

T/SZIoT

团 体 标 准

T/SZIoT XXXX—XXXX

基于 5G 的工业互联网应用系统通用要求

General requirements for 5G-based industrial Internet application system

（征求意见稿）

2022.09.29

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2022 – XX – XX 发布

XXXX – XX – XX 实施

深圳市物联网产业协会 发 布

目 次

前言 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 系统技术架构 2

6 采集层 2

7 网络层 2

8 应用层 3

9 安全管理 5

附录 A（资料性） 5G 混合专网与 MEC 融合 8

附录 B（资料性） 5G 混合专网通信能力 10

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。

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。

本文件由欣旺达电子股份有限公司提出。

本文件由深圳市物联网产业协会归口。

本文件起草单位：欣旺达电子股份有限公司、深圳市标准技术研究院、中国联合网络通信有限公司深圳市分公司、速博达（深圳）自动化有限公司、深圳市欣旺达电气技术有限公司。

本文件主要起草人：贺小鹏、吕品风、陈龙、周强、张旭杰、周大斌、范鑫磊、郭从锋、陈耀忠、周文、梁锐、张建华、杜永博、白雪峰、叶同舟、郑爱媚、余海钊、方锐、毛睿。

本文件为首次发布。

引 言

现在是一个高速发展的社会，科技发达，信息流通，人们之间的交流越来越密切，设备与人之间的交集也越来越密切，大数据就是这个高科技时代的产物，但是目前大数据遇到的瓶颈除了人才紧缺，同时网络受限也成为阻碍之一。设备互联需要更稳定、更快速的网络支撑，大批量的数据分析和交互也需要更大网络带宽支持，传统的4G、Wifi和有线网络存在一定的瓶颈问题，而5G网络具有大带宽、低时延的特性，确保了海量数据的毫秒级传输，是实现工业设备上云、生产流程智能协同的关键。当前技术问题主要体现在：

（1）生产线的灵活部署能力差。生产线上的设备受限于线缆的束缚，设备移动或新增都需要重新对物理网络的线路进行施工改造，对生产线的设备快速调整存在影响。

（2）生产线设备未能实现互联互通。生产线上集成的各种非标设备、标准设备等，设备的软件系统、数据通讯协议、数据采集传输等技术规格不一致，一是未能实现单台设备与MES\WMS\PLM等系统联通，实时上传数据和执行指令；二是设备之间和整体生产线的数据未能互联互通。

（3）工厂的AMR系统的应用，依赖于厂区的无线网络信号，网络质量要求非常高，无线网络需要达到低时延、高稳定的要求。而无线AP的性能，仍存在无线网络信息覆盖不到位或信号干扰、上下层无线信号漫游失联等问题，导致AMR物料车异常，物料未即时送达，产线面临停线风险从而造成损失。

鉴于以上技术问题，特制定本标准。通过将新一代5G技术运用到智能工厂的搭建中，对Pack生产线的应用系统做出规范，形成5G技术应用于工业互联网中的测试平台及智能工厂示范应用，最终形成5G应用工厂（车间）参考模型，带动工业互联网和5G融合发展。

基于 5G 的工业互联网应用系统通用要求

1 范围

本文件规定了基于5G的工业互联网应用系统技术架构、采集层、网络层、应用层的技术要求，以及安全管理要求。

本文件适用于制造型企业Pack生产线工业互联网应用系统的5G改造与应用。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

本文件没有需要界定的术语和定义。

4 缩略语

下列缩略语适用于本文件。

AMF: 接入和移动性管理功能 (access and mobility management function)

AP: 无线接入点 (access point)

CA: 载波聚合 (carrier aggregation)

CT: 通信技术 (communication technology)

ERP: 企业资源计划 (enterprise resource planning)

FDD: 频分双工 (frequency division duplexing)

HLS: 基于HTTP的自适应码率流媒体传输协议 (HTTP live streaming)

IMEI: 国际移动设备识别码 (international mobile equipment identity)

IPC: 工业控制计算机 (industrial personal computer)

IPsec: 互联网协议安全性 (internet protocol security)

JIT: 准时制 (just in time)

PLC: 可编程逻辑控制器 (programmable logic controller)

