JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road · Laurel, Maryland 20723-6099

AOS-21-0519

Fifth Generation (5G) Mobile Broadband Impacts and Recommendations for Public Safety

Department of Homeland Security (DHS)
Science and Technology Directorate (S&T)
Office for Interoperability and Compatibility
Technology Center (OIC-TC)

May 2021

Prepared for:

The Department of Homeland Security Science & Technology Directorate

This document was prepared under funding provided by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) (Contract Number N00024-13-D-6400; Task Order 8018, Task Number S8937, Technology Center Support for First Responders). Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

Authors:

Mr. Emery Annis
Mr. Jay Chang
Dr. Cherita Corbett
Mr. Ryan Pepito
Ms. Elizabeth Parkin
Ms. Ruth Vogel

Contributors:

Dr. Ashutosh Dutta
Mr. Triton Pitassi

The authors would like to express their appreciation to the Department of Homeland Security Science & Technology Directorate sponsor Mr. Cuong Luu.

Please send questions or comments to:

Ms. Ruth Vogel
Program Manager
Johns Hopkins Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099
Phone: 240-228-2425
E-mail: ruth.vogel@jhuapl.edu

ABSTRACT

In support of Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office for Interoperability and Compatibility (OIC) Technology Center (TC), the Johns Hopkins University Applied Physics Lab (APL) team investigated fifth generation (5G) technologies to better understand the potential for enabling improved information sharing at the incident area "edge" network. The goal of this study was to investigate the various impacts, opportunities, and challenges that 5G mobile broadband networks will have on the DHS S&T operational customers and the first responder communities. The APL team took a systems view approach to describe key stakeholders, relevant systems, and communications capabilities that exist today, and extended that view into a mid-term and future 5G technology outlook. Several of the key 5G technology enablers have been investigated to better understand their capabilities, characteristics, and architecture according to the specifications. The relevant 5G technologies that were investigated as part of this effort include the 5G Core Service Based Architecture (SBA), 5G Disaggregated RAN, Multi-access Edge Computing (MEC), Non-Public Networks (NTN), Network slicing, and the Management and Orchestration (MANO) systems which help automate deployment and guarantee resilient scaling and healing. A set of overarching impacts, opportunities, and challenges is provided along with a set of recommendations to leverage 5G technologies as they become available.

EXECUTIVE SUMMARY

The Nation's need for secure, resilient, interoperable, and prioritized communications remains a priority as information sharing and assured command and control provide key decision support capabilities. In today's world of vast and diverse threats, voice-only radios are no longer sufficient; our Nation's public safety communities require full situational context to perform their duties to the best of their abilities. Lessons learned from major disasters, unplanned events, and exercises continue to demonstrate the need for interoperable and secure information sharing for real-time situational awareness.

In recent years, the 4th generation Long Term Evolution (4G/LTE) mobile broadband networks played a crucial role in inter-jurisdictional and inter-disciplinary communications interoperability. This is especially true of voice communications for improved situational awareness and coordination. However, there remains a need for more easily integrated communications systems, increased capacity, reduced latency, and the ability to share information to the right people at the right time.

The fifth generation (5G) of mobile broadband communications promises to revolutionize communications and access to information by providing many improvements over previous generation mobility networks. This includes an order of magnitude improvement in peak data rate, latency, spectrum efficiency, and connection density, and two orders of magnitude improvement in area traffic capacity and network energy efficiency. This means more capacity (tens of gigabits), more users (10^6 per km^2), and sub millisecond latency. 5G further promises to accomplish this with increased resilience, scalability, and quality of experience through advanced automation and business driven service orchestration. While some aspects of 5G have been deployed as early as 2019, many of the advanced features will take years to standardize, develop, and deploy.

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office for Interoperability and Compatibility (OIC) Technology Center (TC), in alignment with its mission to "provide subject matter expertise and core research capabilities needed to maintain the ability to identify and address current and future homeland security challenges in the areas of communication and network capabilities" is closely tracking the 5G standards development, commercial deployments, and the academic and industry research and development trends. Further, OIC-TC is actively investigating the impacts, opportunities, and challenges that will be imposed by 5G to the public safety community.

In order to assess impacts of 5G on the public safety community, the OIC-TC tasked the Johns Hopkins University Applied Physics Lab (APL) to employ a deep dive approach to investigate specific 5G technologies which will enable information sharing at the incident area "edge" network. To facilitate this approach, APL used an active shooter scenario adapted from the National Public Safety Telecommunications Council (NPSTC) Internet of Things (IoT) use case report and assessment, along with lessons learned and recommendations reported from the shooting at the Marjory Stoneman Douglas High School.

