



中国联通 5G 智慧新安防 业务发展白皮书

中国联合网络通信有限公司网络技术研究院

2019 年 6 月



前言

中国联通 5G 智慧新安防业务发展白皮书是以 5G 网络技术发展为驱动，探索公共安全创新业务应用发展为目标，分别就安防产业现状及未来发展趋势、运营商机遇、5G+新安防典型创新业务及 5G 网络解决方案等内容进行逐一阐述解读。

本白皮书是与广大产业界合作伙伴共同努力的成果，联合撰写企业及单位主要包含（按字母顺序排序）：

安徽清新互联信息科技有限公司

华为技术有限公司

杭州海康威视数字技术股份有限公司

上海翊视皓瞳信息科技有限公司

苏州博众机器人有限公司

目录

前言	2
1 安防产业发展现状、趋势及业务发展的新需求	4
1.1 安防产业现状	4
1.2 安防产业发展趋势	4
1.3 安防产业业务发展的新需求	5
2 5G 网络对安防产业的价值及运营商机遇	7
2.1 5G 网络核心特征	7
2.2 5G 网络对安防产业的价值	7
2.2.1 大带宽能力及对安防业务的支持	7
2.2.2 高可靠低时延能力及对安防业务的支持	8
2.2.3 海量连接能力及对安防业务的支持	8
2.3 运营商机遇	8
3 5G 智慧新安防应用及典型业务分析	10
3.1 安防行业应用分类及典型业务	10
3.2 典型业务分析	13
3.2.1 5G 无线固定视频监控	13
3.2.2 5G+安防机器人	15
3.2.3 5G+AR 可穿戴设备	18
3.2.4 5G+车载安防	21
3.2.5 5G+临时布控球	23
3.2.6 5G+无人机	25
4 5G 新安防关键网络技术	27
4.1 新安防对 5G 网络的诉求	27
4.2 5G 网络切片	27
4.2.1 5G 网络切片概述	27
4.2.2 安防业务网络切片隔离方案	29
4.2.3 安防业务网络切片可靠性保障方案	30
4.3 5G MEC	31
4.3.1 中国联通 MEC 概述	31
4.3.2 MEC 助力智能安防	33
4.4 5G 网络安全	34
4.4.1 安防业务安全诉求	34
4.4.2 5G 网络安全目标	35
4.4.3 5G 网络安全策略与架构	35
4.4.4 安防业务 5G 网络安全方案	37
5 5G 时代运营商在安防行业的商业模式分析	39
5.1 安防行业的市场分析	39
5.2 5G 时代运营商在安防行业的商业模式	39
6 总结与展望	40

1 安防产业发展现状、趋势及业务发展的新需求

1.1 安防产业现状

城市化进程的加快给全球城市带来了基础设施、资源和安全方面的巨大压力，各种自然灾害、事故灾难、公共卫生事件和社会安全事件不断发生，给广大人民群众的生命、财产带来巨大的损失；同时人民群众日益增长的物质生活水平要求能够及时对各种公共安全事件进行检测、监测、预警、防护和应急处理，从而提供安全保障。为此，国家出台了一系列政策，推动安防市场的快速增长。在国家政策的驱动下，我国安防产业始终保持高增长态势。根据前瞻产业研究院发布的《中国安防行业市场前瞻与投资战略规划分析报告》统计数据显示，截止至 2017 年底，我国安防行业总收入增长至突破 6000 亿元，年均增长 14.4%，预测在 2020 年我国安防行业总收入将突破 8000 亿元。

从安防市场整体情况来看，视频监控产品占其比例在 50%左右，2014-2016 年期间，视频监控在安防产品应用中的比例分别为 47.06%、48.33%和 50.63%。根据《安防行业“十三五”展望》数据，预计“十三五”期间我国视频监控市场年增长率将达到 15%左右的水准，即到 2020 年我国视频监控市场规模有望达到 1600 亿元以上。而随着人工智能、云计算、网络技术等新兴技术的日渐成熟，视频监控行业将进入重新洗牌的过程，用户对平台软件以及软硬件设备兼容性的需求将会增加，安防已不再仅仅是对设备和服务的需求，而是对整体解决方案及服务的需求。

1.2 安防产业发展趋势

得益于图像处理及编码技术的发展，公共安全视频摄像头不断升级，已经由标清向着高清、超高清的方向发展。在视频监控领域，人们不再满足于“看的见”，而希望能够“看的清”。随着 AR、VR、全息技术在视频监控领域中的应用，人们对视频图像高清化的需求日益彰显。而视频图像的高清化为实现智能化的视频监控提供了重要前提。近些年来，由于深度学习算法的突破以及硬件计算能力的提升，AI 技术被引入公共安全监控领域，使得公共安全监控被赋予了“大脑”，变得更加智能。图像清晰度的提高，可以获取更多关键性的细节，从而大大提高智能视频分析的精度，为智能监控的实现奠定坚实的基础。当前中国的安防行业正加速向高清智能化发展。

传统的智能安防项目以前端处理为主，而高清视频的前端存储以及 AI 的前端分析将会对监控设备的性能提出极高的要求，从而大大增加了前端设备的投入成本；并且大量的前端存储，也加重了前端的负担，使得前端变得笨重、易于发热且耗电快。一些安防厂商逐渐倾向于采用“前端+后端”结合的方案，例如，在前端摄像头采用一些专用的智能算法，实时对一部分视频数据进行结构化处理，而把大容量的公共安全监控数据存储以及更复杂的智能分析放在后端系统实现。随着网络带宽的大幅增加，在安防领域，前端轻量化将会成为趋势。

随着平安城市、雪亮工程等项目在全国范围内的开展，安防产业已逐步从公安、政府等专用领域普及到了各个民用、家用领域。视频监控项目建设规模的与日俱增，带来了海量的视频数据。如何有效存储这些海量数据，如何从海量数据中深度挖掘有价值的信息，如何保障存储数据的可靠性，这些变得十分重要，于是，在后端催生了对云的需求。云计算具有强大的运算能力，能够实现海量级的规模效应和弹性扩展，进行海量数据的挖掘与分析，不仅节省了企业私有的存储空间，而且有利于跨区的搜索。伴随互联网数据的积累、云计算大数据平台技术的成熟应用，越来越多的企业将会产生上云的需求。而对于一些对时延要求较高的应用，边缘计算将会大行其道。因此，“云边协同化”已成为越来越多安防企业的共识，将会在未来的安防解决方案中大放异彩。

未来，“高清智能化”、“前端轻量化”、“云边协同化”将成为安防产业发展的趋势。

1.3 安防产业业务发展的新需求

相对于有线网络而言，无线网络无需布线安装，免去了安装布线的工序和成本；系统组网灵活，缩短了网络建设周期，特别适用于临时、突发性的活动现场；对于一些无法铺设有线网络的场合，无线网络几乎不受地域的硬性限制，是唯一的选择；而且，无线网络的终端平台可以随时随地打开，满足了用户对监控实时性、方便性、灵活性等的需求。因此，在公共安全网络建设上，无线接入将成为不可或缺的重要组成部分。但是，面对安防产业的高清化、智能化、大连接的发展，当前的 3G、4G 网络还无法满足行业对承载网络的性能需求。例如，对于高清视频监控数据的传输，尤其是 4k 以上高清视频的传输，需要网络提供大带宽的支持；针对移动视频监控速率高、时延短的特点，需要网络提供大带宽和低时延的支持；针对应急指挥调度的及时响应和高可靠性的特点，需要网络提供低时延、端到端 QoS 的支持；针对海量监控设备的智能化监控，面临着城市间亿万节点的多元

数据收集与传输的难题，需要网络提供大连接的支持。因此，在安防领域需要引入一种新的无线网络架构来有效解决 3G、4G 网络传输层面的系列问题。

2 5G 网络对安防产业的价值及运营商机遇

2.1 5G 网络核心特征

5G 网络是第五代移动通信网络，相比 4G 网络，5G 网络数据流量密度提升 1000 倍，设备连接数目提升 10~100 倍，用户体验速率提升 10~100 倍，端到端时延降低 5 倍，可以为无线网络用户提供 1-20Gbps 的极速体验速率、毫秒级的超低端到端时延以及每平方公里一百万的连接数密度与数十 Tbps 的流量密度。5G 网络具有大带宽、低时延、海量连接、低功耗的特点，使人与人之间通信，开始转向人与物的通信，直至机器与机器之间的通信，从而为社会经济、生活带来革命性的影响。截至 2018 年 11 月，全球已有 182 个运营商在 78 个国家进行了 5G 试验、部署和投资。我国宣布将在 2019 年开始 5G 试商用，2020 年实现 5G 商用。5G 网络寄托了整个移动互联网产业链未来的希望，可以深度赋能安防产业，满足安防产业的需求。

2.2 5G 网络对安防产业的价值

2.2.1 大带宽能力及对安防业务的支持

近些年，随着大数据、AI 等前沿技术的成熟，安防业务对视频清晰度要求的逐渐提升，安防摄像机从最开始的标清摄像机，发展到准高清的 720P、高清的 1080P 摄像机，直至现在的 4K、8K 超高清摄像机。而随着视频清晰度的提高，视频传输对网络带宽的要求也越来越高。例如，对于采用 4096*2160 分辨率、H.265 视频编码的单路 4K 视频，其带宽速率需求为 10-20Mbps，而对于采用 8192*4320 分辨率、H.265 视频编码的单路 8K 视频，其带宽速率需求约为 40-60Mbps。对于一些 AR、VR、超高清视频等新型移动业务，4G 网络已经不能满足需求，而 5G 网络所具备的大带宽能力将能够以更快的速度提供更加高清的监控数据，而清晰度更高的画面与更丰富的视频细节将使得视频监控分析价值更高。