MEC: 多接入边缘计算 (multi-access edge computing)

MEP: 多接入边缘计算平台 (MEC platform)

MES: 制造执行系统 (manufacturing execution system)

MIMO: 多进多出 (multiple input multiple output)

NR: 新空口 (new radio)

QAM: 正交幅度调制 (quadrature amplitude modulation)

RNIS: 无线网络信息服务 (radio network information services)

RRU: 射频拉远单元全称 (remote radio unit)

RTMP: 实时消息传输协议 (real time messaging protocol)

RTSP: 实时流传输协议 (real time streaming protocol)

SA: 独立组网 (stand alone)

SOP: 标准作业程序 (standard operating procedure)

SPC: 统计过程控制 (statistical process control)

SSL: 安全套接层 (secure socket layer)

SUCI: 订阅隐藏标识符 (subscription concealed identifier)

TDD: 时分双工 (time division duplexing)

UPF: 用户面功能 (user plane function)

UDM: 统一数据管理 (unified data management)
WMS: 仓库管理系统 (warehouse management system)
5GC: 5G核心网 (5G Core)

5 系统技术架构

基于5G的工业互联网应用系统可分为以下三层，见图1：

- a) 采集层：主要包括工业生产现场工业设备上的传感器、扫码枪、摄像头等各类采集终端，实现对生产现场设备、产品、环境、人员等对象的数据采集；
- b) 网络层：物联网关、工业工控机、工业 AP、RRU 等设备，将作为采集层设备采集数据传输的媒介；
- c) 应用层：集成 ERP、MES、WMS 等应用系统，实现从生产的原材料到产品的生产制造过程的精准控制与决策管理，实现应用与生产单元之间的精细高效协同作业。



图1 系统技术架构

6 采集层

6.1 采集设备

- 6.1.1 基于 PLC 和 IPC，通过传感器、扫码枪、工业相机、测试仪器仪表等设备，对产品条码、位置、温度、压力、电阻、电压、外观、故障报警等数据实时采集。
- 6.1.2 通过伺服电机、工业机器人等对生产制造过程精确控制。

6.2 接口协议

设备间通过RS485和RJ45等主流通讯接口，TCP/IP和EtherCAT等通讯协议进行数据互联互通。

7 网络层

7.1 5G 混合专网架构

5G混合专网（以下简称“5G专网”）主要由5G基站、核心网网元AMF/SMF和核心网用户面网元专用UPF/MEC构成。其中5G基站可选公众网络共享或企业侧独立部署，并通过N2接口与用户侧部署的AMF/SMF进行对接，通过N3接口与用户侧部署的UPF/MEC进行对接；核心网用户面网元UPF/MEC独立部署于行业用

户的园区内；核心网网元AMF/SMF可选共用公众网络核心网资源或在行业用户园区内独立部署。5G混合专网架构见图2。

- 注1：5G专网与MEC融合部署方式与能力见附录A。
- 注2：5G专网为用户提供部分物理独享的5G专用网络，能够满足行业用户大带宽、低时延、数据不出园区的需求。该模式下行业用户网内业务数据本地卸载，可通过功能定制优化，减小公众网络故障对用户生产业务的影响，保障生产安全。