Based on emergency response information needs, APL identified and explored relevant stakeholders, systems and communication-based capabilities within the context of an active shooter use case. This report analyzed scenarios into mid-term and future 5G technology impacts. The relevant 5G technologies discussed in detail include the 5G Service Based Architecture (SBA), Multi-access Edge Computing (MEC), Non-public Networks (NPN), network slicing, and the Management and Orchestration (MANO) systems that help automate deployment and guarantee resilient scaling, healing, and service delivery. The goal

was to describe the existing operational gaps and map the various impacts, opportunities, and challenges that 5G would bring to the public safety community. These include the following:

Impacts:

- New emergency responder use cases
- Improved network and radio access resilience
- Cloud-based interoperable solutions

Opportunities:

- Business and mission driven network services
- Faster to market first responder solutions through agile software development methodologies
- Integration with next generation first responder solutions and 911

Challenges:

- Complexity of 5G systems and enablers
- Variability in 5G deployments
- End-to-end mission critical services
- Information security

In order to help the public safety community approach 5G mobile broadband networks as they continue to evolve and be deployed, this report offers a set of recommendations as a path forward to address some of the challenges noted above. These include the following:

Recommendations:

- Levy 5G mobile broadband network requirements, including features, use cases, and functionality from the public safety community
- Develop an information generation, processing, and sharing framework in order to inform all 5G enabled, first responder mission dependent service automation and orchestration
- Develop first responder validation procedures for end-to-end networks and services
- Approach the entire 5G ecosystem of standards development organizations

5G technologies are rapidly being standardized and deployed today. Mobile broadband carriers will deploy solutions incrementally in an attempt to be first to market, and will further aggressively advertise features well before market saturation. This report provides insight regarding the various impacts, opportunities and challenges 5G will imposed on the public safety community and offers a set of recommendations to embrace new technologies for improved situational awareness and decision support.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The Fifth Generation (5G) mobile broadband networks is coming and aspects are already being deployed throughout the nation. Previous mobile broadband networks have already proven their importance among the public safety community for improved access, coverage, and ability to enable interoperability among different jurisdictions and agencies at all levels of government. The 5G mobile networks are expected to bring forth broad ranges of new capabilities enabled by technologies adapted from enterprise networks and cloud computing that has the potential to transform a first responder's ability to execute missions.

This report describes the motivation and relevance of 5G networks among the public safety community, along with describing the various technical architectures of 5G systems. It utilizes an operational systems view of the public safety community response to an active shooter scenario to discuss how 5G solutions can be leveraged to improve information sharing at the edge. Lastly the various impacts, opportunities and challenges imposed on the public safety community are described along with a set of recommendations and path forward. The following provides an overview of how this report is organized:

- **Section 1:** Introductory Comments
- **Section 2:** Includes the operational background and historical implications of mobile broadband networks to the public safety community, along with an introduction to the 5G technical vision
- **Section 3:** Describes the 5G systems architecture along with enabling 5G technologies and vertical use case enablers such as virtualization, service orchestration, edge computing, network slicing, and private networks
- **Section 4:** Describes the active shooter use case scenario, introduces a current operational systems view, and overlays both a mid-term 5G view and future outlook with ubiquitous 5G deployments leveraging all of the enablers discussed.
- **Section 5**: Presents a set of impacts, opportunities, and challenges that the public safety community may face as 5G continues to evolve
- **Section 6:** Offers a set of recommendations for public safety communities as they look to embrace new technologies
- **Section 7:** Conclusion

2 BACKGROUND

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office for Interoperability and Compatibility (OIC) Technology Center (TC) plays a key role in providing the subject matter expertise and core research capabilities for communications and network capabilities among the S&T customer components[1]. The OIC-TC helps to provide their operational customers with capabilities to enable improved information sharing and manages a comprehensive research, development, testing, evaluation and standards program to enhance interoperable emergency communications. This includes investigating emerging technologies that could lead to long-term advancements in public safety communications and supporting research to better understand the technical and operational capabilities and underlying architecture.

The need to deliver the right information to the right person at the right time cannot be minimized. A framework developed by DHS S&T OIC that is referred to as the Mission, Content, Transport Network (MCTn) (Reference [1]), see Figure 1, can be leveraged to plan for information (e.g., video data) across the end user(s), content owner, and transport network provider[2]. Elements of the broader 5G ecosystem, such as edge analytics or business driven service delivery and automated orchestration have the potential to meet many of these goals. As public safety mobility networks are exponentially adopted, decision makers may eventually reach a point of *information overload,* where too much information is presented. This will likely obscure the goal of providing timely and usable situational awareness information to decision makers. Therefore, in addition to 5G technology impacts, consideration must be given to ensure there are equal efforts focused on technology developments to help promote analytics and advanced decision support requirements (e.g., right information is available at the right time, in context of the mission).

[1] https://www.dhs.gov/science-and-technology/office-interoperablity-and-compatiblity

[2] It is important to note that the components of the MCTn framework cannot individually address the needs of the mission owner, so a systematic holistic approach needs to be considered. To this end, the document can be used to understand the concept of the mission owner receiving the necessary content data, delivered on-time in order to successfully complete the mission.

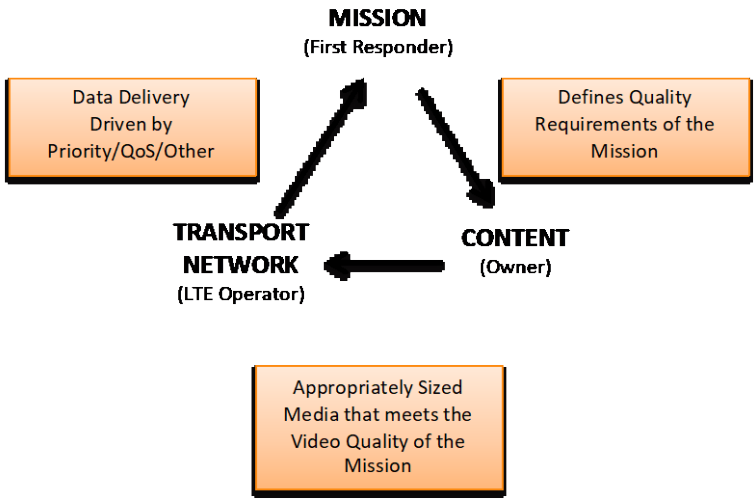


Figure 1 – Mission, Content, Transport Network (MCTn) (Reference [1])

Access to information in this manner continues to be a challenge due to inadequate and unreliable communications systems shared among the public safety community. This is especially true in cases where jurisdictions and agencies use different radio technologies, different radio bands, or completely incompatible proprietary systems and infrastructure. The communications systems which enable interoperability, are often complex, serving as a gateway between disparate technologies. This is especially true for incidents involving multi-jurisdiction and multi-agency public safety response that include a large number of systems and end-users.

