，涉及网络、边缘云及边缘应用，其本质是实现拉近距离降时延、本地计算省带宽、数据隔离保安全、算力卸载降成本。5G 原生支持边缘计算，边缘计算已成为提升新业务端到端用户体验的有效手段。

未来，要构建安全的 5G 边缘计算“环境”，着眼全局、构建统一的 5G 标准和认证体系，着眼基线、落实 5G 安全基线要求，着眼应用、以安全评估促进端到端安全，着眼长远、循序渐进提升网络安全水平。

附录 1
缩略语

序号	缩略语	英文名称	中文名称
1	AI	Artificial Intelligence	人工智能
2	AKA	Authentication and Key Agreement	认证和密钥协商
3	API	Application Programming Interface	应用程序接口
4	CAG	Closed Access Group	封闭接入组
5	CAPIF	Common API Framework	公共 API 框架
6	DDoS	Distributed denial of service attack	分布式拒绝服务攻击
7	EAS	Edge Application Server	边缘应用服务器
8	EES	Edge Enabler Server	边缘使能服务器
9	MEC	Multi-Access Edge Computing	多接入边缘计算
10	MEP	MEC Platform	MEP 平台
11	NID	Network Identifier	网络识别码
12	RAN	Radio Access Network	无线接入网
13	SMF	Session Management Function	会话管理模块
14	TPM	Trusted Platform Module	可信平台模块
15	UEBA	User and Entity Behavior Analytics	用户行为分析
16	UPF	User Plane Function	用户面功能
17	VM	Virtual Machine	虚拟机

附录 2

参考文献

[1] AII- 边缘计算安全白皮书，工业互联网产业联盟，2019.11.

[2] 3GPP TS 33.501. Security Architecture and Procedures for 5G System[S], 3GPP.

[3] 5G-ENSURE_D2.7 Security Architecture[R], 5GPPP.

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

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

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

[7] 5G empowering vertical industries，欧盟 5G PPP.


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