2.2.2 高可靠低时延能力及对安防业务的支持

5G 网络有着毫秒级别的延迟，其意味着更快的响应速度，这对于 VR/AR 安防、移动巡检、应急事故处理等场景意义重大。通过毫秒级低时延 5G 网络，可以实现对无人机/机器人的远程敏捷控制，高效完成巡检任务；对于 VR/AR 场景，VR/AR 产品时常会使体验者产生眩晕感，这一定程度上是因为时延的原因，而 5G 的低时延特性可以有效解决这一问题。5G 低时延的实现，一方面要大幅度降低空口传输时延，另一方面要尽可能减少转发节点，并缩短源到目的节点之间的距离，例如，可以在网络架构方面，通过采用 SDN 和 NFV、网络切片、核心网功能下沉和移动边缘计算（MEC）等关键技术来降低时延。

2.2.3 海量连接能力及对安防业务的支持

IoT 设备的广域物联网设备预计到 2023 年达到 41 亿个，而在短程物联网设备的连接量将达到 157 亿个。5G 所具备的海量机器类通信（mMTC）特性将带来海量的设备连接量，使得安防监控范围进一步扩大，监控数据的获取将更加丰富，这将能够为智能安防云端决策中心提供更广泛、更多维度的参考数据，从而能够更全面地进行分析判断，做出更有效的安全防范措施。5G 的海量连接特性将会再设备的状态监控、资产的跟踪以及物联网和库存监控方面具有重要意义。

2.3 运营商机遇

5G 网络所定义的 eMBB（增强移动宽带）、uRLLC（高可靠低时延通信）、mMTC（海量机器类通信）的三大场景与安防行业未来新型业务的发展方向相吻合，可以通过边缘计算（MEC）技术满足敏捷连接、实时业务的需求，通过网络切片技术提供精细化的 QoS 保障。基于 5G 网络，能够为超高清视频传输、应急指挥调度、无人机/机器人巡检、AR 安防、临时应急布控等多种安防行业应用场景提供保障。运营商具有丰富的网络资源与通信基础设施，同时具备平台建设和维护经验，掌握丰富的大数据资源，特别是伴随 5G 网络建设，核心网向 SDN/NFV 方向演进，网络不再仅仅单纯作为管道，而是能够为行业提供按需服务，将 5G 网络与业务深度融合，从而更好的赋能客户。

目前，政府、企业开展“平安城市”、“蓝天卫士”、“国土卫士”、“名厨亮灶”等

一系列安防业务，以提升民生政绩及企业品牌，一方面为运营商带来对 5G、SDN、NFV 等新型网络建设以及服务的市场空间，另一方面为运营商深度参与行业市场，实现通信技术与行业特定场景融合，带来数据服务、平台服务以及运营服务等提供广阔发展空间。5G 时代的到来、安防市场的繁荣，将为运营商带来巨大的发展机遇。

3 5G 智慧新安防应用及典型业务分析

3.1 安防行业应用分类及典型业务

根据维度的不同，可以对安防行业应用进行不同的分类。

按照应用场景的业务领域，安防行业应用场景可以分为平安城市、社区/园区安防、大型活动/赛事安防、警务安全、生态安全、消防安全、交通安全、食品安全等大类。

应用场景分类	典型业务
平安城市	1: 城市视频监控 2: AR 单兵可穿戴式巡检 3: 机器人巡检 4: 警务车巡检 5: 手持执法记录仪巡检 6: 施工场地视频监控 7: 智能路灯杆 8: 井盖、水位（防汛）、垃圾箱（防恐）、城市管网监测等物联网应用
社区/园区安防	1: 人员、车辆视频监控 2: AR 单兵可穿戴式巡检 3: 机器人巡检 4: 园区巡检车 5: 高清执法记录仪
大型活动/赛事安防	1: 人员、车辆视频监控（卡口、场馆内外.....） 2: AR 单兵可穿戴式巡检 3: 机器人/无人机/警用车巡检 4: 警务车巡检 5: 应急布控（临时布控球.....）

	6: 高清执法记录仪
警务安全	1: 视频监控（人脸比对、车牌识别……） 2: AR 单兵可穿戴式执法 3: 警用机器人/警务车巡检 4: 无人机巡检/追踪 5: 单兵执法（高清执法记录仪……）
生态安全	1: 蓝天卫士（秸秆焚烧视频监控） 2: 国土卫士（工地扬尘、耕地燃烧秸秆视频监控） 3: 机器人巡检（输电线路监控、石油管线监控等） 4: 无人机水域/山区巡检 5: 森林/山区/水源视频监控 6: 无人船巡检 7: 污染源监测、水质监测等物联网应用
消防安全	1: 森林防火视频监控 2: 消防无人机巡检及灭火 3: 机器人消防设施巡查 4: 物联网消防远程监控（智能烟感器、智能消防栓、电气火灾监测、消防电源监测……）
交通安全	1: 道路视频监控（车辆识别……） 2: 视频违章抓拍 3: 无人机道路巡查/事故救援 4: 地铁/公交/机场/火车站的视频监控 5: 交警 AR 实景巡逻
其他安防场景	店铺安防：小微用户安防

	电力安防：高压线/电力塔/电箱监测 医疗安防：病房/药房安全管理及冷链 食品安全：明厨亮灶/餐厅视频监控 教育安防：校园/看护所/幼教视频监控、智慧校车 金融安防：自助区视频监控、人脸识别、人证比对 旅游安防：景区视频监控、文物古迹监管 司法安防：服刑帮教探视、监狱智能监控
--	--

按照对 5G 通信网络的需求，安防行业应用场景可以分为大带宽类、低时延高可靠类、海量连接类。

应用场景分类	典型业务
大带宽类	1：固定高清视频监控 2：AR 安防眼镜/头盔巡检 3：VR 实战化培训 4：机器人/无人机巡检 5：车载视频监控
低时延高可靠类	1：机器人/无人机巡检 2：手持单兵执法 3：应急布控（临时布控球……） 4：应急机动指挥通信（应急通信车……）
海量连接类	危险物品监控、重要物资监控、垃圾处理监测、可燃物排放监测、有毒气体排放监测、医疗废物监测、疾病预防控制监测、水灾火警监测等物联网应用

3.2 典型业务分析

3.2.1 5G 无线固定视频监控

3.2.1.1 业务概述

目前，监控摄像头一般采用光纤回传，面临埋纤成本高、部署周期长、检测维护困难等问题，随着无线网络的普及和带宽提升，无线监控未来将很大程度取代有线监控，尤其是在无无线网络覆盖区域，或者周期性更换地点的环境，无线监控逐渐成为趋势，各种形态的无线摄像机（枪、球、高速云台机等）琳琅满目。在电力、矿山、油田、雪亮工程、乡镇监控中，无线监控已成为主流。

在 4G 时代，数据带宽初步满足了监控的需要，带宽提升到了 1-5M 左右，无线监控得到了较快的发展，但相较于有线网络，带宽不足、覆盖不广、网络不稳定、资费贵，仍然限制了无线监控的应用。相比 4G，5G 速率提高 8-10 倍，无线网络的带宽将达到百 M 级别，实际应用也将达到 10M 以上。目前视频监控的清晰度主流集中于 1080P-4K，在 H.265 编码方式的日趋成熟下，5G 已能较好满足移动监控的网络要求，能够支持高清视频回传。

未来，随着无线接入侧带宽水平的提升，视频传输质量有望进一步提升，无线监控质量将由 4K 提升至 8K，达到和有线监控同质量要求水平，且随着 5G 网络的大规模铺设，未来资费有望大幅度下降；随着 AI 处理芯片的发展，越来越多的智能分析将由云端转移到边缘，并由 5G 实现数据连接与结果输出，从而形成边缘计算、云端汇聚的云边结合模式；随着网络的发展，网络能传输的数据越来越大，视频数据越来越丰富，视频将有平面化向立体化发展，未来通过视频所看到的人、物可以是 3D 化的，指挥中心将成为一个全景信息接收与展示平台。

3.2.1.2 业务功能设计

（1）视频传输：该功能为移动监控的核心应用。无线监控终端将采集的视频编码后，通过无线网络，实时回传到后端平台，管理人员通过多种客户端方式登录平台，获取监控终端现场的实时图像，第一时间了解现场情况，获取最快速、最宝贵、最真实的现场

资料，对于后续的处置，起到重要的资料辅助作用。在视频传输的应用中，涉及多种具体细节性功能，比如：分辨率设置、云镜控制、视频存储、视频分发、视频转码等。

(2) 定位：无线监控在实现了视频监控、语音交互的基础上，需要对目标进行位置确认，具体功能主要包括：当前位置、历史位置、速度、方向以及周边控制应用包括超速、超阈、偏离路线等功能应用

(3) AI 应用：包括人物识别、车辆识别及报警等。

3.2.1.3 网络需求

无线视频监控与其他移动网络的应用不同，监控点需要长时间应用，单位时间内对带宽的占用高，流量巨大。以下列出了不同类型的视频传输业务对网络带宽的需求。

视频业务带宽需求

视频类型	720P	1080P	2K	4K	8K
分辨率	1280*720	1920*1080	2048*1080	4096*2160	8192*4320
压缩算法	H. 264	H. 264/H. 265	H. 264/H. 265	H. 264/H. 265	H. 265
带宽需求	1Mbps	2-4Mbps	4-8Mbps	10-20Mbps	>40Mbps

