



# 中华人民共和国公共安全行业标准

GA/T 1390.6—2025

## 信息安全技术 网络安全等级保护基本要求 第6部分：边缘计算安全扩展要求

Information security technology—Baseline for classified protection of cyber security—Part 6: Extended requirements for edge computing security

2025-10-13发布

2026-02-01实施

中华人民共和国公安部 发布

目次

前言 .....Ⅲ

引言 .....Ⅳ

1 范围 .....1

2 规范性引用文件 .....1

3 术语和定义 .....1

4 缩略语 .....2

5 采用5G技术的边缘计算等级保护对象概述.....3

6 第一级安全扩展要求 .....3

7 第二级安全扩展要求 .....4

8 第三级安全扩展要求 .....5

9 第四级安全扩展要求 .....8

10 第五级安全扩展要求 .....11

附录A(资料性) 基于5G技术边缘计算等级保护对象的应用场景和架构 .....12

附录B(资料性) 基于5G技术边缘计算等级保护对象的局域网应用场景与架构 .....13

附录C(资料性) 基于5G技术边缘计算等级保护对象的广域网应用场景与架构 .....14

参考文献 .....16

## 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GA/T 1390《信息安全技术 网络安全等级保护基本要求》的第 6 部分。GA/T 1390 已经发布了以下部分：

- 第 2 部分：云计算安全扩展要求；
- 第 3 部分：移动互联安全扩展要求；
- 第 5 部分：工业控制系统安全扩展要求；
- 第 6 部分：边缘计算安全扩展要求；
- 第 7 部分：大数据系统安全扩展要求；
- 第 8 部分：IPv6 网络安全扩展要求；
- 第 9 部分：区块链安全扩展要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由公安部网络安全保卫局提出。

本文件由公安部信息系统安全标准化技术委员会归口。

本文件起草单位：公安部第三研究所、公安部网络安全保卫局、中国移动通信有限公司研究院、西安电子科技大学、华为技术有限公司、中国电信股份有限公司、北方实验室(沈阳)股份有限公司。

本文件主要起草人：陶源、刘秀龙、李末岩、任娟娟、何余、方煦譔、黄敏、杨凯、游志勇、曹进、郑献春、沈雪丽、李海涛。

# 引 言

GA/T 1390《信息安全技术 网络安全等级保护基本要求》旨在提出不同网络安全保护等级的基线安全要求,指导等级保护对象的安全建设和监督管理。GA/T 1390 拟由以下部分组成。

- 第 1 部分:安全通用要求。旨在提出适用于所有网络安全等级保护对象的安全基线要求。
- 第 2 部分:云计算安全扩展要求。旨在提出适用于云计算平台/系统的安全扩展要求。
- 第 3 部分:移动互联安全扩展要求。旨在提出适用于采用移动互联技术的等级保护对象的安全扩展要求。
- 第 4 部分:物联网安全扩展要求。旨在提出适用于物联网的安全扩展要求。
- 第 5 部分:工业控制系统安全扩展要求。旨在提出适用于工业控制系统的安全扩展要求。
- 第 6 部分:边缘计算安全扩展要求。旨在提出适用于采用边缘计算技术的等级保护对象的安全扩展要求。
- 第 7 部分:大数据系统安全扩展要求。旨在提出适用于采用大数据技术的等级保护对象的安全扩展要求。
- 第 8 部分:IPv6 网络安全扩展要求。旨在提出适用于 IPv6 等级保护对象的安全扩展要求。
- 第 9 部分:区块链安全扩展要求。旨在提出适用于区块链等级保护对象的安全扩展要求。
- 第 10 部分:生成式人工智能安全扩展要求。旨在提出适用于生成式人工智能等级保护对象的安全扩展要求。
- 第 11 部分:低空智联网安全扩展要求。旨在提出适用于低空智联网等级保护对象的安全扩展要求。
- 第 12 部分:智能车联网安全扩展要求。旨在提出适用于智能车联网等级保护对象的安全扩展要求。

信息安全技术 网络安全等级保护基本要求 第6部分:边缘计算安全扩展要求

1 范围

本文件规定了采用 5G 技术的边缘计算网络系统(不含运营商核心网)的第一级到第四级的安全扩展要求。

本文件适用于采用 5G 技术的边缘计算等级保护对象的安全建设和监督管理。

注:采用 5G 技术的边缘计算网络系统(不含运营商核心网)的第五级安全测评不在本文件中进行描述。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 22240 信息安全技术 网络安全等级保护定级指南
- GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求
- GB/T 25058 信息安全技术 网络安全等级保护实施指南
- GB/T 36958 信息安全技术 网络安全等级保护安全管理中心技术要求

3 术语和定义

GB/T 22239、GB/T 22240、GB/T 25070、GB/T 25058 和 GB/T 36958 界定的以及下列术语和定义适用于本文件。

3.1

**边缘计算 edge computing**

在边缘或边缘附近进行数据处理与存储的分布式计算形式。

[来源:GB/T 42564—2023,3.2]

3.2

**多接入边缘计算 multi-access edge computing**

包含一种或多种类型的接入技术的边缘计算系统。

[来源:ETSI GS MEC 001 V2.1.1,3.1,有修改]

3.3

**园区 park**

业务运营的实体区域。

3.4

**MEC 平台 multi-access edge computing platform**

提供多接入边缘计算的所有相关软硬件资源。

3.5

**边缘应用 edge computing application**

部署并运行在边缘节点上的应用程序,在边缘实现对数据的本地处理和业务逻辑的本地执行。

[来源:GB/T 42564—2023,3.8]

3.6

**5G 5th generation**

符合第五代 3GPP 规范的电信系统。

注:由 5G 核心网、5G 接入网和用户设备组成。

[来源:3GPP TR 21.905 V17.1.0,4.1,有修改]