As an example, Figure 2 below, borrowed from the Next Generation First Responder (NGFR) integration demonstration in Harris County Texas, provides a view of what interoperability looks like today in the operational sense, with a fire command staff juggling multiple radios and tablets to maintain connectivity among all involved jurisdictions and agencies.

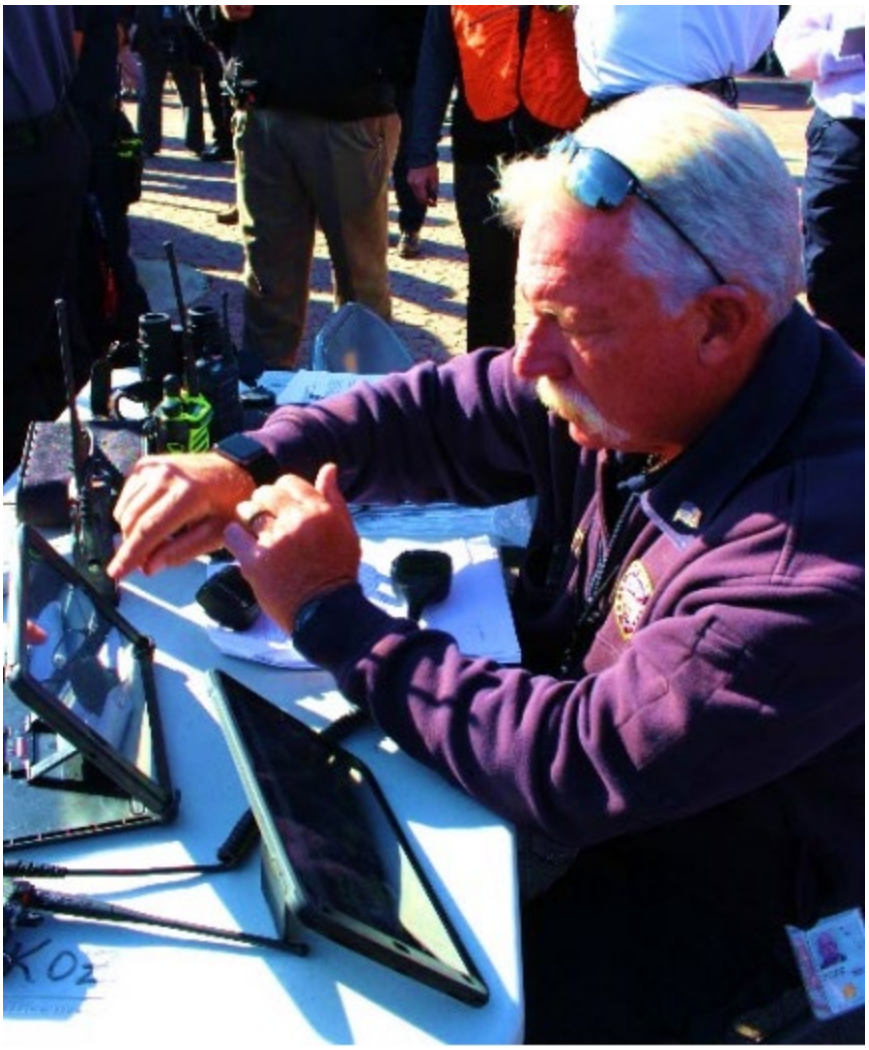


Figure 2 – Port of Houston Fire Command (Reference [2])

Interoperability for improved coordination and collaboration is key to ensure the safety of citizens, public safety, and first responders. Additionally, economies of scale savings are possible when jurisdictions and agencies can interoperate using common systems and software to communicate. This is enabled in a large part by strict adherence to a standards based approach and well-defined interfaces guaranteeing the ability to share/exchange data in a standardized and repeatable manner. Leveraging commercial mobile broadband technologies such as 5G could prove to be extremely impactful for the public safety community.

2.1 Next Generation Emergency Responder Communications Requirements

Access to information by public safety end-users comes with additional requirements to ensure they are better protected, connected, and fully aware. The Next Generation First Responder (NGFR) Apex Program[3] outlines a vision that includes integrated and autonomous access to information with advanced

[3] https://www.dhs.gov/science-and-technology/ngfr

collaboration and coordination capabilities. This is only enabled through next generation communications systems with:

- assured delivery
- increased capacity
- information timeliness guarantees
- automation
- advanced routing

Communications systems must be designed to provide secure guaranteed access and transport for the public safety community. This includes priority and preemption for overloaded networks as referenced by the National Public Safety Telecommunications Council (NPSTC), who defines mission critical as "an expectation that system coverage and availability is not lost and that limited data losses do not impact mission critical systems" and states that a mission critical data communications system "must not suffer loss of service availability due to single point failures" (Reference [3]).