3.2.1.4 可应用场景

目前无线固定监控主要应用在光纤网络造价高、监控分散、位置可能产生变动的区域，应用场景包括：

- 1) 电力线、电力塔等监控
- 2) 旅游景区、建筑工地等监控
- 3) 乡镇道路监控
- 4) 水利、矿山等无人值守监控
- 5) 森林防火、水源、河流资源管理的远程无线监控;
-

未来，随着 5G 网络的兴起，无线网络的普及，目前固定有线监控的应用场景，都有可能成为无线监控的应用场景。

3.2.2 5G+安防机器人

3.2.2.1 业务概述

随着科学技术的发展，机器人正加速进入国防、公共安全等各个部门，产生了积极的社会和经济效益。特别是近年来，随着安防、人工智能和移动机器人等技术的提高，以及移动通信网络、云计算等基础设施的完善，安防机器人的技术水平不断提高，相关产品日渐成熟。因此，国内外警察部门都开始在重大活动安保任务中试点使用安防机器人。

安防机器人的种类很多，可以分为监控类机器人、智能巡检机器人、侦查类机器人、排爆类机器人和武装打击机器人。

（1）监控类机器人：此类机器人能够提供更加全面的安全监控服务，它们不仅是家庭好帮手，同时在工业、公司、网吧、电力环境监控、化工远程操控等场所都有广泛的应用。

（2）智能巡检机器人：此类机器人主要携带红外热像仪和可见光摄像机等检测装置，可将画面数据传输至远端监控系统，其中增加了运行中的事故隐患和故障先兆功能，可进行自动判定和报警。由于智能巡检机器人在环境应对、性能强大等方面具有人力所不具备的特殊优势，其被广泛应用到安防巡检等特殊场所。

（3）侦查类机器人：此类机器人必须拥有智能敏捷的“身手”，通过安装控制装置可以在山地、陡坡等多种地形实时传送文图和语音信息，主要用于对敌目标探测、识别等。

（4）排爆类机器人：此类机器人是一种遥控装置，可以自动行走，并带有机臂进行各种排爆作业。它替代人接近可疑物，进行爆炸物识别、转移和销毁等作业，能够通过有线和无线操作进行控制，有跨越一定障碍的能力。

（5）武装打击机器人：此类机器人一般具备监控、侦查、子弹打击等功能，主要应用于反恐行动中。

安防机器人近年来的发展体现了如下的发展趋势：解决方案系统化、平台模块化、功能智能化和布控快速化。未来，随着 5G 网络的成熟，安防机器人的功能智能化和布控快速化的

3.2.2.2 业务功能设计

安防机器人可以实现对环境、人员、车辆、意外事件等要素的信息感知，在服务人民群众的同时有效保障安全。为此，安防机器人具备的主要功能包括：人脸抓拍，实时比对；夜间巡逻，红外感知；精确定位，精准导航；自主巡逻，智能避障；实时监控，信息回传；远程控制，人机交互。

结合具体应用场景和实战要求，安防机器人系统划分为四个方面：

1. 任务部署系统，通常是装备指控平台和机器人本体的指挥车，方便将机器人本体快速部署于任务现场。
2. 数据操控指挥平台，实现机器人编队控制，警务功能信息汇总的信息平台系统。
3. 安防机器人本体，执行安防任务的机器人平台，包括移动平台载体和警务功能模块。
4. 安全的网络通讯系统，实现机器人本体与数据操控指挥平台的数据互联。



图：安防机器人的重点技术方向

在硬件配置上往往需要云台变焦相机、双向语音对话、语音和视频传讯功能、蜂鸣、爆闪灯、远光灯和示廓灯等。

3.2.2.3 网络需求

在安防机器人应用中，目前网络多使用 Wi-Fi 或者 4G 网络驱动。而 WIFI 和 4G 网络在以下几个方面会存在问题：

(1) 网络服务质量保障差：安防机器人是传感技术、人工智能以及互联网技术的典型融合应用，需要借助无线网络连接支撑以实现远程可视化监控以及人机协同作战能力。对于

当前 4G 网络架构，传统网络设备硬件和软件紧耦合，难以为特定业务应用提供服务质量保障，致使应用感知较差，难以满足业务真是诉求。

（2）无法实时监控：安防机器人搭载多路高清摄像头，对网络传输的上行带宽及传输时延要求较高。目前，4G 网络带宽不足以支撑安防机器人的实际业务应用，无法实现多路高清视频的实时回传需求。

（3）移动性差安全性弱：安防机器人采用 Wi-Fi 作为备选无线连接方案可实现视频实时回传的业务需求。但由于 Wi-Fi 不具备大范围覆盖能力，大幅限制了移动机器人的巡检能力。另一方面，由于 WiFi 加密方式有很多不安全因素，难以满足移动安防的安全接入要求。

5G 作为新一代移动通信技术发展的主要方向，利用 5G 网络支持的增强型移动宽带（eMBB）、大规模机器通信（mMTC）、高可靠低时延通信（uRLLC）三大特性，不仅可以大幅提升移动警务高带宽业务的体验，其低时延、高可靠的网络特性更契合机器人安防应用的网络诉求。主要体现在以下几个方面：

（1）灵活的差异化服务质量保障机制：5G 网络引入 SDN/NFV 技术，通过网络控制平面与用户平面的分离，将有效的根据业务需求实现硬件资源的动态配置和高效调度，最终可实现业务应用的差异化服务质量保障。

（2）高效的传输和时延保障能力：5G 具备高性能、低延迟与高容量特性，将可有效的提供传输和时延的保障。

（3）安全保障：5G 网络未来将引入网络切片能力，可为行业客户提供差异化的安全服务，形成专业的高安全切片，满足业务应用的安全需求。

3.2.2.4 可应用场景

安防机器人可以用于园区安防、工厂巡检、大型活动/赛事巡检等场景中，主要应用包括：

- （1）实现对巡逻范围内犯罪分子、重点人员的识别、定位、报警和跟；
- （2）协助实现人员密集区的指引、疏散、排查和便民问答；实现便民服务；
- （3）实现警务大厅的便民服务，包括公安业务问答、窗口导引、业务自主办理；等。

3.2.3 5G+AR 可穿戴设备

3.2.3.1 业务概述

随着警务安防工作范围不断扩展和复杂化，对于公安以及警务等政府相关部门来说，如何实现公安/警务系统的智能化、提高警员工作效率就显得尤为重要。增强现实（AR）与安防行业结合，可以使执法人员通过音视频信息采集，多警种信息深度融合，辅助情报研判，实现联动指挥。目前的 AR 设备大多在前端进行 AI 处理，导致计算量低，设备发热量大、使用时间短、体积大、造价高等问题，5G+AR，利用 AR 的先进技术，结合 5G 环境的大带宽、低时延的技术支撑，尤其是 5G 网络边缘云的技术，将极大的减轻前端负载，增强前方 AR 设备佩戴人员巡检的便利性；安防人员通过佩戴 AR 设备，随时走动执行任务，可以在真实空间中看到实时叠加的 3D 或全景的现场信息，使得很多事后查证的场景将向事前预警前移，从而创造更多事件预防价值，最终推动整个安防产业的持续繁荣发展。

目前针对安防领域的不同情景所应用的 AR 智能眼镜产品也不大相同：未来可应用于高级别安防场景的多功能智能警用头盔；应用于安防全场景的便携式智能眼镜；应用于刑侦场景的隐蔽式智能眼镜以及应用于战备场景的头盔结合式眼镜。



图：AR 可穿戴设备的各种形态

3.2.3.2 业务功能设计

5G+ AR 可穿戴设备，能够实现前后端音视频交互、AI 智能比对、AR 显示操作等功能。其业务功能主要有：

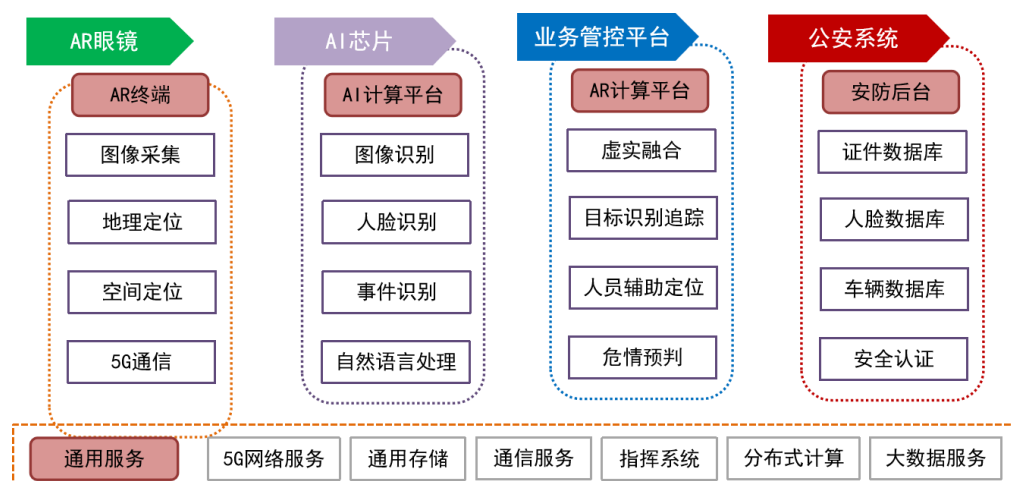
视频采集，巡检人员佩戴专用的 AR/MR 巡检头盔或眼镜，进行巡检，头盔或眼镜的高清视频采集摄像头实时采集巡检人员的第一视角画面，并将所采集到的视频信息进行结构化处理后通过 5G 网络传到云端或 MEC 边缘服务器进行人脸识别；