3.7

**5G 专网 5G private network**

采用 3GPP 5G 标准构建的不与公共网络交互的隔离网络。

[来源:3GPP TS 22.261 V19.4.0,3.1,有修改]

3.8

**网络切片 network slice**

在共享基础设施上构建的提供特定网络能力和网络特征的专用网络。

[来源:3GPP TS 23.501 V18.3.0,3.1,有修改]

3.9

**用户面功能 user plane function**

提供用户面数据转发、处理的网络功能,负责与外部数据网络互连,分组路由转发,数据包检测和用户面策略执行等。

3.10

**会话管理功能 session management function**

负责会话建立、修改和释放,IP 地址分配和管理,UPF 设备选择的网络功能。

3.11

**空口 air interface**

用户终端设备与基站之间的无线传输接口。

4 缩略语

下列缩略语适用于本文件。

5G-GUTI:5G 全局唯一临时标识(5G Globally Unique Temporary Identifier)

DDoS:分布式拒绝服务(Distributed Denial of Service)

GPS:全球卫星定位系统(Global Positioning System)

GUTI:全球唯一临时标识符(Globally Unique Temporary Identifier)

MEC:多接入边缘计算(Multi-access Edge Computing)

SMF:会话管理功能(Session Management Function)

SUCI:用户隐藏标识符(Subscription Concealed Identifier)

SUPI:用户永久标识符(Subscription Identifier)

UE:用户终端设备(User Equipment)

UPF:用户面功能(User Plane Function)



## 5 采用5G技术的边缘计算等级保护对象概述

本文件用于明确采用5G技术的边缘计算网络系统(不含运营商核心网)的安全扩展要求,主要针对5G用户终端设备、无线接入设备、边缘设备 and 应用服务器区部分(不含运营商核心网)提出特殊安全要求,用于支撑 GB/T 22239—2019 指导采用5G技术的边缘计算等级保护对象(第一级到第四级)的安全建设和监督管理。

采用5G技术的边缘计算等级保护对象由5G用户终端设备、无线接入设备、边缘设备和应用服务器区四部分组成(见图1),基于5G技术边缘计算等级保护对象的应用场景和架构见附录A,基于5G技术边缘计算等级保护对象的局域网应用场景与架构见附录B,基于5G技术边缘计算等级保护对象的广域网应用场景与架构见附录C。

在图1中,Uu接口指5G用户终端设备与5G基站之间的空口,N3接口指5G基站与UPF设备之间的数据接口,N4接口指SMF设备与UPF设备之间的信令接口,N9接口指UPF设备与UPF设备之间的数据接口,N6接口指UPF设备与应用服务器区之间的数据接口。5G用户终端设备通过Uu接口接入无线接入设备。无线接入设备负责用户面和控制面数据的空口传输,并通过N3接口与边缘设备连接。

边缘设备为UPF设备,负责用户面数据的转发,通过就近或园区内部署,满足低时延和数据不出园区的要求。UPF设备通过N4接口与运营商核心网SMF设备连接,并由SMF设备向UPF设备发送控制面信令,控制用户面会话建立、更新和撤销。UPF设备通过N6接口与应用服务器区的5G行业应用平台/系统或MEC平台交互用户面数据。

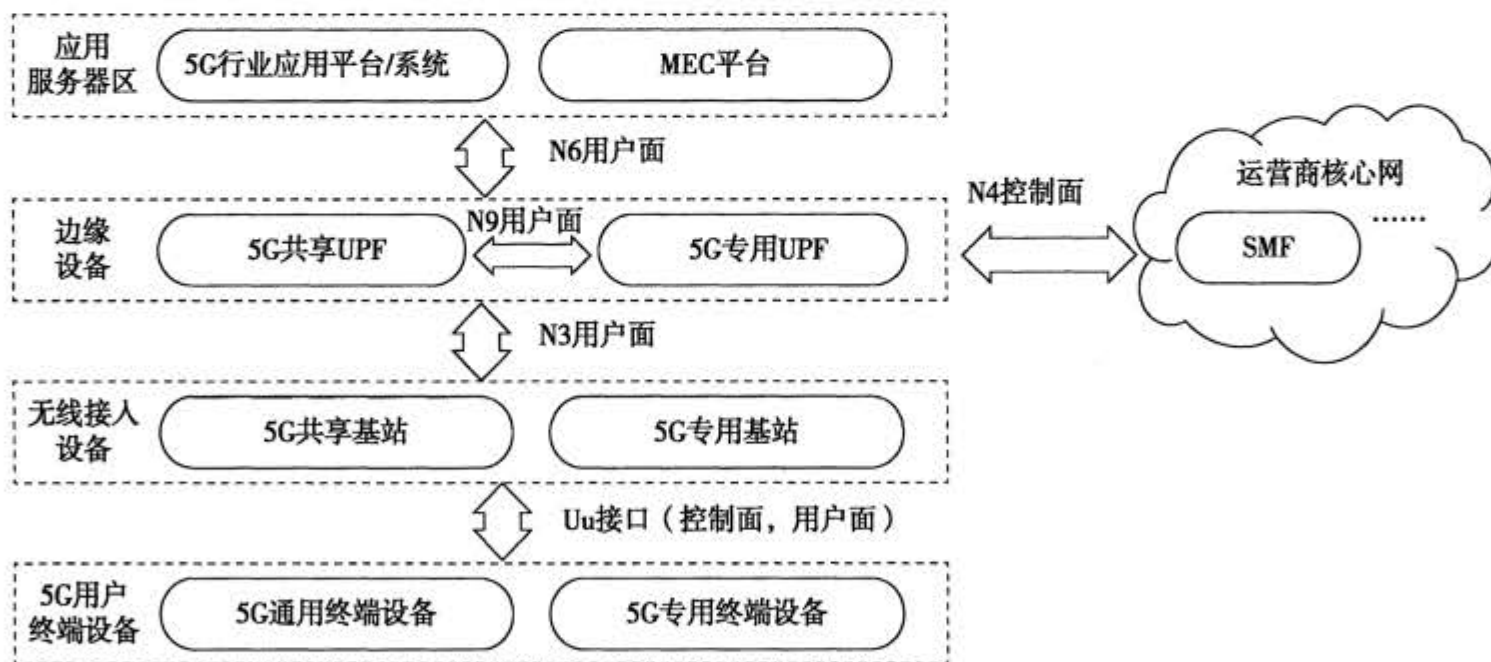


图1 采用5G技术的边缘计算等级保护对象示意图

## 6 第一级安全扩展要求

### 6.1 安全通信网络

应将由电信运营商或其他外部单位运营维护的5G基站、UPF设备、MEC平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段。