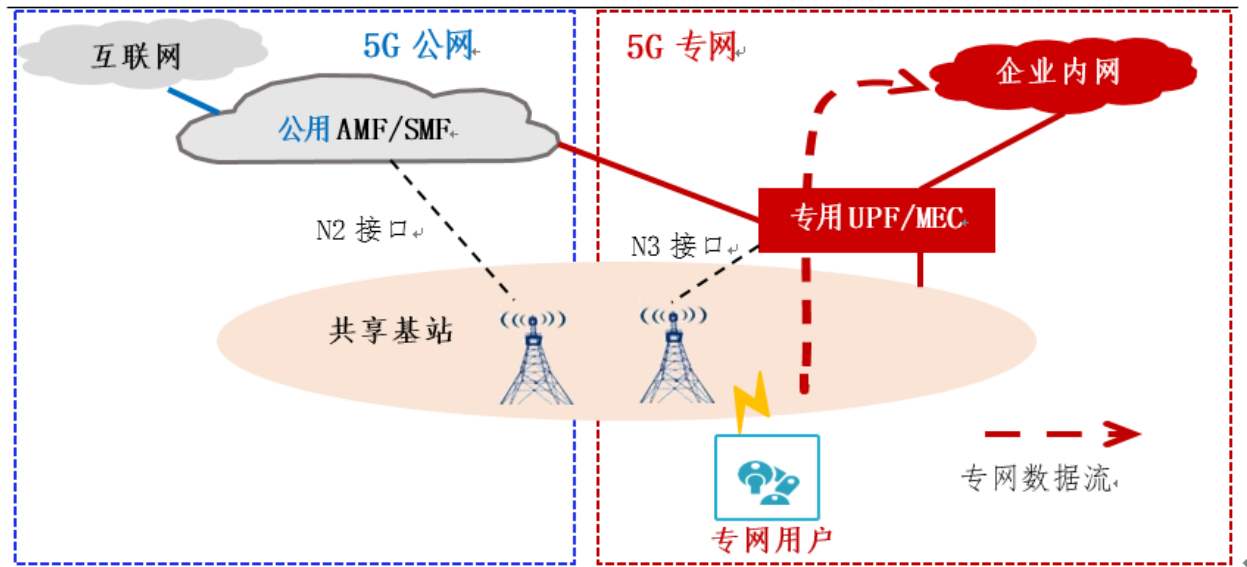


图2 5G混合专网网络架构

7.2 5G混合专网业务路由

- 7.2.1 在接入选网流程中，5G基站对接核心网AMF、UPF，并为专网用户规划专有切片标识。专网用户终端在园区搜索到无线信号，发起接入注册流程，基站根据终端上所带标识选择用户侧专用核心网AMF，AMF负责对用户进行接入认证和鉴权（UDM配合），认证成功后建立会话，用户可正常进行数据业务。
- 7.2.2 专网用户或专网终端注册成功后，专网用户的数据转发流程：专网终端→专网基站→专网UPF/MEC→企业内部应用。

7.3 5G混合专网通信

- 5G专网通信应具备以下功能和性能：
- a) 支持时隙配比灵活可调、子载波间隔、多MIMO能力以及CA载波聚合能力；
 - b) 下行信号应兼容Wi-Fi6；
 - c) 支持IPv4单栈、IPv6单栈以及IPv4/v6双栈；
 - d) 下行峰值速率不低于800Mbps，上行峰值速率不低于220Mbps；
 - e) 采集层设备到现场MEC服务器，发出PING Request到收到PING Reply之间的时延平均值不超过20ms；
 - f) NR业务建立成功率不小于99%，网络丢包率小于0.1%；
 - g) 在SA架构下，5G专网的移动性管理支持：
 - 1) 空闲态和连接态下NR到NR移动性过程，包括小区重选、切换和重定向；
 - 2) 空闲态和连接态下NR到LTE移动性过程以及空闲态和连接态下的LTE到NR移动性过程；
 - 3) 网络切片选择及管理能力，切片和5G专网终端上的业务进行绑定。

- 注1：NR模式和SA模式通信能力见附录B。
- 注2：5G专网支持下行高达Gbps的用户体验速率、数十Gbps的用户峰值速率、整个区域的流量密度至少可以达到Tbps/km²。

8 应用层

8.1 基本要求

应用层围绕着核心系统即MES以及其他集成系统应具备以下三个基本功能：

- a) 数字化监控：通过采集生产设备等数据，进行设备监控、源监控，从而做出分析及提升产能；
- b) 全面运营数字化管理：打通 ERP、MES、WMS、QMS、APS、PLM、CRM、SAP、设备及 HR 等信息系统数据；
- c) 精益物流。

8.2 基本 MES 功能

8.2.1 生产过程管理

应具备产品生产全过程的无间隙管控、设备防错与追溯、无纸化电子SOP、JIT拉动式的物流配送等功能。

8.2.2 生产排程管理

应根据人员、设备、线体以及产品标准工时等基础设定和约束条件，对生产进行排程。

8.2.3 全制程质量管控

应具备以下功能：

- a) 通过品质预警机制对生产过程中的品质异常及时反馈、跟踪并处理；
- b) 自动进行质量数据分析并生成多维度质量分析报告,如SPC统计分析报告；
- c) 具备自动预警与停线机制。