Increased capacity will be necessary to support the growing demands and technology-assisted missions at the incident edge. This includes access to higher quality data such as 4k or 8k video, 3D point mapping, or advanced positioning, navigation, and responder identification. It is also envisioned that numerous sensors and smart devices will be deployed everywhere including on-body, in-vehicle, in-building, or via rapid deployment of drones or robots. Each of these will need reliable access to the network and will also place varying loads on the network, the aggregate of which could be very large.

Communication systems must also provide real time access to information. Stale information can result in poorly informed decisions and actions which can place the public or emergency responders in harm's way. Various information sharing systems that exist today operate by collecting, aggregating, fusing, and redistributing that data. In some cases, this process is manual and requires human intervention at each step. This tends to result in delays of getting critical information to key decision makers, which can range from minutes to hours depending on the size and type of event.

Advanced routing, meaning optimally selecting the best path data will take as it traverses the network and RF communications environment, will be key to ensure the right information is sent to the right place at the right time. Though increased quality of secure information and guaranteed delivery is important, it will be extremely critical to filter information to ensure the operator is not inundated with too much information. It will be necessary to uniquely identify each operator by their type and role, and only transmit the information pertinent to their role. Furthermore, it will be necessary to accomplish this as easily and autonomously as possible without requiring laborious configuration.

It is thus necessary to look at the existing and future standards based communications technologies to determine which can bridge the various operational gaps to better protect and enable decision makers. Mobile broadband communications technologies such as the 4th Generation Long Term Evolution (4G/LTE) has been serving to bridge those gaps recently. The latest generation of mobile broadband network technology, 5G, is under development and some aspects have already been deployed. These technologies are likely to be critical to the public safety community due to the adoption by the public and the future ubiquity of access throughout the nation.

2.2 MOBILE BROADBAND COMMUNICATIONS FOR PS COMMUNITY INTEROPERABILITY

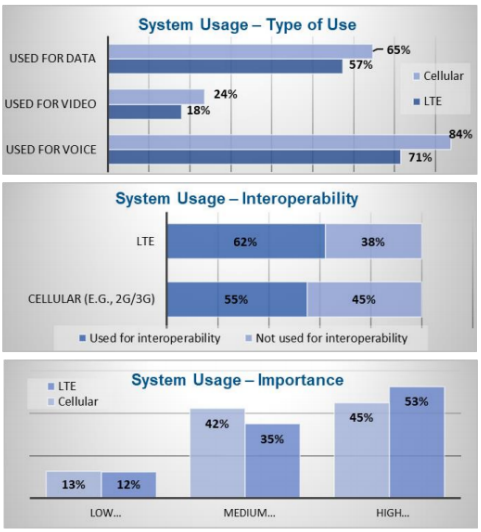
Mobility broadband networks have been widely embraced by the public as a means to communicate via both voice and data. Since 4G/LTE launch in 2010, the network has grown to provide more capacity and coverage for less money with average download speeds increasing from 1.3 Mbps to 41 Mbps over this period (Reference [4]). According to the recent Federal Communications Commission (FCC) 2020 Communications Marketplace Report (Reference [5]) among the 3 major service providers including AT&T, T-Mobile, and Verizon, national coverage includes 98% of the U.S. population and at least 84% of U.S. road miles.

The 4G/LTE networks have revolutionized the way consumers use their mobile devices through increased download speed and access to the internet including high definition video streaming, collaborative communications applications including both social media and ride sharing platforms, and access to real-time public data through live-mapping navigation applications. The public safety community has also greatly benefited from 4G/LTE technology both through commercial deployments as well as through the FirstNet Network[4]. According to the SAFECOM Nationwide Survey (SNS)[5] which solicited information directly from the public safety community, commercial wireless technologies such as 2G/3G cellular and 4G/LTE communications have been critical for both voice and data communication and interoperability. This includes 37% of responders claiming to utilize "bring your own device" commercial wireless service and 21% using government issued equipment. Of particular interest is a note from the SNS that was recently included in the National Emergency Communications Plan (NECP) webinar on how 5G could impact emergency communications[6] stating "over half of respondents indicated that the cellular and LTE systems they use is provided through a commercial, subscription-based service" and "over 55% of respondents indicated that they use cellular and LTE systems for interoperability."

[4] https://firstnet.gov/
[5] https://www.cisa.gov/safecom/sns
[6] https://www.cisa.gov/necp-webinars

SNS: Technology Use

- Of those using cellular and Long-Term Evolution (LTE) networks, more public safety organizations are using them for voice services than data services
- Over half of respondents indicated that the cellular and LTE systems they use is provided through a commercial, subscription-based service
- Over 55% of respondents indicated that they use cellular and LTE systems for interoperability
- Almost two-thirds say their cellular and LTE systems support day-to-day situations without intervention
- Over 45% of organizations indicate their cellular and LTE systems are highly vital for mission function



Eric Runnels
December 9, 2020

Figure 3 – SAFECOM Nationwide Survey Technology Use of LTE (Reference [6])

While 4G/LTE has been impactful, it is still primarily used for voice communication and limited access to data, such as video, is still dependent on manual processes and often limited by capacity or latency constraints. The FirstNet network has played a key role in providing guaranteed priority and preemption, however FirstNet plays no role in guaranteeing access to the right information at the right time. The next iteration of mobile broadband networks, 5G, is rapidly being standardized and deployed, and promises to bring a broad range of new capabilities, automated processes and control, and mission critical services to both the commercial and public safety communities.