### 6.2 安全建设管理

应选择具有基础电信业务经营资质的5G电信运营商,其所提供的5G网络应为所承载的业务应用

系统及数据传输业务提供不低于其安全保护等级的安全保护能力。

### 6.3 安全运维管理

应具有使用 5G-GUTI 替代 SUPI 的能力,实现 5G 用户信息的隐私保护。

## 7 第二级安全扩展要求

### 7.1 安全物理环境

在业务数据不出园区的场景下,应将 5G 基站、UPF 设备和 5G 用户终端设备部署在园区内。

### 7.2 安全通信网络

安全通信网络架构应满足以下要求:

- a) 5G 行业应用系统不运行在低于其安全保护等级的 5G 网络上;
- b) 将由电信运营商或其他外部单位运营维护的 5G 基站、UPF 设备、MEC 平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段;
- c) 网络通信设备不包含其供应商、生产商或开发人员不再支持的软件和硬件组件,例如已达到生命周期或不再支持的组件。

### 7.3 安全区域边界

#### 7.3.1 边界防护

5G 网络 N6 接口与应用服务器网络之间的访问和数据流应通过边界网关设备,并设置访问控制规则。

#### 7.3.2 访问控制

5G 用户终端设备应开启接入认证功能。

#### 7.3.3 入侵防范

边缘应用应具有安全防御能力。

### 7.4 安全计算环境

应提供 MEC 平台用户设置其所属的不同虚拟机之间的访问控制策略的功能。

### 7.5 安全建设管理

#### 7.5.1 电信运营商选择

应选择具有基础电信业务经营资质的 5G 电信运营商,其所提供的 5G 网络应为所承载的业务应用系统及数据传输业务提供不低于其安全保护等级的安全保护能力。

#### 7.5.2 应用软件采购

应用软件采购应满足以下要求:

- a) 5G 用户终端设备、MEC 平台等安装、运行的应用软件来自可靠分发渠道或使用数字签名;
- b) 网络通信设备的产品及服务符合国家标准、行业标准。



## 7.6 安全运维管理

### 7.6.1 5G 用户终端设备管理

应指定人员定期巡视 5G 用户终端设备的部署环境,对可能影响设备正常工作的环境异常进行记录和维护。

### 7.6.2 隐私管理

应具有使用 5G-GUTI 替代 SUPI 的能力,实现 5G 用户信息的隐私保护。

## 8 第三级安全扩展要求

### 8.1 安全物理环境

在业务数据不出园区的场景下,应将 5G 基站、UPF 设备和 5G 用户终端设备部署在园区内。

### 8.2 安全通信网络

#### 8.2.1 网络架构

网络架构应满足以下要求:

- a) 5G 行业应用系统不运行在低于其安全保护等级的 5G 网络上;
- b) 将由电信运营商或其他外部单位运营维护的 5G 基站、UPF 设备、MEC 平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段;
- c) 网络通信设备不包含其供应商、生产商或开发人员不再支持的软件和硬件组件,例如已达到生命周期或不再支持的组件;
- d) 网络通信设备自身具有入侵检测能力,防止对设备的攻击入侵。

#### 8.2.2 通信传输

通信传输应满足以下要求:

- a) 通过 5G 网络的空口、UPF 设备承载的数据等采用逻辑独立的信道传输;
- b) 使用 5G 网络的空口、UPF 设备进行指令或相关数据交互的操作,采用加密认证技术手段实现身份认证、访问控制和数据加密传输;
- c) 具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据完整性保护能力;
- d) 具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据机密性保护能力;
- e) 具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据防重放保护能力;
- f) 具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据完整性保护能力;
- g) 具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据机密性保护能力;
- h) 具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据防重放保护能力;
- i) 具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数据完整性保护能力;
- j) 具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数据机密性保护

能力。

### 8.2.3 无线安全

应具有空口干扰检测和干扰定位能力。

### 8.2.4 入侵防范

入侵防范应满足以下要求：

- a) 具有伪造北斗、GPS等信号的检测和防御能力；
- b) 具有空口信令面DDoS攻击的检测和防御能力；
- c) 具有传输端口的访问控制能力,设置访问控制规则；
- d) 具有用户面数据的流量检测能力。

## 8.3 安全区域边界

### 8.3.1 边界防护

5G网络N6接口与应用服务器网络之间的访问和数据流应通过边界网关设备,并设置访问控制规则。

### 8.3.2 访问控制

访问控制应满足以下要求：

- a) 5G用户终端设备开启接入认证功能,并支持采用5G网络进行双向认证；
- b) 对5G专网中存在多种业务系统的,通过数据网络名称(DNN)或网络切片等方式对不同业务系统进行安全隔离,并限制无权限访问相关业务系统的5G用户终端设备接入业务系统所在的网络；
- c) 能根据5G用户终端设备所在的区域,控制其接入相应5G专网权限,限制5G用户终端设备在非授权区域访问5G专网及相关业务系统。

### 8.3.3 入侵防范

入侵防范应满足以下要求：

- a) 边缘应用具有抗击多种高级攻击的安全防御能力；
- b) 具有对5G用户终端设备恶意行为(例如UE互访、地址欺骗等)的检测,并对存在恶意行为的5G用户终端设备进行处置的能力。