AI 识别，识别分析系统能够对视频流和图片进行快速解析，提取出人脸、车辆等信息，实时与行业用户业务系统各种数据库进行比对，产生判断结果并最终在 AR 设备实现渲染，全面提升事件处理的效率和质量；

AR 功能，实时地计算摄像机影像的位置及角度，并实时叠加相应文字/图像/视频/3D 动画模型等信息技术。

现场指挥，采用高清摄像头，实现第一视角记录，为远端指挥中心实时了解现场情况，进行决策提供保障；远端指挥中心的可视化指令通过 AR 设备直接传递到前方人员，实现远程指挥调度。

其他功能，还可以通过增加记录取证\语音对讲、实时翻译、直播等功能，实现智慧新警务场景的应用需求。



图：5G AR 可穿戴设备功能架构

3.2.3.3 网络需求

AR 技术对社会的各个行业产生了很大的影响，过去的 AR 产品因为带宽和延时的因素导

致传输能力受限、交互互动体验不强和终端移动性差等问题，致使 AR 应用一直不能得到很好的推广。例如，在 AR 的体验中，由于时延问题，会让人产生现实与信息叠加不及时的问题。而要解决当前 AR 延时问题，一般需要网络时延稳定至少保持在 10-50 毫秒之间，对于 AR 来说要达到不错的用户体验需要稳定的 50Mbps 以上的带宽和 ms 级的延时，这在 4G 时代是无法实现的，唯有 5G 能满足这样的高速传输能力。

AR 用户体验对网络带宽和时延的要求

用户体验级别	带宽	时延
一般	5Mbps 以上	小于 100ms
较好	20Mbps 以上	小于 50ms
极好	50Mbps 以上	小于 5ms

3.2.3.4 可应用场景

AR 安防眼镜可用于执法、作业监管、案情模拟、应急救助等场景中，主要包括：

- 1) 警务场景（公安执法监管、安保维稳、天网防控、实战演练）；
- 2) 政务场景（国土、水利巡查、城建管理）；
- 3) 消防、交通事故等应急救援场景。

3.2.4 5G+车载安防

3.2.4.1 业务概述

车载监控系统为社会文明发展、社会和谐和人民出行安全起到十分重要的保护作用。在车载视频监控中,由于车辆不停的移动,无线通信网络传输成为唯一的选择。在 2G-4G 时代,网络技术还不能达到超高清视频的要求,而随着 5G 时代的到来以及云计算、AI 技术的发展,车载无线监控的发展趋势正朝着高清化乃至超高清化、智能化、云储存化的方向发展,同时,5G 网络的边缘云技术,保障了后端处理的实时性,拓宽了车载视频监控应用的范围。5G+车载安防通过在车辆安装车载视频监控系统,实现实时抓拍人脸、违法行为等,借助于 5G 网络的高带宽、低时延特性,传输高清视频,结合后端 AI 能力,实现应急指挥、融合调度,实时处置突发事件,从而为公共安全保驾护航。

3.2.4.2 业务功能设计

车载移动布控的业务功能根据车辆属性的不同,有较大区别:

一类是大型客运车辆,其主要业务功能有:一、过程记录,对车辆运输过程中全程录像,实现全程有据可查;二、事件监测与预警,对驾驶员超速、疲劳驾驶、夜间开车等行为进行监测并向驾驶员和后台发出预警;三、运营规范管控,对高速停车、中途停车载客、异常区间停车、路线偏离、赖站、跳站等运营行为进行监管,后端人员可以通过 5G 网络实时获得监控录像并与驾驶员进行实时交互。

二类是执法车辆/船舶,其主要业务功能有:一、过程记录;二、信息采集,在车辆/船巡逻过程中,智能采集过程中的人、车、船信息,实现人脸识别、身份证/护照核验、车牌识别等,并与执法基础库进行实时比对,能够现场发现嫌疑目标并进行甄别;三、指挥联动,指挥中心人员在获得视频信息后可以与前端人员进行交互,实现远程指挥,多方联动,事故快速处置等。

三类是小型运营车辆,其主要业务功能有:一、过程记录;二、信息比对,对驾驶员进行信息比对,确保人证车证合一,保护乘客安全;对乘客进行身份信息收集,并实时上报基础库;三、对跨区域、偏远地区驾驶等异常行为进行预警。

3.2.4.3 网络需求

随着对车载监控视频传输的高清化需求的提升，车载视频监控对网络大带宽的需求也日益强烈；同时，为了提高前后端交互的实时性以及联动指挥的效率，车载视频监控需要网络具有低时延的特性；车载终端随时运动、基站切换频繁，造成了视频无线网传的不可确定性，为了提升车载视频无线网传的效果，需要网络能够提供无缝切换的特性，保障较小的网络抖动。

3.2.4.4 可应用场景

- 1) 警用车的执法、巡逻；
- 2) 石油化工的危险品车辆监控；
- 3) 金融押运车的监控；

3.2.5 5G+临时布控球

3.2.5.1 业务概述

当紧急事故发生时，临时布控球设备可作为应急处置时重要的信息采集来源，设备可拉杆箱携带，随时随地，移动部署，快速完成架设，且可避免不必要的投资；配合应急通信手段，将现场采集的高清视频通过 5G 网络进行实时回传及本地存储，指挥中心在后端能够对现场实际情况全方位掌握，当发现突发情况是也可以通过布控设备进行喊话提醒，提高了指挥调度的效率；设备布设灵活，可自动升降桅杆，远近高低全覆盖，实现无死角快速布防。

3.2.5.2 业务功能设计

临时布控在安防应用中包括前端感知采集设备、后端存储计算设备、软件业务平台几种形态。前端设备可以为枪机、球机、筒机、布控球、针孔摄像机、摄录一体机以及全息摄像机等；后端设备可采用 NVR；软件业务平台可为视频监控综合应用管理系统。

其中临时布控球可在任意人流密集场所（例如公交车、车载、机场）定点或者车载移动部署，前端设备通过 5G 网络把现场的图像、声音实时传到后端，后端可以通过 AI 技术进行大库比对，进行人脸识别、特定行为识别等，从而进行报警，也可以通过指挥中心与现场进行语音交互或可视化交互，实现远程指挥；前端设备可支持定位功能，录像和抓拍的照片均可叠加定位信息。

3.2.5.3 网络需求

临时布控由于其主要应对的是一些突发、应急场景，因此其对高清乃至超高清视频、图像的传输以及网络时延的需求比无线固定布控更为迫切。

3.2.5.4 可应用场景

5G+临时布控球可用于临时卡口布控、重大活动周边的高点临时布控等，能够在重大社会活动、演唱会、重大外事活动、领导出行保卫、重大会议等临时或突发事件以及抢险抢修中发挥重大作用，也可用于公安行业的（1）案件侦查、蹲点守候，（2）突发事件、

反恐制暴，（3）隐蔽侦查、跟踪监视，（4）现场勘查视频记录，（5）运用单兵设备进行案件侦查实时记录；交通行业的（1）酒驾稽查现场布控，（2）黑名单拦截布控；等。

3.2.6 5G+无人机

3.2.6.1 业务概述

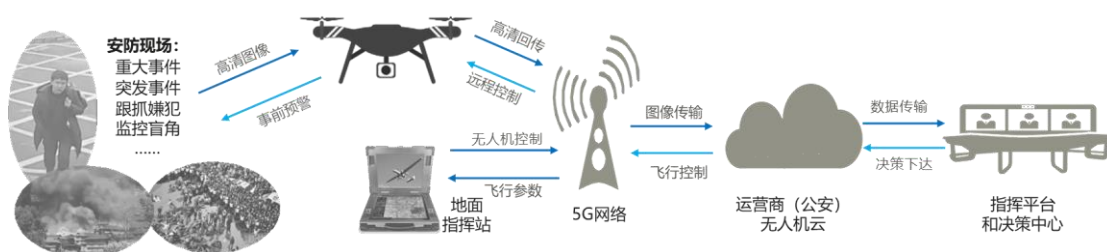
无人机通过搭配不同功能的挂载，可以满足客户的多种需求，在处理自然灾害、事故救援以及社会安全事件等方面发挥出重要作用。随着无人机技术的逐渐成熟，无人机系统也从单纯的航拍系统发展为多功能应用平台，即无人机在除了搭载相机之外，还可以携带喊话器、抛投器、气体探测器、探照灯等各类多功能挂载以完成不同的行业任务。特别在一些紧急任务中，仅通过人力往往难以及时到达目的地，工作人员作业时也可能存在安全风险，无人机可实现空域高点视频回传，具有快速、高效、灵活的调遣能力，除此之外，使用无人机替代人工作业更具备安全性。

通过 5G 联网无人机，可以实现更大范围安全飞行（一般加密 WIFI 控制无人机，不超过 5 公里，而且信号容易被黑客干扰截获）；基于 5G，无人机可支持 4K 以上视频回传，支撑人脸识别等高带宽应用，回传更多情报信息。