8.2.4 可视化管理

应能用可视化管理工具全制程监控生产进度、品质状况、设备状态与效率，实时反馈生产问题，实现电子看板、邮件、短信和企业微信等自动推送功能。

8.2.5 设备与治具（备件）管理

应对设备与治具（备件）进行全面管控。

8.2.6 生产追溯管理

应能通过条码管理，实现人、机、料、法、环等信息追溯。

8.2.7 智能仓储管理

应能通过物料条码化管理，对物料进行IQC检验、收料、发料、退料、报废、调拨、盘点等运作。

8.2.8 物联网中间件/接口

8.2.8.1 应能集成通用设备接口,实现各行业设备和测试设备之间的深度集成、数据交互和数据协同。

8.2.8.2 应能通过中间件、接口等方式将生产过程中的数据以 5G 网络传输至数据库。

8.3 数据分析报表

应能提供基本的数据分析能力,如通过生成数据分析报表等方式优化改良生产过程。

8.4 AI 应用

8.4.1 AI 合规

可利用RTSP、RTMP、HLS等通用协议把特定场景部署的摄像机（或接入现有的监控视频）接入应用系统，通过AI算法实现生产、安全等智能化管控。

8.4.2 AI 质量检测

可通过AI质量检测取代人工的方式实现效率提升和成本控制。

9 安全管理

9.1 设备安全

9.1.1 访问控制与审计

可采用安全审计技术实现人与IT资产的关联，从账号、授权、认证、审计等多个维度提供安全管控。企业应对运维人员的运维操作进行控制和审计，对整个运维过程从“事前预防”、“事中控制”和“事后审计”进行全程参与：

- a) 事前预防：建立“自然人-资源-资源账号”关系，实现统一认证和授权；
- b) 事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制；
- c) 事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定。

9.1.2 弱点发现

应使用具备最新特征漏洞库的漏洞扫描与检测设备，快速发现网络资产，准确识别资产属性，全面扫描服务器操作系统及应用系统的漏洞，清晰定性安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而在发现漏洞的基础上实现设备安全自主掌控，见图3。

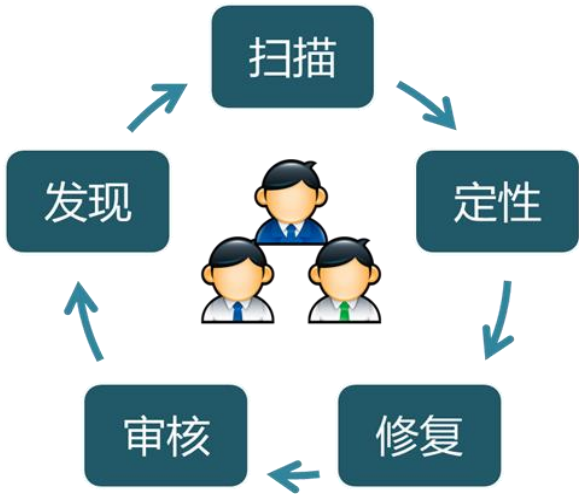


图3 漏洞扫描过程

9.1.3 恶意代码防范

应从安全技术、安全管理和意识两方面防止设备感染病毒：

- a) 技术层面：在终端上安装部署防病毒系统，并升级防病毒软件到最新的防病毒库，阻止已存在的病毒样本攻击；
- b) 管理和安全意识层面：
 - 1) 不打开陌生人或来历不明的邮件，防止病毒通过邮件的附件产生攻击；
 - 2) 不点击 office 宏运行提示，避免来自 Office 组件的病毒感染；
 - 3) 从正规途径获取需要的软件，不应双击打开 .bat、.vbs 等后缀名文件；
 - 4) 定期备份设备中重要的数据、文件和配置，以保障中病毒后可以安全恢复。