## 8.4 安全计算环境

### 8.4.1 身份鉴别

应具有主认证之外的二次认证方式,以确保仅授权的UE访问用户所属网络。

### 8.4.2 5G用户终端设备安全

5G用户终端设备安全应满足以下要求：

- a) 固件及固件升级包上线前进行安全性检测；
- b) 具有软件白名单控制能力,能根据白名单控制应用软件安装、运行。

### 8.4.3 访问控制

应提供 MEC 平台用户设置其所属的不同虚拟机之间的访问控制策略的功能。

### 8.4.4 入侵防范

应在 MEC 平台提供虚拟机逃逸攻击的检测机制,防止虚拟机对虚拟化管理平台的入侵攻击,防止虚拟机获取虚拟化管理平台的控制权限。

### 8.4.5 数据安全

应具有空口用户面数据和控制面数据的机密性和完整性功能。

## 8.5 安全管理中心

安全管理中心集中管控应满足以下要求:

- a) 分离业务系统流量与 5G 网络管理流量;
- b) 建立设备管理的安全传输通道,对 5G 电信运营商提供的网元设备进行安全管理;
- c) 具有安全配置核查能力,避免不安全配置导致的安全风险;
- d) 具有空口用户面和控制面的安全算法优先级配置行为的安全审计功能。

## 8.6 安全建设管理

### 8.6.1 电信运营商选择

应选择具有基础电信业务经营资质的 5G 电信运营商,其所提供的 5G 网络应为所承载的业务应用系统及数据传输业务提供不低于其安全保护等级的安全保护能力。

### 8.6.2 应用软件采购

应用软件采购应满足以下要求:

- a) 5G 用户终端设备、MEC 平台等安装、运行的应用软件来自可靠分发渠道或使用数字签名;
- b) 网络通信设备的产品及服务符合国家标准、行业标准;
- c) 5G 用户终端设备、MEC 平台等安装、运行的应用软件由授权的开发者开发;
- d) 5G 基站和 UPF 设备的软件实现安全自动化构建;
- e) 5G 基站和 UPF 设备的软件实现版本控制和配置管理。

## 8.7 安全运维管理

### 8.7.1 5G 用户终端设备管理

5G 用户终端设备管理应满足以下要求:

- a) 指定人员定期巡视 5G 用户终端设备的部署环境,对可能影响设备正常工作的环境异常进行记录和维护;
- b) 对 5G 用户终端设备的入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定,并进行全程管理。

### 8.7.2 隐私管理

隐私管理应满足以下要求:

- a) 具有使用 5G-GUTI 替代 SUPI 的能力,实现 5G 用户信息的隐私保护;
- b) 具有增强的用户身份保密措施,除紧急呼叫外,使用 SUCI 或 5G-GUTI 在注册过程中传输 SUPI。

### 8.7.3 网络能力开放接口

应加强网络能力开放接口安全防护能力,防止攻击者从网络能力开放接口渗透进入行业应用网络。

## 9 第四级安全扩展要求

### 9.1 安全物理环境

在业务数据不出园区的场景下,应将 5G 基站、UPF 设备和 5G 用户终端设备部署在园区内。

### 9.2 安全通信网络

#### 9.2.1 网络架构

网络架构应满足以下要求:

- a) 5G 行业应用系统不运行在低于其安全保护等级的 5G 网络上;
- b) 将由电信运营商或其他外部单位运营维护的 5G 基站、UPF 设备、MEC 平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段;
- c) 网络通信设备不包含其供应商、生产商或开发人员不再支持的软件和硬件组件,例如已达到生命周期或不再支持的组件;
- d) 网络通信设备自身具有入侵检测能力,防止对设备的攻击入侵。

#### 9.2.2 通信传输

通信传输应满足以下要求:

- a) 通过 5G 网络的空口、UPF 设备承载的数据等采用硬隔离机制(无线采用 5G 专用基站或载波隔离或资源块预留,传输采用 FlexE、TDM、光波长切分等方式隔离,UPF 设备采用专用部署模式)的信道传输;
- b) 使用 5G 网络的空口、UPF 设备进行指令或相关数据交互的操作,采用加密认证技术手段实现身份认证、访问控制和数据加密传输;
- c) 具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据完整性保护能力;
- d) 具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据机密性保护能力;
- e) 具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据防重放保护能力;
- f) 具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据完整性保护能力;
- g) 具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据机密性保护能力;
- h) 具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据防重放保护能力;
- i) 具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数据完整性保护能力;
- j) 具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数据机密性保护能力。



### 9.2.3 无线安全

无线安全要求应满足以下要求：

- a) 具有空口干扰检测和干扰定位能力；
- b) 在5G基站工作范围内,具有对发射仿冒无线信号的伪基站进行检测的能力。

### 9.2.4 入侵防范

入侵防范应满足以下要求：

- a) 具有伪造北斗、GPS等信号的检测和防御能力；
- b) 具有空口信令面DDoS攻击的检测和防御能力；
- c) 具有传输端口的访问控制能力,设置访问控制规则；
- d) 具有用户面数据的流量检测能力。

## 9.3 安全区域边界

### 9.3.1 边界防护

5G网络N6接口与应用服务器网络之间的访问和数据流应通过边界网关设备,并设置访问控制规则。

### 9.3.2 访问控制

访问控制应满足以下要求：

- a) 5G用户终端设备开启接入认证功能,并支持采用5G网络进行双向认证；
- b) 对5G专网中存在多种业务系统的,通过硬隔离机制(无线采用5G专用基站或载波隔离或资源块预留,传输采用FlexE、TDM、光波长切分等方式隔离,UPF设备采用专用部署模式)对不同业务系统进行安全隔离,并限制无权限访问相关业务系统的5G用户终端设备接入业务系统所在的网络；
- c) 能根据5G用户终端设备所在的区域,控制其接入相应5G专网权限,限制5G用户终端设备在非授权区域访问5G专网及相关业务系统。