3.2.6.2 业务功能设计

无人机系统由飞行器搭载不同的挂载进行现场拍摄或执行特殊任务，现场的图像和数据信息可以通过 5G 实时传到地面站，也可以直接传送到指挥中心平台，提供指挥人员现场信息；同时可以与指挥车结合，将图像信息实时传回指挥车大屏，通过指挥车进行移动指挥。

飞行器可以通过地面站进行手动操控，也可以通过指挥官软件设置航迹路径和其他自动飞行任务。此外，飞行器支持多种挂载，可以通过灵活搭配满足客户的不同需求。



5G 无人机安防业务应用

3.2.6.3 网络需求

4G 网络环境下，无人机到地面站传输视频最高分辨率为 1080P，传输的图像质量不高，而且网络传输不稳定，时延较大。而在安防场景中，无人机需要具有高度的可靠性、及时的进行反应、不间断地进行现场的实时跟踪，同时能够实时回传高清视频用于人眼或计算 AI 的分析识别。5G 的大带宽、低时延的特性将能很好的解决上面的问题。

5G 无人机安防网络指标

视频类别	上行速率	下行速率	业务端到端时延	控制端到端时延	定位精度
1080P	6Mbps	300Kbps	<500ms	<100ms	<1m
4K 高清	25Mbps	300Kbps	<200ms	<20ms	<0.5m

数据来源：IMT-2020

3.2.6.4 可应用场景

5G+无人机业务可用于各种立体监控、智能巡检、突发应急等场景，包括区域巡检、边防巡逻、环境监测、道路巡检、水利监测、港口管理、事故勘察、消防指挥、抢险救灾等。

4 5G 新安防关键网络技术

4.1 新安防对 5G 网络的诉求

随着我国平安城市、智慧园区等各项建设的持续开展，以及各行业用户安防意识的不断增强，视频监控市场一直保持稳定增长。然而，大多数摄像头一直没能摆脱传统人工监控方式，由此导致大量的视频数据堆积、监控实时性差、视频检索困难等问题，一旦有案件发生，海量摄像头带来的检索工作需要耗费大量警力。借助 AI 处理海量监控视频数据成为行业整体趋势，视频监控系统的升级创新不断创造新的市场需求。高帧率、超高清和 WDR（宽动态范围摄像，能够在很差的照明条件下成像），这些特性将产生大量的数据流量。现有的 4G 网络无法满足多路高清视频回传要求，只有通过 5G 网络才能满足超高清视频数据量大、实时性高的要求。

网络整体诉求	典型分辨率	典型帧数	带宽需求	可靠性要求	可维护性
端到端切片保障数据安全性	1080P/2K/4K	30fps	6/15/50Mbps	最小保留带宽，数据隔离	弹性伸缩

通过 5G 一方面可摆脱线缆的束缚进行快速安装和扩展，一方面可提供 4K/8K 及更高清晰度的视频实时传送。不论是采用无线高清视频监控器还是带摄像头的无人机，采集的视频信息即可通过 5G 网络实时回传，并可结合移动边缘计算服务器中进行图像识别、地理信息等数据处理和分析，为监控中心提供预测预警、实时监控、轨迹追踪、快速检索等服务。随着云和移动边缘计算的推出，可以支持更多的人工智能辅助监控应用。摄像机则需要 7*24 小时不间断地进行视频采集以支持这些应用。

4.2 5G 网络切片

4.2.1 5G 网络切片概述

5G 端到端网络切片是指将网络资源灵活分配，网络能力按需组合，基于一个 5G 网络虚拟出多个具备不同特性的逻辑子网。每个端到端切片均由核心网、无线网、传输网子切片组合而成，并通过端到端切片管理系统进行统一管理。

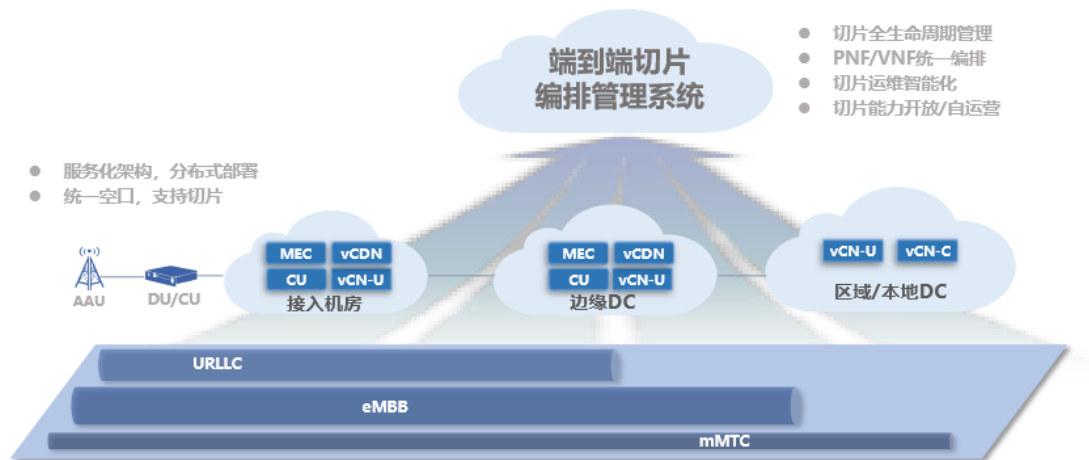
5G 网络切片的概念具有丰富的特征，一般来说认为网络切片是面向租户，满足差异化 SLA，可独立生命周期管理的虚拟网络，是面向特定的业务需求，满足差异化 SLA（Service Level Agreement），自动化按需构建相互隔离的网络实例。网络切片是 SDN/NFV 技术应用于 5G 网络的关键服务。一个网络切片将构成一个端到端的逻辑网络，按切片需求方的需求灵活地提供一种或多种网络服务。5G 网络切片具备了“端到端网络保障 SLA、业务隔离、网络功能按需定制、自动化”的典型特征：

端到端 SLA 保障：5G 网络切片由核心网、无线、传输等多个子域构成，网络切片的 SLA 由多个子域组成的端到端网络保障。网络切片实现多域之间的协同。包括网络需求分解，SLA 分解，部署与组网协同等。

业务隔离：网络切片还需要支持针对公共安全、漫游用户或托管 MVNO 等特定用户提供逻辑隔离的网络，为不同的应用构建不同的网络实体。逻辑上相互隔离的专用网络确保不同的切片之间业务不会相互干扰。并对优先级、计费、策略控制、安全性和移动性等进行功能差异定制。

功能按需定制、动态编排：5G 网络将基于服务化的架构，同时软件架构也将进行服务化重构，以此形成网络可编排的能力。面向不同行业多样化的网络需求，5G 网络可以提供按需编排的能力，为每个应用提供不同的网络能力。同时，5G 网络分布式特点可以根据不同的业务需求部署在不同的位置，来满足不同的业务时延的要求。网络切片需要支持运营商，对时延、移动性、可用性、可靠性和数据速率等网络性能提供差异化定制，例如有些情况需要 5G 系统支持的非常高的数据速率或流量密度，而另一些情况需要支持非常低的延迟和非常高的通信服务可用性。

自动运维、多租户运维：自动化是网络发展的目标。相对于传统网络一张大网满足所有要求，5G 通过切片技术将一张网裂变成多张网，理论上 5G 的繁荣必然会带来运维难度大幅增加，因此自动化是 5G 网络必然要具备的一个特征。从节奏上来说，一次性地实现全自动化非常困难。通过分割网络切片生命周期中各个环节的操作，允许 workflows 中的每个环节都支持人工，半自动或者全自动的方式进行处理，伴随着用户网络规划能力的发展，以及网络的扁平化，简单化，最终达成自动化。网络切片允许向特定租户（比如公共安全行业用户）提供定制化的网络服务，租户对网络具备一定的操作管理能力。租户运维人员所具备的知识与能力模型与传统运营商运维人员不同，需要面向租户的运维人员提供易观察、易操作、易管控的运维界面，实现租户的“自助服务”。



4.2.2 安防业务网络切片隔离方案

网络切片隔离主要包括以下两大维度：公安与其他行业及个人用户通信业务之间的隔离，以及公安自身不同分区业务之间的隔离。针对上述两大维度，可从接入网（含空口、基带、协议栈等）、传输网和核心网三个层面分别定制不同的隔离策略。

(1) 接入网隔离方案

接入网的整体功能分为三个部分，空口 / 射频、基带处理和高层协议栈。

高层协议栈功能具备灵活的隔离架构，既可以完全共享，也可以对不同区域或类型的业务进行按需隔离。

在空口频谱资源的使用策略上，安防业务和运营商网络中的其他业务共享频谱资源，采用相同的上下行配比。所有业务在时域和频域两个维度都可进行动态的按需调度。其中 uRLLC 和 eMBB 可以共享频段，通过不同的物理层参数、调制编码方案、调度方案等达成差异化的时延、可靠性目标。

基于频谱资源共享的前提，接入网的低层设备资源如射频、前传、基带等部分功能与资源也都是共享的。

针对公安业务网络切片中可能存在的紧急保障类需求，可以通过优先接纳、负载控制等技术，优先保障高优先级业务，避免其他切片中的业务影响公安业务的性能表现。

在确有必要的情况下，运营商可以为公安配置特定的抢占策略，以抢占其他优先级更低的切片资源。

(2) 传输网隔离方案

RAN 与 CN 之间的回传网络连接可以用运营商网络，以便达成更好的 E2E 切片配合效果。回传网络的业务切片，根据对安全和可靠性的不同诉求，分为硬隔离和软隔离。