9.2 网络与通信安全

9.2.1 5G 专网安全

9.2.1.1 5G 专网应综合考虑网络认证密钥管理架构与公网的一致性、专网安全能力开放布局以及专网多层次的安全隔离度等内容，满足电信级通信设备安全要求，确保网络及业务的安全、完整、可用。5G 专网安全架构参见图 4。

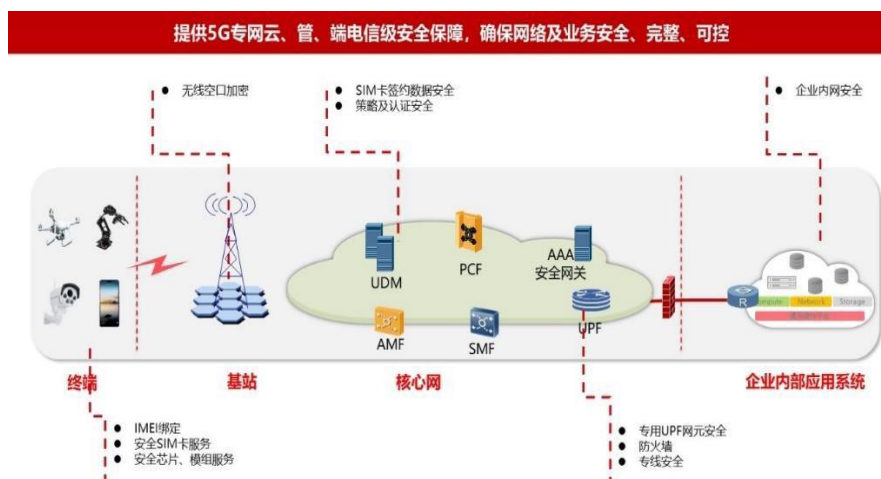


图4 5G 专网安全架构示意图

9.2.1.2 5G 专网应采用与公网统一的认证框架、建立统一的密钥体系，并支持多种接入方式和接入凭证，保证各类终端设备安全地接入专网，实现用户专网及公网的无缝切换，灵活并且高效地支持各种应用场景下的身份鉴权。

9.2.1.3 5G 专网应采用电信级 EAP-AKA 和 5G AKA 认证方法，避免非法用户接入。

9.2.1.4 5G 专网应考虑安全能力开放布局，既能保证开放的网络能力安全地提供给第三方，也能保证网络的安全能力（如加密、认证等）能够开放给第三方使用。5G 专网的开放安全能力包括但不限于：

- a) 基于 5G 专网接入认证向第三方提供业务层的访问认证¹；
- b) 基于终端智能卡（如 UICC/eUICC/ iUICC）的安全能力²。

9.2.1.5 5G 专网应通过 IMEI 绑定、SIM 卡 SUCI 加密定制化安全芯片/模组等方式为专网行业用户终端提供安全保障。

9.2.1.6 5G 专网应考虑多层次的安全隔离度，包括园区内专网自身的硬件安全、机房安全管理、专网与公网之间的安全以及加密管理等。应在外部网络出口部署防火墙或安全网关设备，实现网络安全隔离，防止外部攻击。

9.2.1.7 5G 专网应通过无线 NR 支持对空口信令和用户面数据的加密和完整性保护，配置多种加密及信息完整性安全算法保障空口安全。

9.2.1.8 5G 专网应具备容灾安全保障，可通过提供硬件备份、链路容灾及网元级容灾等不同程度的网络容灾保障，在网络单点故障情况下保障业务连续性。

9.2.2 通信安全

9.2.2.1 宜通过 IPsec 为 IP 网络通讯提供端到端的安全服务，保护 IP 网络通信免遭窃听和篡改，抵御网络攻击。

9.2.2.2 采用 IPsec 通信的两端（简称 IPsec 对等体）宜通过加密与数据源验证等方式，保证 IP 数据包在网络上传输时的私密性、完整性、真实性与防重放，具体要求如下：

- a) 私密性：IPsec 协议实体（采用 IPsec 通信的网元或网络设备）对用户数据进行加密，以密文的方式进行传输，防止其他人未经授权获取网络上传递的用户数据；
- b) 完整性：IPsec 协议实体对接收到的数据进行校验，以确保数据没有被篡改；
- c) 真实性：IPsec 协议实体对数据源进行身份认证，以确保数据来自真实的发送方；
- d) 防重放：IPsec 协议实体识别并拒绝恶意用户重复发送截取的报文。