### 9.3.3 入侵防范

入侵防范应满足以下要求：

- a) 边缘应用具有抗击多种高级攻击的安全防御能力；
- b) 具有对5G用户终端设备恶意行为(例如UE互访、地址欺骗等)的检测,并对存在恶意行为的5G用户终端设备进行处置的能力。

## 9.4 安全计算环境

### 9.4.1 身份鉴别

应具有主认证之外的二次认证方式,以确保仅授权的UE访问用户所属网络。

### 9.4.2 5G用户终端设备安全

5G用户终端设备安全应满足以下要求：

- a) 固件及固件升级包上线前进行安全性检测；



- b) 具有软件白名单控制能力,能根据白名单控制应用软件安装、运行。

#### 9.4.3 访问控制

应提供 MEC 平台用户设置其所属的不同虚拟机之间的访问控制策略的功能。

#### 9.4.4 入侵防范

应在 MEC 平台提供虚拟机逃逸攻击的检测机制,防止虚拟机对虚拟化管理平台的入侵攻击,防止虚拟机获取虚拟化管理平台的控制权限。

#### 9.4.5 数据安全

应具有空口用户面数据和控制面数据的机密性和完整性功能。

### 9.5 安全管理中心

安全管理中心集中管控应满足以下要求:

- a) 分离业务系统流量与 5G 网络管理流量;
- b) 建立设备管理的安全传输通道,对 5G 电信运营商提供的网元设备进行安全管理;
- c) 具有安全配置核查能力,避免不安全配置导致的安全风险;
- d) 具有空口用户面和控制面的安全算法优先级配置行为的安全审计功能。

### 9.6 安全建设管理

#### 9.6.1 电信运营商选择

应选择具有基础电信业务经营资质的 5G 电信运营商,其所提供的 5G 网络应为所承载的业务应用系统及数据传输业务提供不低于其安全保护等级的安全保护能力。

#### 9.6.2 应用软件采购

应用软件采购应满足以下要求:

- a) 5G 用户终端设备、MEC 平台等安装、运行的应用软件来自可靠分发渠道或使用数字签名;
- b) 网络通信设备的产品及服务符合国家标准、行业标准;
- c) 5G 用户终端设备、MEC 平台等安装、运行的应用软件由授权的开发者开发;
- d) 5G 基站和 UPF 设备的软件实现安全自动化构建;
- e) 5G 基站和 UPF 设备的软件实现版本控制和配置管理。

### 9.7 安全运维管理

#### 9.7.1 5G 用户终端设备管理

5G 用户终端设备管理应满足以下要求:

- a) 指定人员定期巡视 5G 用户终端设备的部署环境,对可能影响设备正常工作的环境异常进行记录和维护;
- b) 对 5G 用户终端设备的入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定,并进行全程管理。

### 9.7.2 隐私管理

隐私管理应满足以下要求：

- a) 具有使用 5G-GUTI 替代 SUPI 的能力,实现 5G 用户信息的隐私保护；
- b) 具有增强的用户身份保密措施,除紧急呼叫外,使用 SUCI 或 5G-GUTI 在注册过程中传输 SUPI。

### 9.7.3 网络能力开放接口

网络能力开放接口应满足以下要求：

- a) 应加强网络能力开放接口安全防护能力,防止攻击者从网络能力开放接口渗透进入行业应用网络；
- b) 应加强网络能力开放接口暴露面收敛。

## 10 第五级安全扩展要求

略。

附录 A  
(资料性)

基于 5G 技术边缘计算等级保护对象的应用场景和架构

从应用场景、地理位置、服务范围等角度,采用 5G 技术的边缘计算等级保护对象可以分为局域网 5G 行业应用和广域网 5G 行业应用两大类,采用 5G 技术的边缘计算等级保护对象示意图见图 A.1。

- a) 局域网 5G 行业应用:一般限定在特定地理区域内,基于 5G 网络实现接入应用的业务闭环安全,保障应用的核心业务和数据不出园区,主要适用于工业制造、钢铁、采矿、港口、教育、医疗等园区/厂区型应用场景。
- b) 广域网 5G 行业应用:一般不限定地理区域,通常基于电信运营商提供的端到端广域网络,通过 5G 的虚拟或物理切片等方式实现不同行业不同业务的安全通信与业务数据承载,主要适用于交通、电力、车联网以及跨域经营的特大型企业等应用场景。