2.3 5G Networks

The latest version of mobile broadband networks, known as 5G, promises to revolutionize future communications, access to information, and bring about a multitude of new use cases including connected "things" and access immersion enabled by Virtual Reality (VR) and Augmented Reality (AR). The International Telecommunication Union (ITU) established a set of enhanced key capabilities for 5G communications over previous IMT Advanced (4G) in the IMT Vision for 2020 and beyond which is illustrated in Figure 4 (Reference [7]). This includes an order magnitude increase in peak data rate, latency, spectrum efficiency, and connection density, and two orders of magnitude increase in area traffic capacity and network energy efficiency. This means more capacity (tens of gigabits), more users (10^6 per km^2), and sub millisecond latency.

The ITU also defined key capability enhancements and three pillar usage scenarios of 5G communications, which set the stage for the breadth of capabilities. These are illustrated in Figure 4 and include Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC). The eMBB use case encompasses access to data similar to today

however with increased capacity for streaming 4K video among others. The URLLC use case will support self-driving cars, factory automation, and both VR and AR applications. In this use, case there is a need to ensure safety through reliability of message delivery for end-to-end communications as well as providing extremely low latency to ensure autonomous systems can operate at the speed of human perception. The mMTC use case will enable the Internet of Things (IoT) which could include “smart” sensors and systems in homes, cities, highways, and public infrastructure.

Mobile network operators have begun to deploy aspects of the 5G networks as early as 2019, however focus thus far has remained on upgrades to ensure interoperability with existing 4G networks, virtualization of core functionality for high-availability, and the eMBB use case for increased network capacity.

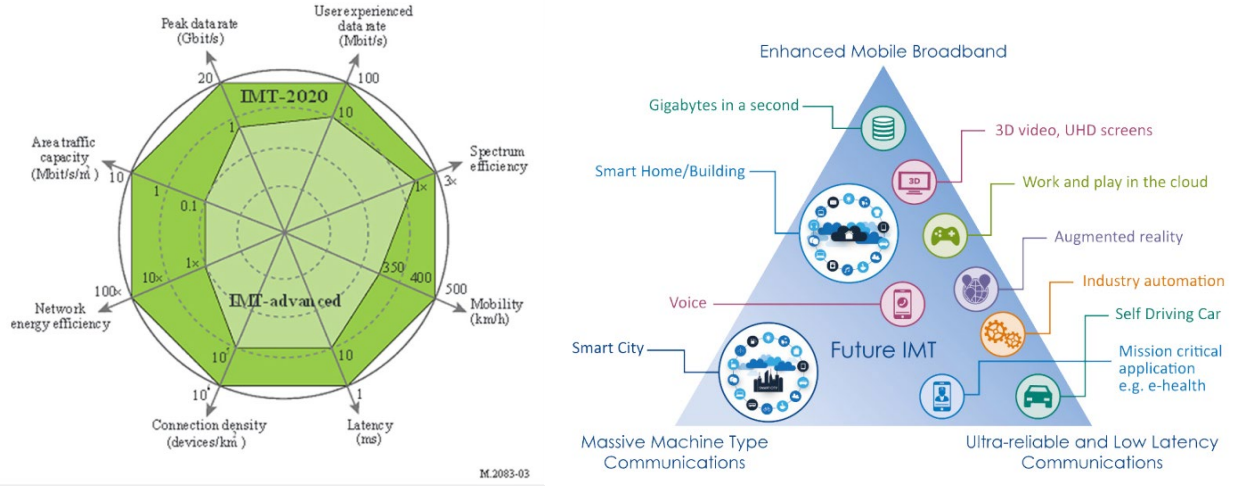


Figure 4 – IMT 2020 key capability enhancements (Left). IMT 2020 usage scenarios for 5G (Right) (Reference [7])

The ultimate vision for 5G networks is quite large and thus systems architects and standards development organizations have had to completely redesign many aspects of previous 4G networks. This includes the requirement to enable the broad range of new use cases using a single underlying architecture of radio address technologies, transport networks, and core network infrastructure. In order to meet many of the capacity, density, latency, and resiliency requirements, the network has grown closer to the edge and been designed with flexibility in mind, thus the overall footprint and complexity has grown considerably.

This has forced engineers to take a very different approach to the development of 5G infrastructure. No longer can single purpose mobility systems hardware be developed to provide solely voice calls and data for worldwide deployment. Systems today must be robust, dynamic, resilient, adaptable, programmable, and easily deployable, easy to monitor, and easily upgradable. This results in a software driven approach to 5G built upon cloud infrastructure and demands a need for analytics driven autonomous control including self-configuration, self-protection, self-healing, and self-optimization.

Additionally, 5G networks are being designed to be business driven from the top down and constructed into services offered to the end user. This includes both end-user application and service delivery, as well as the network configuration that governs the operations of access, mobility, and transport, among others. This approach to business enablement is shown in Figure 5 where the enterprise use cases, business models, and value proposition are shown at the top, accessible via business enabler Application

Programming Interfaces (APIs) from the large library of modular Network Functions (NFs) and value enabling capabilities. These NFs are logical instantiations of radio access technologies and network routing, firewall, or quality of service rule sets which are deployed to the physical infrastructure and resource layer shown at the bottom. The End-to-End (E2E) management and orchestration layer consistently monitors for appropriate Key Performance Indicators (KPIs) and trigger conditions, and deploys new NFs for scaling and healing purposes as well as new configuration to existing elements.