9.3 平台安全

平台宜从以下五个维度确保平台业务的安全性：

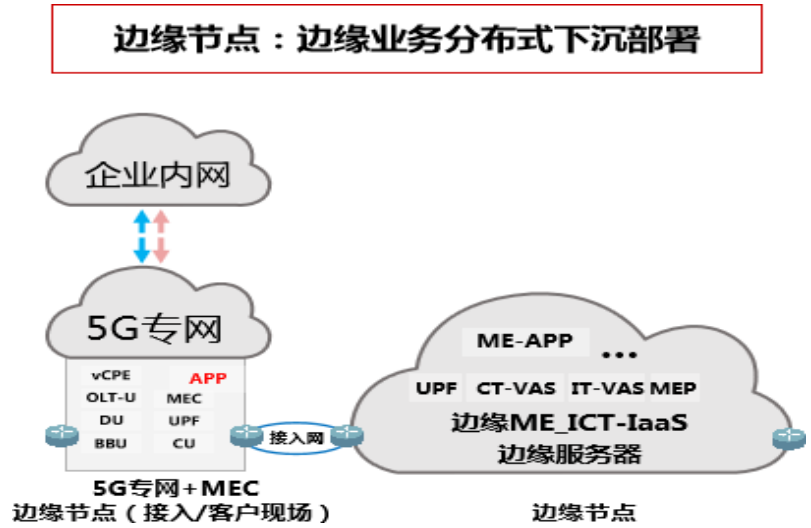
1) 业务层与网络层互信时用户在通过网络接入认证后可以直接访问第三方业务，简化用户访问业务认证，提高业务访问专网的效率。
2) 可拓展业务层的认证维度，增强专网对业务认证的安全性。

- a) 传输安全：采用 SSL 进行传输加密，并采用数据脱敏处理技术，对敏感数据进行 Hash、加密、遮盖、替换、洗牌、变换等处理，保障数据在上传、共享、下发等场景中不会被监听、窃取和篡改；
- b) 数据安全：根据业务场景、合规需求和安全要求，对数据进行分类分级和隔离加密保护，使用国密 SM9、AES256 等加密算法保障数据在业务平台中的存储安全，并使用入侵检测和防御系统，防止系统入侵、拖库或者内部原因导致数据外泄；
- c) 使用安全：对敏感数据使用国密、AES256 位等加密算法，并在使用过程中严格遵循“最小化原则”保障只有所有者和被授权人具备解密查看等权限。
- d) 监控审计：详细记录登录及资源访问操作，包括密钥管理、数据加解密、操作人、操作时间、源 IP 地址、资源对象、操作名称及操作状态，并能进行审计追溯。
- e) 安全合规：按照 PDCA 模式，建立涵盖合规要求、合规执行、合规检查、合规整改、合规评价的闭环管理机制；采取相应的技术手段、通过有效的管理措施，保障平台免遭威胁，将威胁带来的不良后果降到最低。

附录 A
(资料性)
5G 混合专网与 MEC 融合

A.1 部署方式

在实际部署时，5G专网+MEC能为行业用户提供从最基础的网络分流能力到各种CT-VAS（Value-Added Service）/IT-VAS能力的不同组合（CT-VAS/IT-VAS由基于运营商的MEP统一提供），充分满足企业业务对网络及PaaS能力的需求。当部署5G专网时，在企业侧部署的MEP可与边缘UPF、5GC对接，MEP提供基础的平台ICT-IaaS功能，MEP上部署CT-VAS/IT-VAS能力以及各种SaaS应用，并对企业用户提供自运维接口，适配用户侧业务对于网络能力、ICT-VAS、SaaS的灵活调度需求，见图A.1。