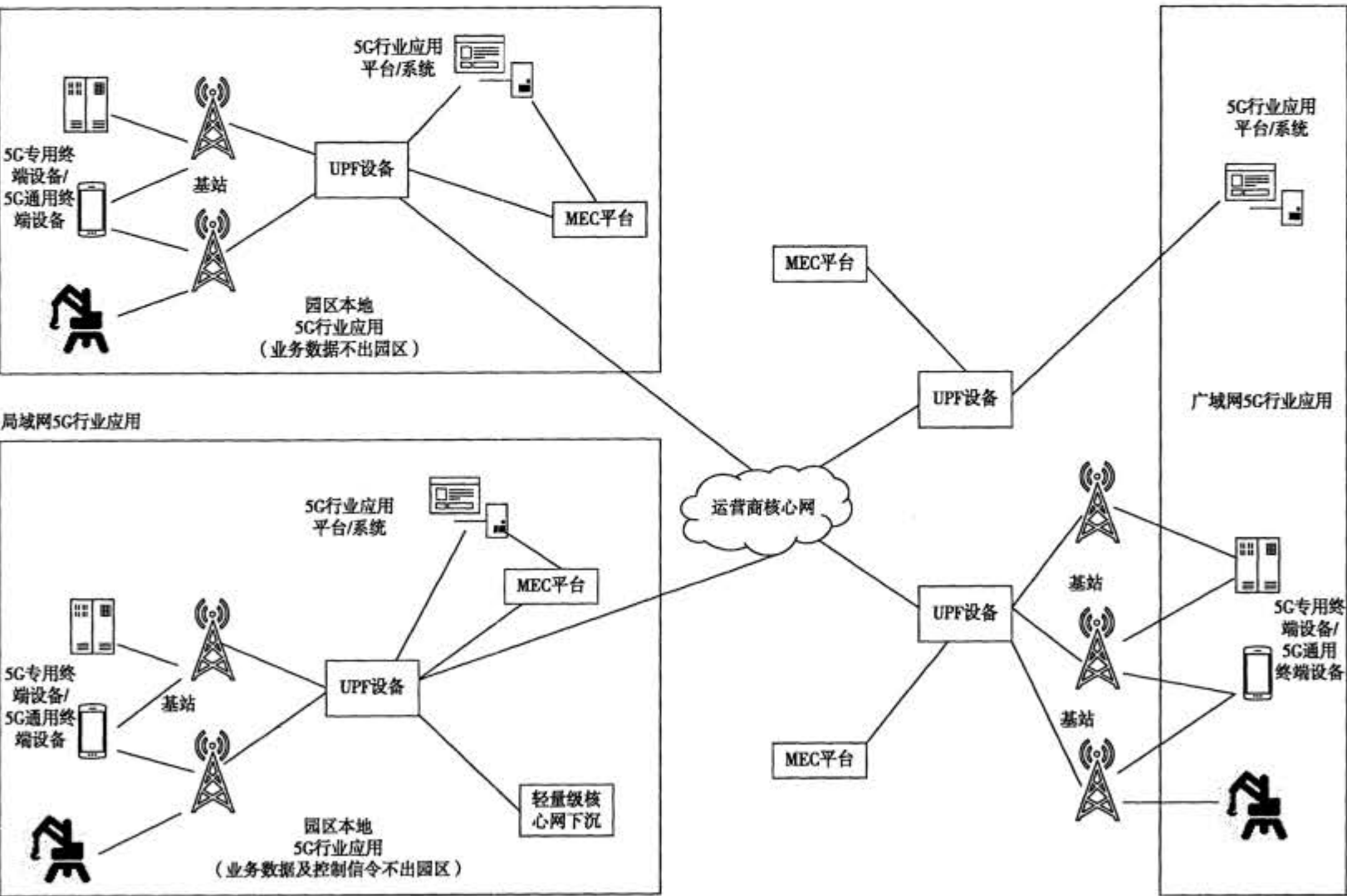


图 A.1 采用 5G 技术的边缘计算等级保护对象示意图

与传统信息系统相比,采用 5G 技术的边缘计算等级保护对象通过 5G 网络提供的网络切片能力,构建从 5G 用户终端设备到 5G 基站、再到 MEC 平台、再到业务应用平台的端到端局域或广域虚拟网络。保障虚拟专网资源和公众网络的逻辑隔离甚至物理隔离,并通过边缘计算能力,在园区区域内构建独享或部分独享的虚拟网络资源。提供就近的数据传输、存储、计算、处理等,以满足业务应用对于快速处理、安全、低时延等的需求。

附录 B  
(资料性)

基于 5G 技术边缘计算等级保护对象的局域网应用场景与架构

局域网 5G 行业应用也称为面向园区本地的 5G 行业应用,面向园区本地的 5G 行业应用安全的首要原则是保障核心业务数据不出园区。见图 B.1 所示。

在网络部署方面,面向园区本地的 5G 行业应用安全架构一般可分为两类:

- a) 针对只需要用户面数据流进行安全保障的 5G 行业应用,核心网通过下沉 UPF 设备到园区来实现本地业务数据分流到企业内网,保障业务数据不出园区;
- b) 针对对于专网要求极高的少数 5G 行业应用,不但要求行业业务的数据流不出园区,也要求网络控制面数据不出园区,一般需要将 5G 核心网(控制面+用户面)整体下沉到园区。