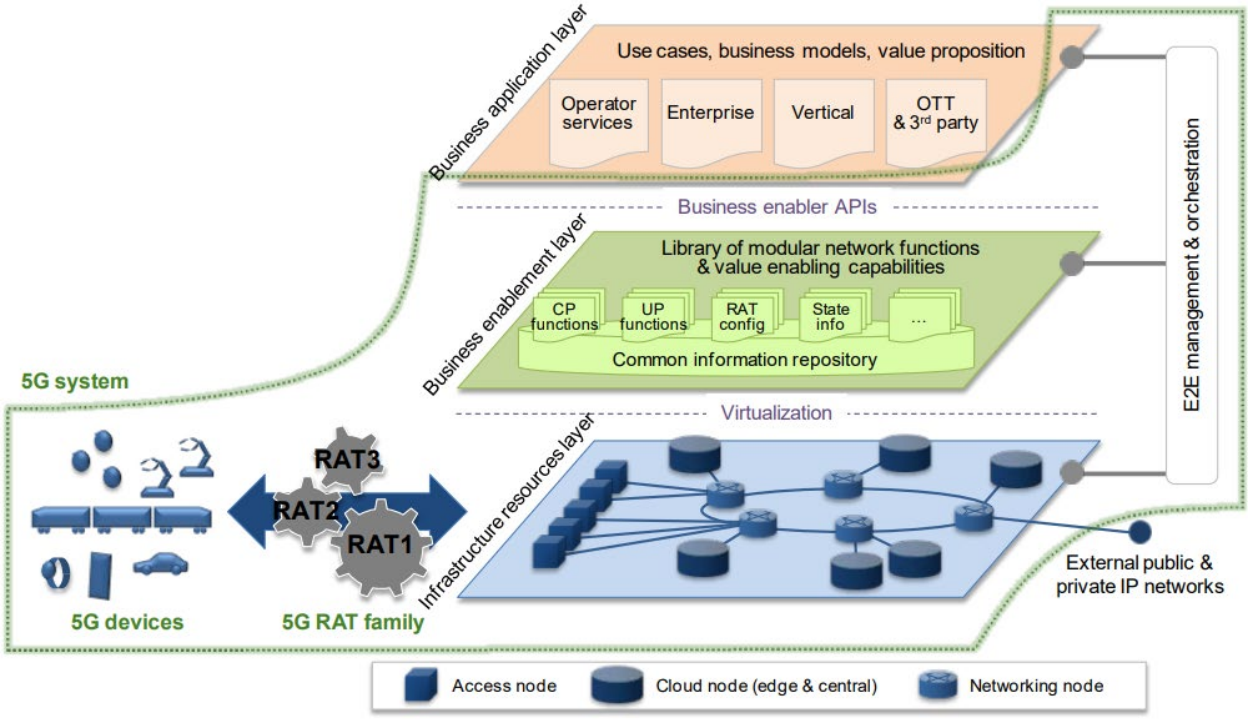


Figure 5 – Business Driven 5G Architecture (Reference [8])

This model allows for end users to define end-to-end service requirements and functionality at the business application layer in much finer granularity than previous generation mobility networks. Mobile network operators will be able to provide fully integrated solutions that encompass networks, clouds and platforms, with dynamic customization. These capabilities, along with features such as virtualization, cloudification, and centrally managed service orchestration will provide increased flexibility, agility, and resilience needed by the public safety community.

While there are many technologies that will comprise 5G networks, this paper's focus is on some of the core components that will be critical to enable all of the envisioned 5G use cases previously noted, namely, the 5G Service-based Architecture (SBA), Network Function Virtualization (NFV), Multi-access Edge Computing (MEC), Network Slicing, Non-Public Networks (NPN), and the Management and Orchestration (MANO) systems which help automate deployment and guarantee resilient scaling, healing, and service delivery. Some of these enablers fall outside the normal scope of mobility broadband standards development organizations and thus are governed by other entities. These are especially important to note as many public safety community solutions that enable interoperability on 5G networks will leverage these technologies.

While mobile network operators may manage the end-to-end solutions, it is possible many other organizations will play a large role as well. It is thus important for the public safety community to understand the various impacts and challenges these solutions may bring.

2.4 Relevant Use Case

An emerging area that is of considerable interest to the public safety community is the use of IoT sensors and other devices for improved situational awareness, enhanced common operating picture, improved responder health and safety, improved efficiency and cost savings, and improved access to potentially lifesaving patient data. Therefore, an active shooter (e.g., school shooter) use case was chosen to facilitate the investigation of the impacts and challenges that 5G may bring as the decisions made during this type of an event are highly dependent on real-time information that is provided by a variety of user devices (e.g., body-worn cameras, fixed cameras, sensors). The use case referenced in this document was adopted from the NPSTC Public Safety IoT Use Case Report and Assessment Attributes Report (Reference [9]) and identifies eight (8) public safety use cases with increasing incident scale, starting from a traffic stop involving a single police officer, up to extreme weather events involving multi-service and multi-jurisdictional response at various levels of government. The use case versus incident scale from the NPSTC report is shown in Figure 6. The report was based on services over FirstNet. Today, FirstNet is rooted on 3GPP's LTE standard; however, the same use case scenarios are applicable on 5G networks and may be further enhanced by the capabilities of 5G.