图A.1 边缘节点 MEC 与 5G 专网融合部署

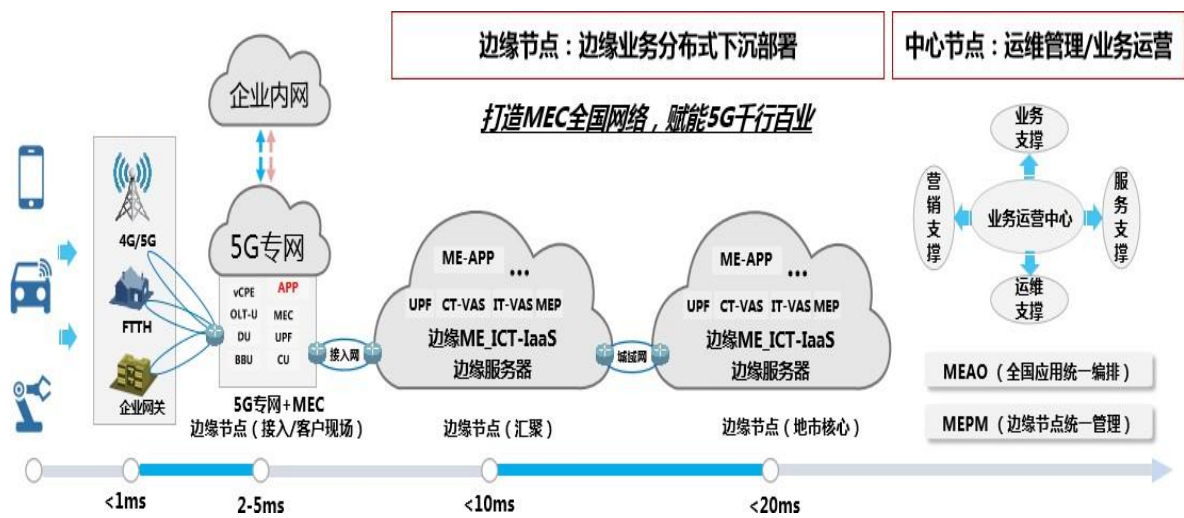
A.2 协同能力

A.2.1 概述

5G专网与垂直行业的深度融合将加速应用场景创新、改变生产方式、提升生产效率、支持垂直行业生产效能可持续增长。5G专网以“MEC边网一体”、“企业IT平滑对接”的协同能力，满足用户面向宽带化、移动化、物联化、多业务融合发展的需求，为用户提供专建专维、专用专享、量身定制、灵活便捷的5G专网服务。

A.2.2 MEC边网一体能力

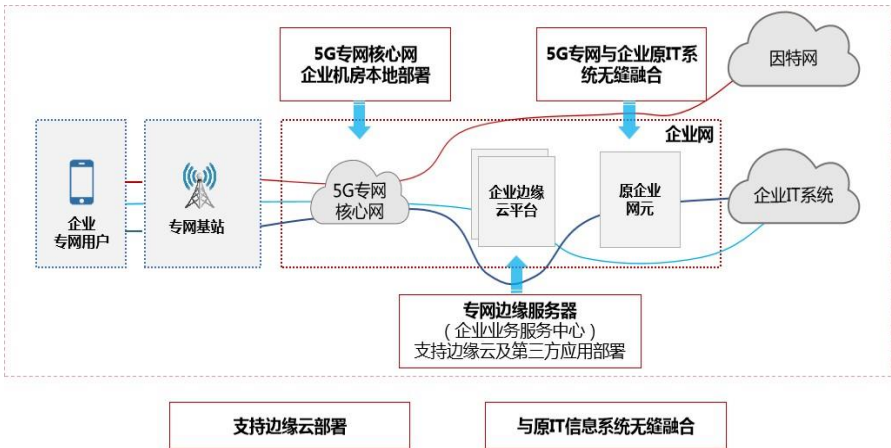
5G专网搭载 MEC 边缘云生态，在本地化卸流的同时提供计算资源与运行环境的就近部署，一方面降低网络通信时延，另一方面实现企业应用的快速搭建、部署与上线。MEC平台增强了网络联接的控制与管理，融合了算力下沉、动态路由、TCP加速、RNIS无线网络信息、CT增值应用能力、实时编解码、AI推理、VR渲染、VCDN等IT增值应用能力。通过边缘生态，可根据行业用户的多元化需求，按需将边缘应用和服务，推送到MEC实现开通、升级或者替换。见图A.2。