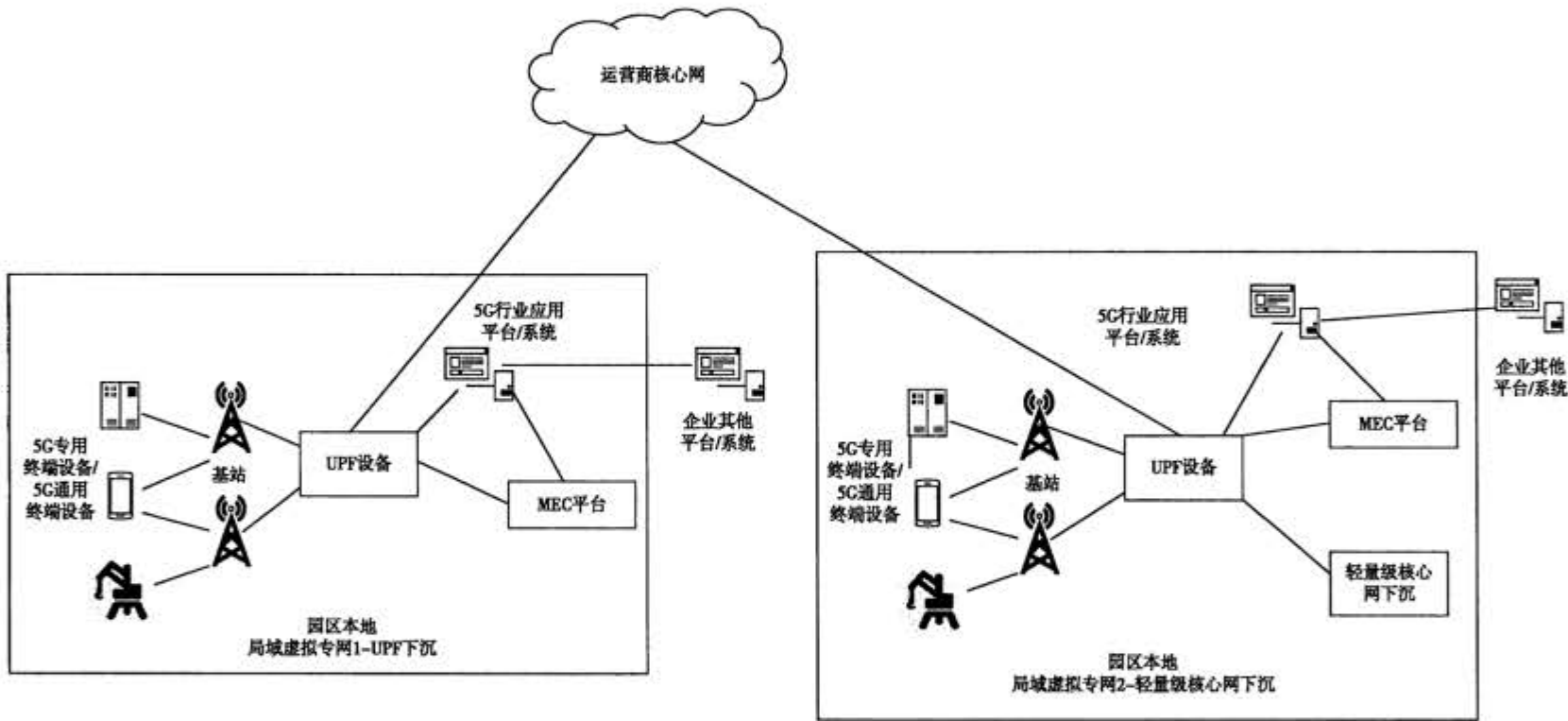


图 B.1 采用 5G 技术边缘计算等级保护对象的局域网应用场景与架构图

附录 C  
(资料性)

基于5G技术边缘计算等级保护对象的广域网应用场景与架构

面向广域网的5G行业应用是基于电信运营商5G网络的广域覆盖能力,在较大地理区域提供信息系统和业务应用所需的数据传输能力,具有覆盖广、跨域大的特点。面向广域的5G行业虚拟专网由5G无线接入网、5G核心网、MEC平台、5G行业应用平台/系统组成。

按照行业应用对5G网络资源的共享情况,面向广域网的边缘计算安全总体逻辑架构分为两大类。

- a) 基于网络资源共享的逻辑架构(如图 C.1 所示),在该模式下:
- 1) 无线网络方面,各行业应用共同使用电信运营商的5G无线网络资源;
  - 2) 核心网方面,行业应用可根据需求共用核心网控制面和用户面,也可以通过逻辑专用切片实现核心网控制面资源的虚拟专用;
  - 3) 用户面网元UPF设备根据是否共用和是否虚拟化分为多应用共用、虚拟专用或者物理专用。