硬隔离基于 TDM 时隙交叉实现，软隔离基于 VLAN 和 QoS 实现，支持灵活的业务区分。通过支持软硬隔离的传输网络切片可以满足安防需求。

(3) 核心网隔离方案

在无线蜂窝网 3GPP 标准中已经明确，核心网在逻辑功能上严格隔离，区分切片，每个切片都有专用的功能。

核心网隔离有两大类方案：物理隔离，如物理服务器安防专用，当有极高的安全需要，可将服务器部署在不同地理位置；逻辑隔离，即安防与其他业务共享硬件服务器、区分虚拟机。

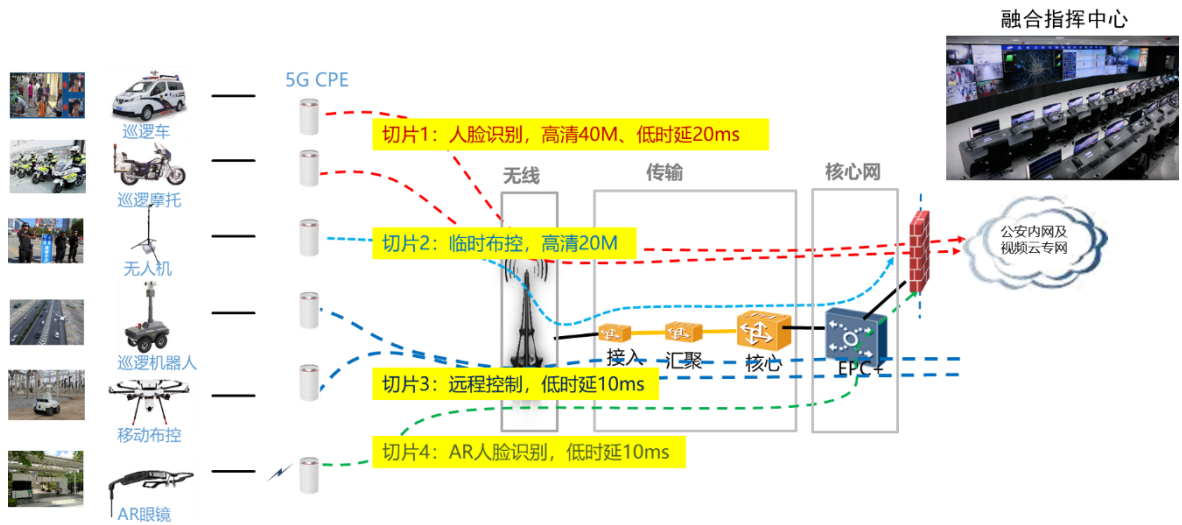
4.2.3 安防业务网络切片可靠性保障方案

公网运营商网络可为关键、核心的安防业务网络切片提供至少 99.99% 的整体网络通道可用度服务，并有多样化的保障机制来满足不同业务需求。

(1) 传输硬管道和主备保护链路：传输为安防业务网络切片提供硬管道，保护业务传输不受其他业务影响，保证业务的带宽和时延等。运营商核心网和回传部分的传输通道可以采用备份机制，基于快速主备倒换技术，支持安防业务在主用和备用通道之间无损迁移。

(2) 故障检测与快速处理：运营商通过部署实时监控技术，针对网络中的多项运行指标进行联合分析，检测不同类别的异常场景，进行故障隔离和快速恢复。

未来 5G 切片技术，在公网上搭建超高速专车道，保障公安等关键业务的安全、无干扰的承载，可按业务需求定制网络特性，并且端到端保障业务 QOS。



4.3 5G MEC

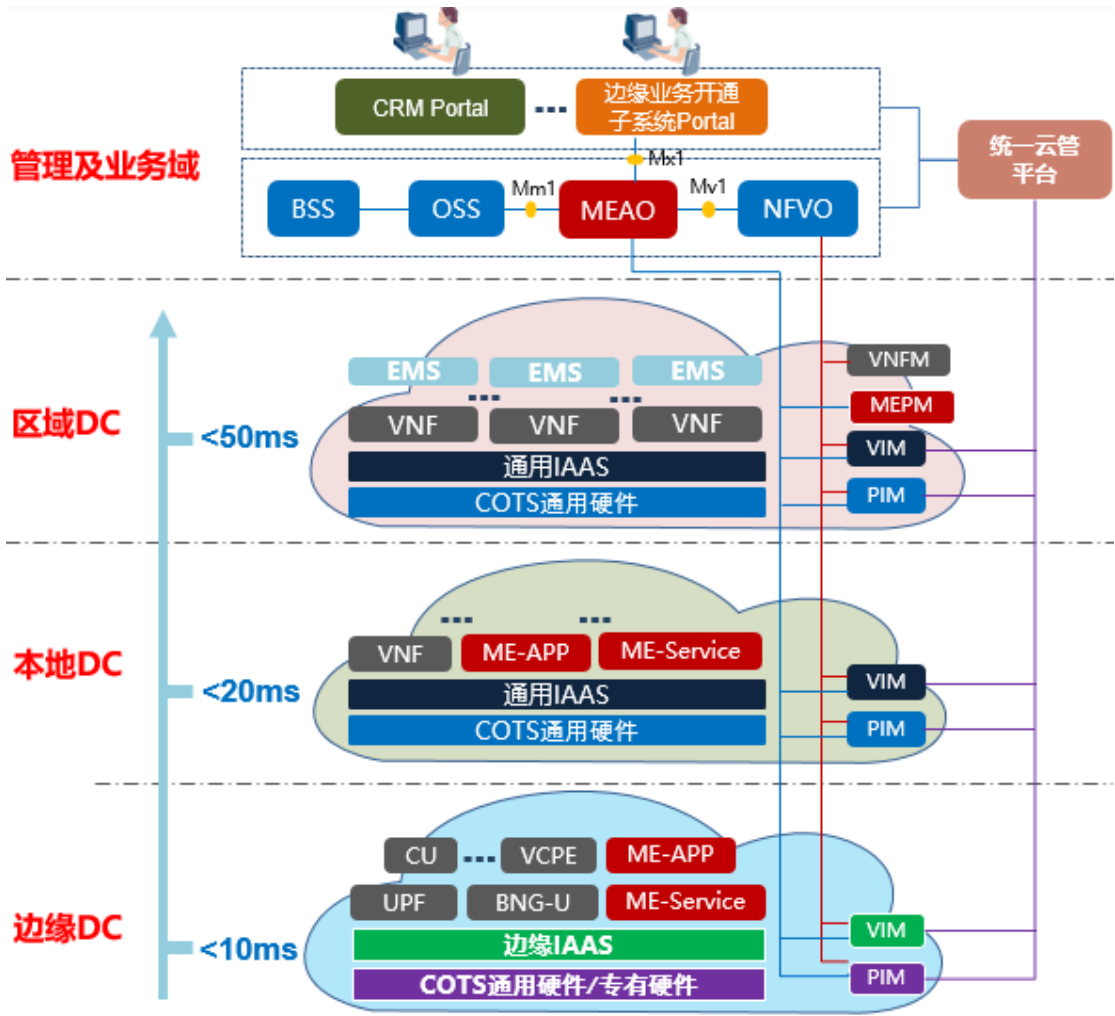
多接入边缘计算技术（MEC）是 ICT 融合的产物，是 5G 网络转型的关键技术，以迎合未来高清视频、VR/AR、智能安防、工业互联网、车联网等业务发展需求。移动边缘计算（MEC）技术通过为无线接入网提供 IT 和云计算能力，使得业务本地化、近距离部署成为可能，促使无线网络具有低时延、高带宽的传输能力，并且回传带宽需求的降低极大地减少了运营成本；MEC 运行在网络边缘，其逻辑上不依赖于网络其他部分，这对于安全性较高的应用非常重要；MEC 服务器通常具有较高的计算能力，特别适合于分析处理复杂数据；同时位于网络边缘的 MEC 能够实时获取例如基站 ID、无线资源利用率等网络数据以及与用户位置相关的上下文信息，从而为用户提供差异化的服务和业务体验；此外，MEC 平台可将无线网络能力开放给第三方业务应用以及软件开发商，从而加速为创新型业务的研发部署。

4.3.1 中国联通 MEC 概述

数以万计的边缘 DC 是运营商相对于 OTT 的绝佳优势资源，使得边缘计算具有广阔的应用空间。中国联通在构建以 DC 为核心的全云化网络基础上打造 MEC 边缘云整体架

构，MEC 边缘云与通信云融合建设，实现三层 DC 的部署架构。按照集约化的部署要求，管理面大区集中，DC 间采用 SDN 组网实现远程配置与管理能力。边缘云与通信云、公有云、私有云互通，实现云边协同能力。

在中国联通边缘云整体布局中，按照集团集约化的建设要求，管理面大区集中，业务面下沉贴近用户，与通信云融合建设，构建三层 DC 架构，如下图所示。



图：中国联通边缘与集约化三层部署架构

区域 DC：部署 MEC 管理面 MEPM 并实现与集团 MEAO 对接，MEPM 管理本大区所有本地与边缘的业务，实现业务的开通，删除以及日常维护。

本地 DC：部署边缘云 CUBE-Edge 平台，满足不同行业的业务需求。边缘云与通信云共 IaaS 平台，边缘云业务纳入到 MEAO/MEPM 进行管理。边缘云提供与公有云、私有云的对接能力，实现云边协同。本地 DC 适合部署 VCDN、AR/VR、视频监控等的广覆盖业务。