图A. 2 MEC 边网一体能力

A. 2. 3 企业IT平滑对接能力

可将5G专网核心网元私有化部署，开放专有接口对接企业服务器，实现5G专网在行业用户现有IT系统上“即插即用”的功能。可将5G专网运维与企业现有的IT业务管理融合，打通行业用户平台之间的数据孤岛，通过网络运行数据监测或预报自身的业务数据、生产效率、能耗分布区域。见图A. 3。



图A. 3 企业 IT 平滑对接能力

附录 B
(资料性)
5G 混合专网通信能力

B.1 NR 模式通信能力

5G 专网在 5G-NR 模式下支持的频段和带宽见表 B.1。5G 专网可根据行业用户的需求，支持 LTE FDD、TD-LTE、WCDMA、CDMA 和 GSM 等模式。

表 B.1 专网终端 在 5G-NR 模式下的工作频段和带宽

工作频段	上行频段 (MHz)	下行频段 (MHz)	最大带宽 (MHz)	双工模式
n78	3300 - 3800	3300 - 3800	100/200 ^a	TDD
n41	2496 - 2690	2496 - 2690	100	TDD
n1	1920 - 1980	2110 - 2170	20/30/40/50 ^b	FDD
n3 ^c	1710 - 1785	1805 - 1880	30	FDD
n8 ^c	880 - 915	925 - 960	20	FDD
n79 ^c	4400 - 5000	4400 - 5000	100	TDD
n77 ^c	3300-4200	3300-4200	100	TDD
n258 ^c	24250-27500	24250-27500	NA	TDD
^a n78 100MHz 带宽要求必选支持，n78 200MHz 带宽推荐支持； ^b 根据芯片支持情况要求支持； ^c 可选支持。				

B.2 SA 模式通信能力

5G 专网在 SA 组网模式下，n1 以及 n78 频段上可达到的行峰值速率见图 B.2。其中 NR TDD 基本配置为：2.5ms 双周期，特殊时隙配比 10：2：2，下行采用 4 流 256QAM，上行采用 2 流 256QAM；FDD 基本配置为：单载波 20/50MHz，下行采用 4 流 256QAM，上行采用 2 流 256QAM。

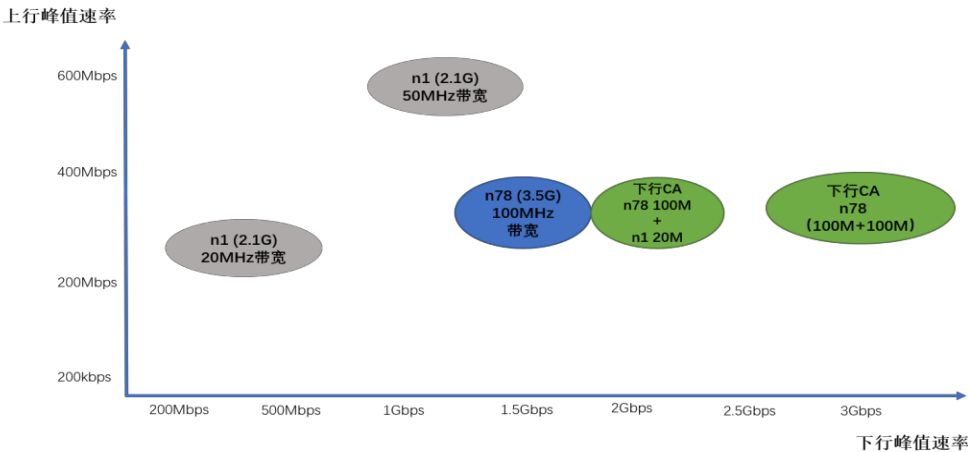


表 B.2 n1 以及 n78 频段上下行峰值速率 (SA 组网)

注：如果专网在 3.5GHz 段上采用了与公网不同的帧结构，那么相应的专网终端、专网模组也可进行定制。对于其他的时隙配比、调制机制、带宽容量的情况下，5G 专网终端的上下行峰值速率会有相应的表现。