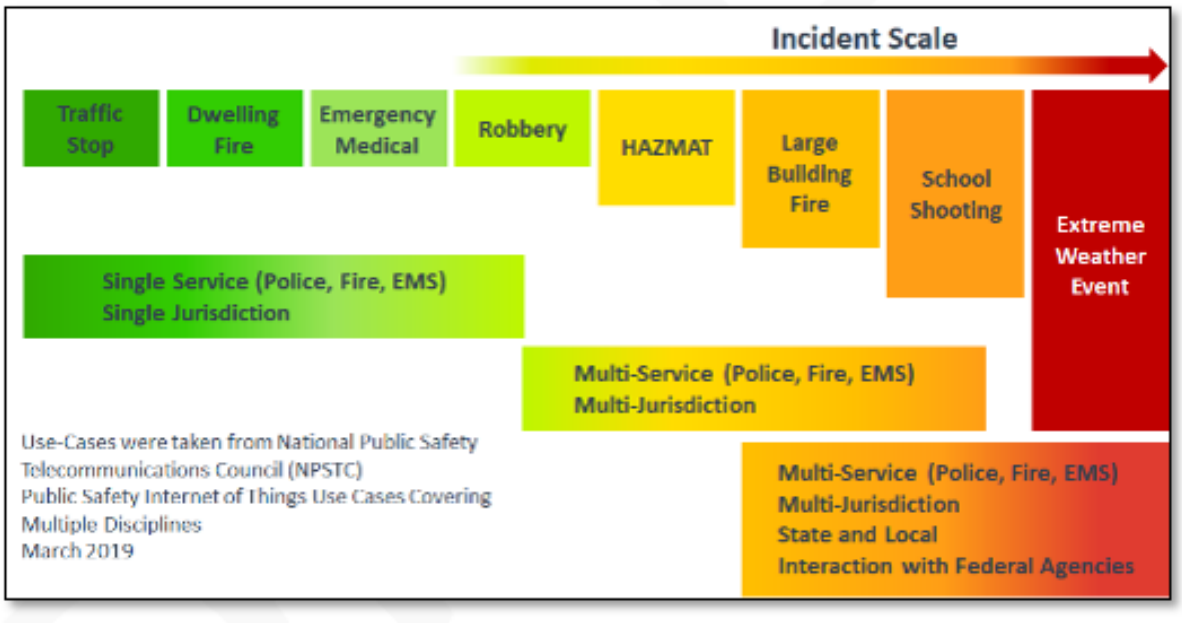


Figure 6 – NPSTC Use Cases versus Incident Scale

The NPSTC IoT use cases are based on the applicability of the data to support public safety disciplines driven by their specific needs. While each of the eight (8) use cases could benefit from the enhancements enabled by 5G, the school shooting use case will be used for 5G impact research since the use case is sufficiently complex allowing the key findings to be applied to other use cases identified by NPSTC. While the remainder of this report focuses on the school shooter scenario and leverages lessons learned from

past exercises and events, the term active shooter is used interchangeably throughout, as the public safety community response would likely be the same regardless of the location of the incident.

The active shooter scenario would likely progress through many phases of the incident, including:

- initial event detection and reporting,
- dispatch and emergency response arrival on scene,
- establishment of incident command,
- scene containment and control,
- evacuation, treatment, triage, and transport of injured,
- multi-service and multi-jurisdiction coordination (e.g., SWAT or bomb squad), and
- post-event forensics.

In order to further scope the discussion, this report focuses primarily on information sharing at the "edge" incident area network as depicted in Figure 7.