边缘 DC：满足大型企业数据本地化处理以及时延敏感性业务的部署需求。由于边缘机房资源受限，联通提出了轻量化 ME-IaaS 以及通用与专用硬件融合的方案。边缘 DC 采用极简运维、独立自制、即插即用，提供本地分流能力，适合部署车联网、工业控制、智能场馆等业务应用。

中国联通在集团成立 MEC 边缘云全国管理中心，集中部署 MEAO，并与 OSS、通信云 NFVO 实现对接，获取全网软硬资源信息，提供集中运维、统一 LCM、统一编排、统一配置分发能力。联通边缘云向上构建统一的能力开放平台，并提供统一的接口与界面开放给第三方使用。与此同时，联通 MEC 边缘云采用 SDN 组网架构，统一管理边缘云和中心云，实现基础设施自动化部署，为 VNF/APP 按需、动态拉起包含计算、存储、网络的 IaaS 资源，通过远程 SDN 的集中管理，提高整体运维效率。

4.3.2 MEC 助力智能安防

智能新安防的核心是智能视频监控体系的应用，其中人工智能技术的融入大大丰富了智能监控的深度，智能安防适用于安全工地、河道监控、雪亮工程、平安城市等场景，旨在降低综合成本，提高部署效率。智能安防面临的问题有：

（1）视频监控属于大带宽需求业务，数据都将通过核心网络进行传输，导致运营商网络核心网络负荷过大，成本增加；

（2）在监控场景地处偏远时，有线监控部署方式，会对导致项目施工成本过高、维护难度较大。

为了应对上述问题，联通在多地进行了智能安防的业务试点。在有线覆盖困难区域通过 5G 网络连接摄像头，通过 MEC 边缘云业务平台上的智能监控系统接入，MEC 服务器部署在就近机房，基站与核心网之间链路支持 bypass 切换，实现本地业务分流的同时保护公网业务连续不中断，系统自动识别需要处理的监控数据，分流至联通边缘云监控平台上，再通过专线转发到对应的监控中心。

利用 5G + MEC 的方式部署方式更加灵活，缓解了部分区域的线路维护难度，有效节约安防部署的施工成本、加快了施工进度。同时，在边缘侧加载 AI 应用，面向智能安防、视频监控、人脸识别等业务场景，提供便捷、快速的智能统计、分析，降低管理人员的监管压力，数据通过 5G 网络，安全性得到保障，搭载在边缘侧的应用，比公有云响应更为及

时。边缘云低时延、大带宽、快速响应等特性可以有效弥补当前基于 AI 的视频分析中产生的时延大、用户体验较差的问题，实现本地分析、快速处理、实时响应。

4.4 5G 网络安全

4.4.1 安防业务安全诉求

随着技术升级和革新，安防监控系统朝着网络化、高清化、智能化、集成化的方向发展。高清视频监控设备和系统的不断发展，人们对社会安全保障需求越来越高，高清安防监控已经融入了各行各业，城市公安、交通、金融、环保、电力、医疗、教育等行业管理部门为提高管理水平，对城市范围内大型联网安全与视频监控平台的需求大量增加，其中尤以城市公安和金融领域的需求最为突出。伴随着平安城市建设如火如荼地开展，高清监控系统的优势逐渐被用户所认可，从局部小范围建设向全局大范围建设转变，安防监控平台全面迈入了高清时代。

随着视频监控业务的普及，安防监控需求从办公环境向生产环境延伸，从室内环境向室外环境延伸，从本地监控向远距离监控延伸。这些变化使得视频监控业务的部署更复杂，须要适应多种接入场景，甚至恶劣的环境。网络监控由于其业务特殊性，要求较高的 QoS 保障，基于网络的视频监控系统保障视频监控业务的可靠连续和高质量。5G 网络的高带宽、大连接及低时延的特性，为高清视频监控业务提供了网络基础。

基于 5G 网络，高清安防监控系统可以提供行为识别、数据获取、视频诊断等业务，其中行为及事件分析类可以提供越界侦测、可疑遗留物检测、逆行检测、聚众检测、摄像头遮盖检测等业务；数据获取类可以提供车牌识别、车速识别、流量统计等业务；视频诊断类可以提供视频信号异常检测与视频质量不佳检测业务。

安防系统对安全的要求非常高，需要提供可靠、规范、安全、多样、抗干扰的网络连接服务。主要包括：

信息采集安全：包括保证数据的机密性和完整性,采用抗干扰技术，保障信息采集避免受到其他网络或设备的干扰，并避免干扰其他网络或设备，同时也要保证用户的隐私不被泄露。

网络层安全：除了通信系统本身所需要的安全机制外，还需要提供数据的机密性和完整性保护，避免数据被窃听和篡改。同时也需要对信息采集的设备进行接入认证和授权，保证用户的合法性。

平台层安全：业务平台需要对所接入的业务应用进行认证和授权，保证合法的应用接入平台，同时也需要进行业务数据的机密性和完整性保护，避免数据的泄露和篡改。

业务应用安全：通过提供端到端的安全，保证业务应用数据的机密性和完整性，同时也要对用户隐私进行保护，防止用户隐私泄露。

4.4.2 5G 网络安全目标

5G 网络高速率、大连接、低时延的网络特性，以及垂直行业与移动网络深度融合的业务特征，使得 5G 网络不仅需满足基本通信安全，适应多种网络接入方式及新型网络架构，还需为多样化的业务提供提供差异化安全服务。5G 网络安全总体目标包括：

保障通信及数据安全：提供机密性及完整性保护，保障语音及数据的通信安全；提供增强的隐私保护机制，保护用户隐私信息。

支持异构接入安全：提供统一认证框架，支持多种接入方式和接入凭证，保证终端设备安全接入网络。

保障新型网络架构安全：提供 SDN/NFV 安全机制，保障虚拟资源、软件资源、数据、管理及控制的安全；提供网络切片安全机制，切片安全隔离，安全管理。

支持差异化安全：提供按需的安全保护，满足多种应用场景的差异化安全需求。

开放安全能力，保障能力开放安全：支持数字身份管理、认证能力等的安全能力开放；提供全面的安全机制，保障网络能力开放本身的安全。

4.4.3 5G 网络安全策略与架构

（1）总体安全策略

以保障网络和业务安全可靠运行为目的，合理划分安全域，制定域内域间安全策略和防护方案。

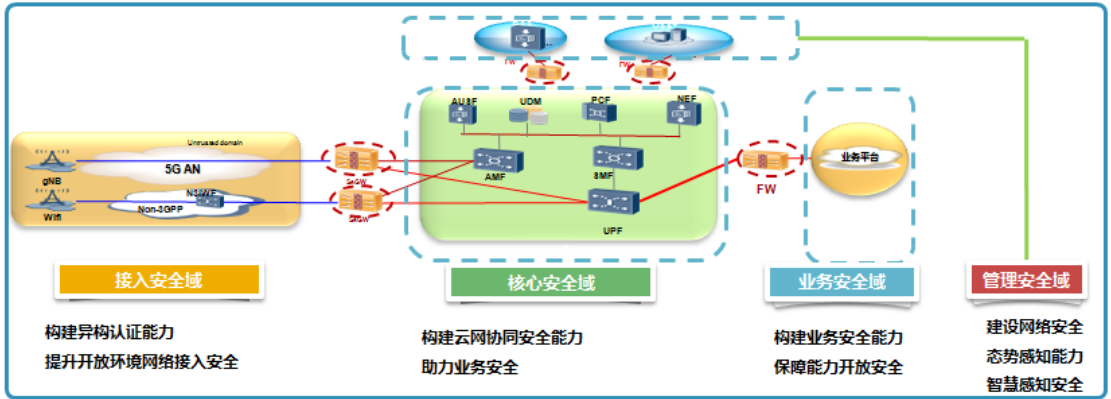
将 5G 网络划分为接入网域、核心网域、业务平台域、运营管理域四大安全域。通过安全域的划分，形成完整的防护体系，对同一安全域内的业务网元进行统一规范的保护，限制安全风险在网内的任意扩散，从而提升网络安全性，保障业务有效开展。

接入安全域重点构建异构认证能力，提升网络接入安全。接入域处于用户侧网络环境之中，为保障网络和业务的安全性，应重点保证对用户鉴权功能可用性，对用户数据和信令进行保护。

核心安全域重点建设云网协同安全能力，助力业务安全。该域需要与内外部业务平台对接，因此需开展入侵检测、攻击防御、数据保护等工作，同时针对该域的云化、软件化特性对集中控制器、南北向接口等进行重点防护。

业务安全域重点构建业务安全能力，保障能力开放安全。该域包括能力开放平台、自营及第三方业务平台等，因此既要防护网络侧对业务的攻击和滥用，也要防止利用平台和应用对网络发起的攻击。