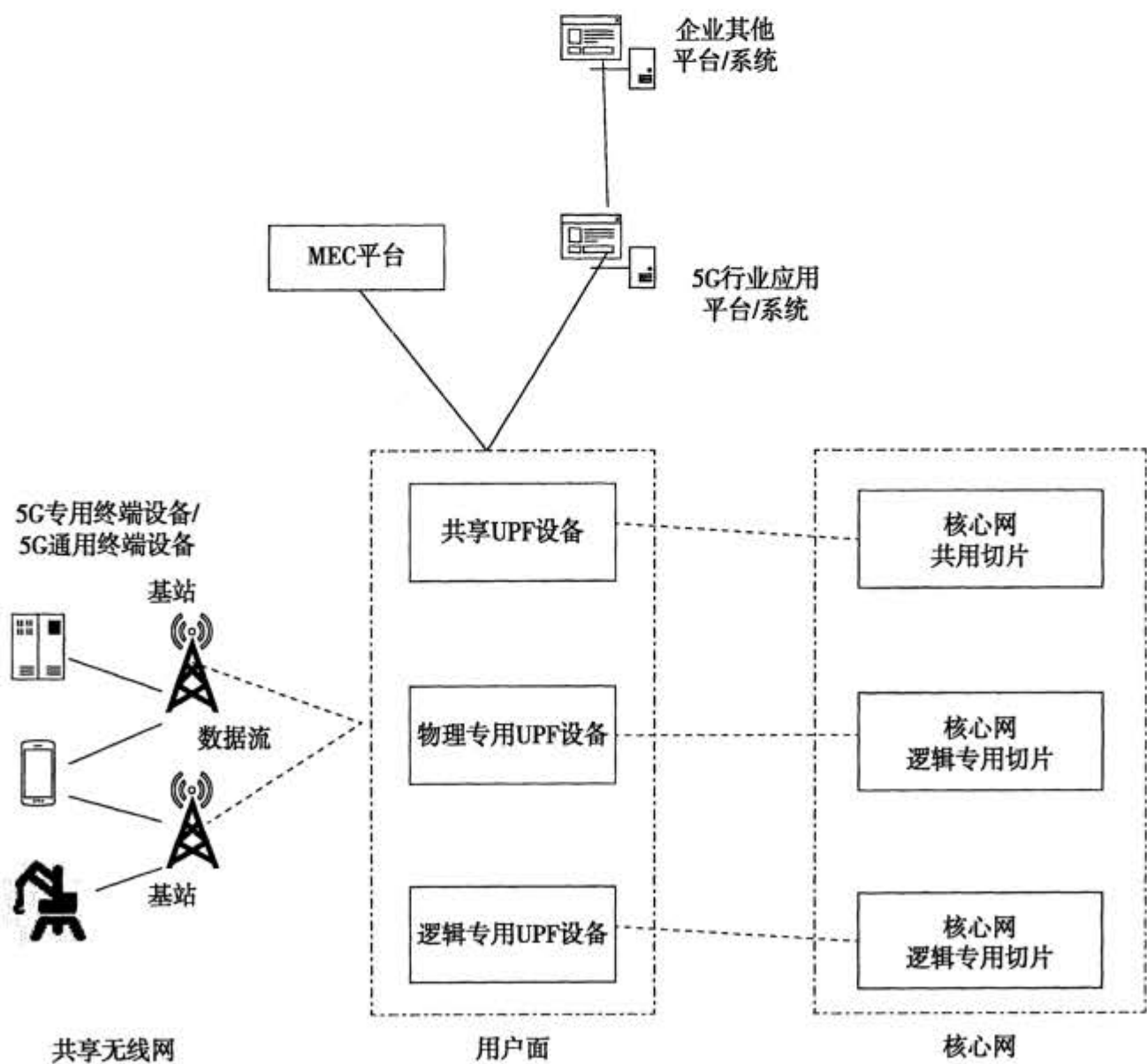


图 C.1 基于网络资源共享的广域网 5G 行业应用安全架构图

- b) 基于物理资源独享的逻辑架构(如图 C.2 所示),在该模式下:
- 1) 无线网络方面,各行业应用共同使用运营商的5G无线网络资源;
  - 2) 核心网方面,行业应用可根据需求使用运营商提供的物理隔离的专用切片方式满足业务传



- 输需求,核心网控制面通过专用服务器承载物理专用的切片实现物理资源独享;
- 3) 用户面网元UPF设备根据是否虚拟化分为虚拟专用或者物理专用,实现业务流量隔离。

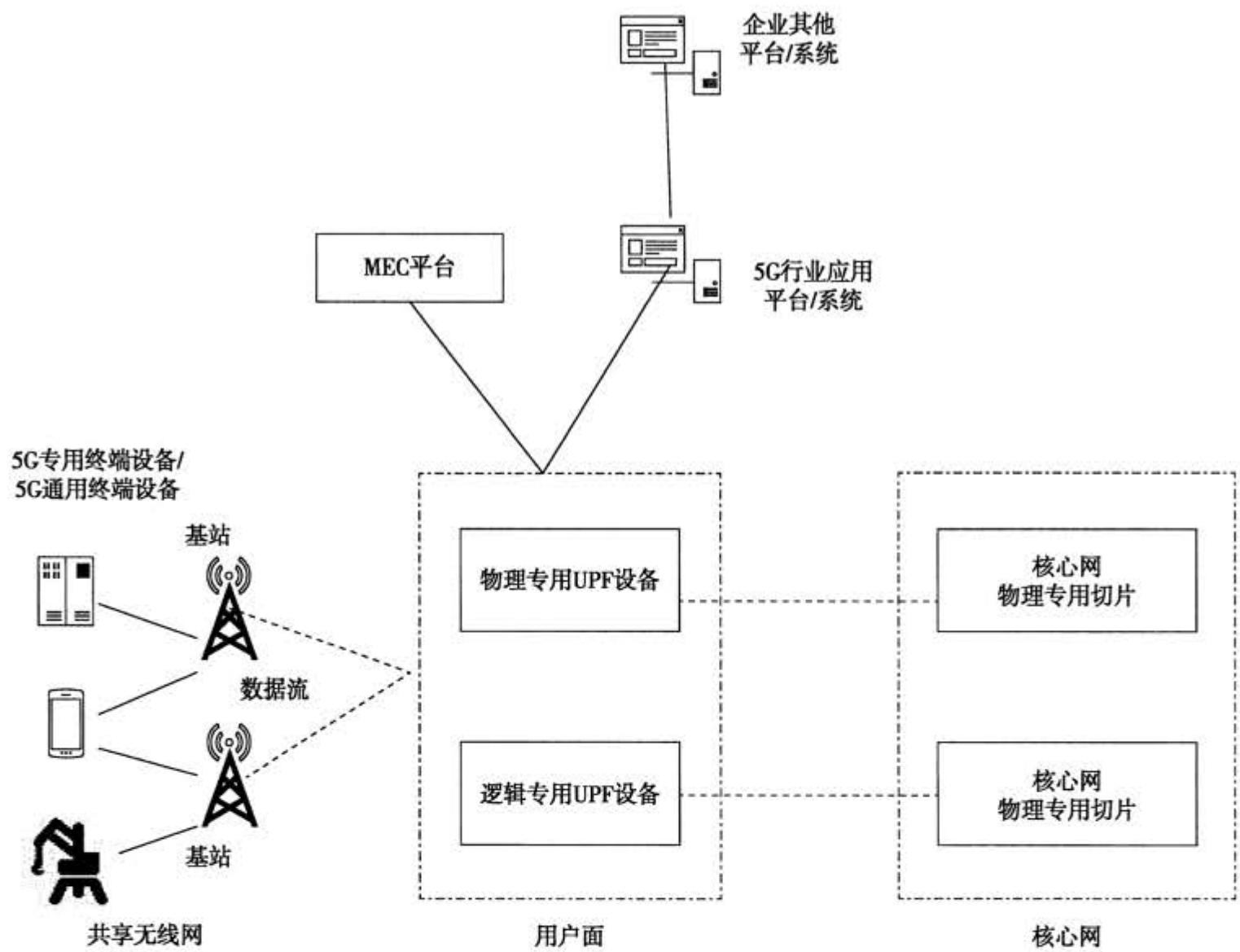


图 C.2 基于物理资源独享的广域网 5G 行业应用安全架构图

参 考 文 献

- [1] GB/T 42564—2023 信息安全技术 边缘计算安全技术要求
  - [2] 3GPP TR 21.905 V17.1.0 Vocabulary for 3GPP Specifications
  - [3] 3GPP TS 22.261 V19.4.0 Service requirements for the 5G system
  - [4] 3GPP TS 23.501 V18.3.0 System architecture for the 5G System
  - [5] 3GPP TS 33.501 V18.3.0 Security architecture and procedures for 5G System
  - [6] ETSI GS MEC 001 V2.1.1 Multi-access Edge Computing(MEC): Terminology
-