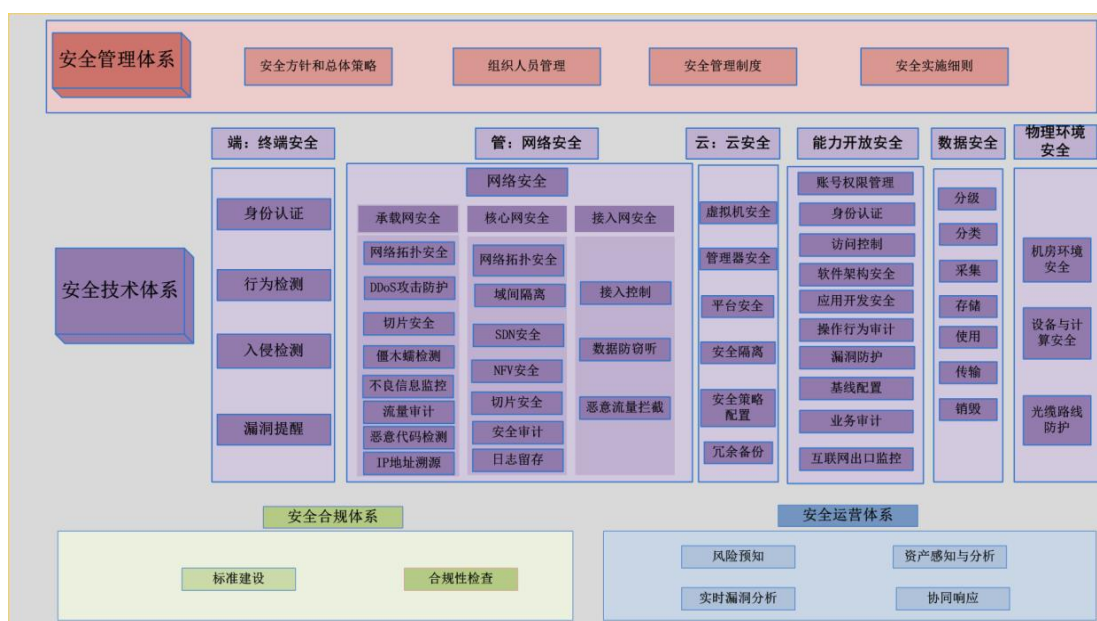
管理安全域重点构建网络安全态势感知能力，智慧感知安全。建设 5G 网络全网安全态势感知能力，借助 AI、云计算等技术，提升 5G 网络威胁感知和威胁处置能力。



图：5G 网络安全域

(2) 安全体系架构

构建全方位、立体化的 5G 网络安全整体架构，融合安全管理体系、安全技术体系、安全合规体系以及安全运营体系，提升网络安全防护能力。



图：5G 网络安全架构

安全管理体系是 5G 网络安全工作的行为规范，是安全工作的制度保障，是安全管理的重要基础性工作。安全管理体系包括安全方针和总体策略、组织人员管理、安全制定管理、安全实施细则等内容。

安全技术体系为 5G 网络安全实施定义了所需的技术方法、安全防护能力要求，为网络与信息安全提供技术保障。安全技术体系包括：终端安全、网络安全、云安全、能力开放安全、数据安全、物理环境安全等。

安全合规体系为 5G 网络建设运营提供安全合规保障。安全合规体系包括：安全标准建设、合规性检查。

安全运营体系保障 5G 网络与业务稳定运行，是管理制度、安全规范要求和控制措施的落实体现。安全运营体系包括：风险预知、资产感知与分析、实时漏洞分析、协同响应等。

4.4.4 安防业务 5G 网络安全方案

对于安防类应用，管侧安全重点聚焦“网络专用、横向隔离”，5G 网络将重点关注网络切片安全，以及网络安全的能力开放两方面。通过网络切片来保障，不同的切片/业务除开在性能、QoS 方面的差异之外，还因承载数据的敏感程度差异，具有不同的安全等级要求。为了满足上述安全需求，网络切片需要提供不同切片实例之间的隔离机制，防止本切片内的资源被其他类型网络切片中网络节点非法访问。根据安防业务的不同将网络功能

分割成不同的网络切片时，需进行切片内的认证和授权，当切片管理的某些功能开放给第三方时，需建立由运营商控制的主认证和授权与由第三方控制的二次认证和授权的融合机制。

(1) 5G 核心网提供多层次的切片安全保障，为安防业务提供差异化的隔离服务。5G 切片安全机制主要包含三个方面：UE 接入安全、网络域安全，外网设备访问安全。

① UE 接入安全：通过接入策略控制来应对访问类的风险，由 AMF 对 UE 进行鉴权，从而保证接入网络的 UE 是合法的。另外，可以通过 PDU（分组数据单元）会话机制来防止 UE 的未授权访问。

② 网络域安全：网络域通信安全可以分为三种情况：

A、NF 间互访安全：NF 理论上具备访问其他所有 NF 的能力，因此切片内的 NF 需要安全的机制控制来自其他 NF 的访问，防止其他 NF 非法访问。安全机制可考虑使用 NF 间的认证与授权机制。

B、不同切片间 NF 的隔离：不同的切片要尽可能保证隔离，各个切片内的 NF 之间也需要进行安全隔离，比如，部署时可以通过 VLAN（虚拟局域网）/VxLAN（虚拟扩展局域网）划分切片。

C、切片内的 NF 间安全：切片内的 NF 之间通信前，按需可以先进行认证，保证对方 NF 是可信 NF，然后通过建立安全隧道保证通讯安全，如 IPSec。

③ 外网设备访问安全：在切片内 NF 与外网设备间，部署虚拟防火墙或物理防火墙，保护切片内网与外网的安全。如果在切片内部署防火墙则可以使用虚拟防火墙，不同的切片按需编排；如果在切片外部署防火墙则可以使用物理防火墙，一个防火墙可以保障多个切片的安全。

(2) 5G 网络安全能力开放，助力新安防实时更灵活的安全保障措施。体现 5G 网元与外部业务提供方的安全能力开放，包括开放认证与密钥管理。也可以根据业务对于数据保护的安全需求，提供按需的用户面保护。

5 5G 时代运营商在安防行业的商业模式分析

5.1 安防行业的市场分析

安防行业的市场具有三个环节：安防产品、安防工程以及安防运营服务和其他。其中，安防工程这一环节利润最为微薄；在技术升级、产品同质化和成本降低的背景下，安防产品市场的利润空间逐渐被压缩，企业只卖硬件将难以生存；在安防商业模式的发展演进中，安防运营服务处于整个产业金字塔体系的最顶尖，将是未来发展的新方向。在美国，大多数安防企业集中在利润比较丰厚的市场环节，企业的运营质量较高；而在我国，据 2017 年的统计，安防工程占安防行业总产值的比重为 61%，安防产品占安防行业总产值的比重为 32%，而安防运营服务只占安防行业总产值的 7%。因此在我国，安防运营服务将会具有很大的发展空间。在安防运营服务中，用户购买的不再是产品，而是实用的服务运营方案。但是要做到这一点并不容易，需要安防服务商在服务、管理、技术等方面具有较强的整体实力。

5.2 5G 时代运营商在安防行业的商业模式

运营商具有强大先进的网络通信资源、庞大的集团客户群体、完备的运营体系，在促进安防联网以及网络资源共享方面能够产生巨大的推动力，在安防系统集成以及安防运营服务方面具有天然的优势。在 3G、4G 时代，运营商主要充当了管道商，而在移动互联网的发展浪潮中，运营商在基础管道服务上的价值不断下降。随着 5G 时代的到来，高额的网络投资的回报周期加长，在提速降费的政策背景下，运营商管道的价值会进一步被压缩。因此，在 5G 时代，运营商若想抓住机遇，必须转变原有的商业模式，不能再仅仅依据单一的管道流量收费模式，而是需要能够采用多种商业模式，具有差异化服务提供能力，构建统一平台，逐步提供规模化的服务。

下面从运营商角度，给出三种安防应用的商业模式。

模式一：管道模式

对于运营商而言，管道始终是其特有的优势资源。在一些场景下，政府、公安等用户会根据项目需求集中采购整套移动监控设备及平台系统，仅需由运营商提供通信管道服务。在这种情况下，运营商可以针对行业客户大带宽、低时延、海量设备连接的需求，通过网络切片向用户提供差异化的服务，从而实现不同的收费。

模式二： ICT 项目建设模式

根据客户需求，运营商作为集成商，采用 ICT 项目方式进行交付，向客户提供端到端的解决方案。

模式二：“以租代建”模式

这种模式类似于项目市场的 ppp 模式。即，由政府或用户规划项目，由运营商投入资金，对项目进行建设，但所有权归运营商所有；项目建成后，以租赁的方式，交给用户使用。在此种模式中，运营商可以对基础设施进行出租，例如出租 MEC 基础设施，也可以构建统一的视频监控平台，将能力开放，面向用户开展平台出租业务，从而实现规模化运营。

6 总结与展望

人工智能技术的发展对传统安防的升级改造具有重要意义。在安防领域，如果说 AI 是一个产品内部引擎，那么网络则是一个外部应用管道，但是，受限于当前网络，智能安防的诸多需求还远远不能满足。譬如，作为安防产业重要组成部分的视频监控，其具有高清、高带宽、户外广域部署的需求，急需运用高效的网络技术来促使视频监控系统数据传输的快速、高质量完成，而现有的 3G、4G 网络将无法很好的满足这一需求。5G 所具备的特性，将会为其与智慧安防的深度结合创造条件，有利于安防监控范围的进一步扩大，能够获取到更多维的监控数据，从而促进智能安防的发展。

5G 的落地将加速智能安防向商用、民用端的全面渗透；5G 商业化的全面部署必将为安防行业带来全新的技术变革，为安防行业带来更多的机遇。