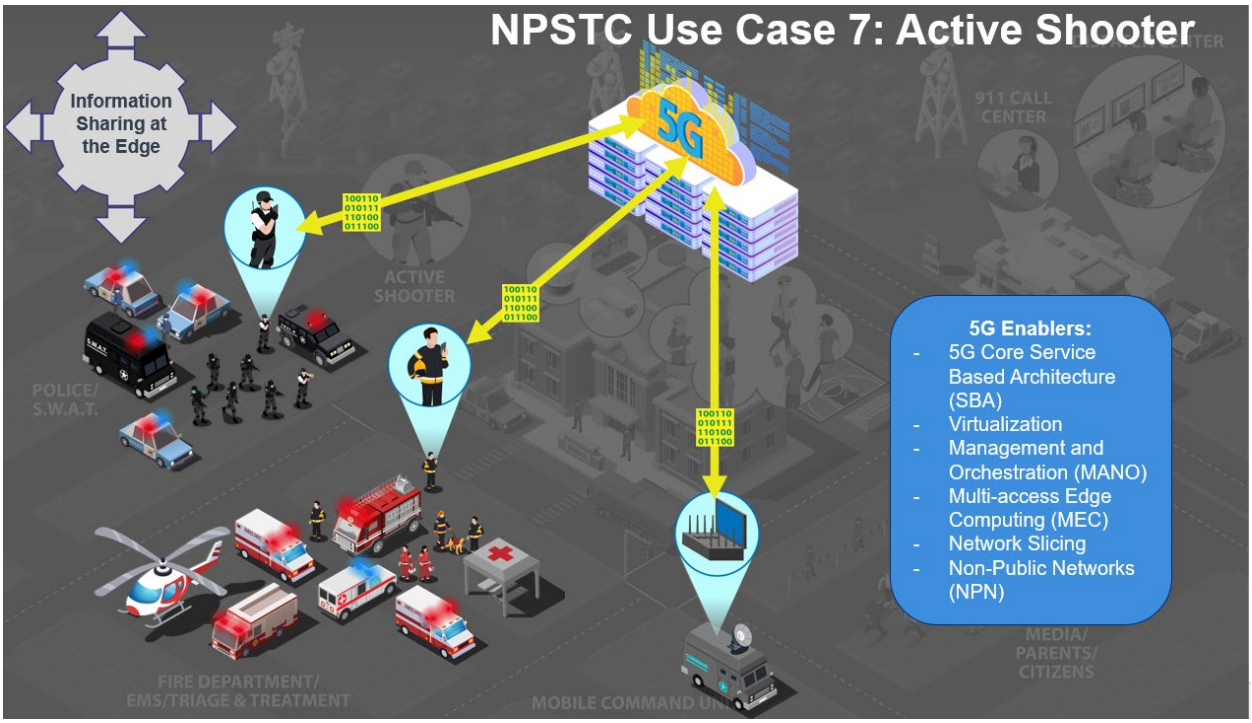


Figure 7 – 5G Information Sharing at the Edge

In addition, there are various data types described in the use case and video data will play more of a critical role in the future. Video in general requires considerable amount of network resources, but live video requires even more reliable and secure connections in order to deliver and meet the quality and latency requirements for critical incident decisions. Compared to other types of data, video is the most demanding. As a result, this report will use video as the reference data to apply to 5G elements and its impact to the future state of data sharing and interoperability among the end user community.

This report describes 5G technologies and enablers as defined by relevant standards. This report was scoped to describe the capabilities and characteristics of technologies, including impacts and challenges to interoperability and other implications to the public safety community. Cybersecurity considerations

are outside the scope of this report due to the multitude of potential permutations to set up and implement. While Cybersecurity is a critical component of any network and should be designed and engineered upfront, the purpose of this paper was to explore future evolving technological impacts. Therefore applying cybersecurity methods and mitigations were considered premature at this phase. Cybersecurity is a critical factor and should be incorporated in the next phase of investigation. End users in the public safety community rely on information exchange and depend on integrity and availability of data. Furthermore, public safety users must trust their information to perform their daily duties. This inherent trust can only be enabled through incorporating best practices and methodologies rooted in cybersecurity.

The use case is described from a systems view perspective, detailing the various operational components that will arrive on the scene and need to communicate and coordinate as well as various remote supporting entities. This includes the school resource officer, law enforcement, fire and rescue, emergency medical services, incident and unified command personnel, and the Public Safety Answering Points (PSAP). The mobile and the on-body systems are described along with the transport networks and the information they exchange.

Video dissemination will be scoped as sourced from three sources including fixed cameras within the school, an Unmanned Aerial System (UAS) launched via the incident commander, and responding unit's body-worn cameras. The systems view will first be described as it would under current operational conditions with little to no 5G components present. Two additional progressions in time are then provided which describe a mid-term scenario with limited 5G operational components and a future scenario where many of the visionary elements of 5G technologies have been placed into the environment. In order to prepare for this systems view, the following section takes a dive into each of the 5G enablers.

3 5G ENABLERS

As previously noted, one of the most important components of interoperable solutions for the public safety community is strict adherence to standards and common interfaces. The next generation 5G mobility networks are entirely dependent on standards for world-wide ubiquity of access and interoperability among the public; however, there is no single Standards Development Organization (SDO) which governs all aspects of the 5G vision. The primary organizations for solutions discussed in this report include the Third Generation Partnership Project (3GPP)[7] and European Telecommunications Standards Institute (ETSI)[8]. The 5G ecosystem however includes many others including the Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)[9], Internet Engineering Task Force (IETF)[10], Open Networking Foundation (ONF)[11], and Open-Radio Access Network (O-RAN) alliance[12], MEF[13], among others.

The 3GPP is the primary SDO for all 5G radio access, Core Network (CN), and service capabilities. The 3GPP unites seven telecommunications SDOs including ARIB[14], ATIS[15], CCSA[16], ETSI[17], TSDSI[18], TTA[19], and TTC[20], and provides their members with a stable environment to create Reports and Specifications that define 5G technologies. 3GPP is influenced by a set of industry associations and their members, including the GSMA[21], NGMN[22], CTIA[23], 5G Americas[24], TIA[25], among others. These industry associations are comprised of both mobile broadband vendors such as Samsung, Ericsson, Nokia, and Qualcomm, as well as carriers such as AT&T, Verizon, and T-Mobile who ultimately contribute to the 5G specifications through implementation trials and deployments. This ecosystem of 5G standards development is illustrated in Figure 8.

[7] https://www.3gpp.org/about-3gpp
[8] https://www.etsi.org/about
[9] https://standards.ieee.org/
[10] https://www.ietf.org/
[11] https://opennetworking.org/
[12] https://www.o-ran.org/
[13] https://www.mef.net/
[14] https://www.arib.or.jp/english/
[15] https://www.atis.org/
[16] http://www.ccsa.org.cn/english/
[17] https://www.etsi.org/
[18] https://tsdsi.in/
[19] http://www.tta.or.kr/eng/
[20] http://www.ttc.or.jp/e
[21] https://www.gsma.com/
[22] https://www.ngmn.org/
[23] https://www.ctia.org/
[24] https://www.5gamericas.org/
[25] https://tiaonline.org/

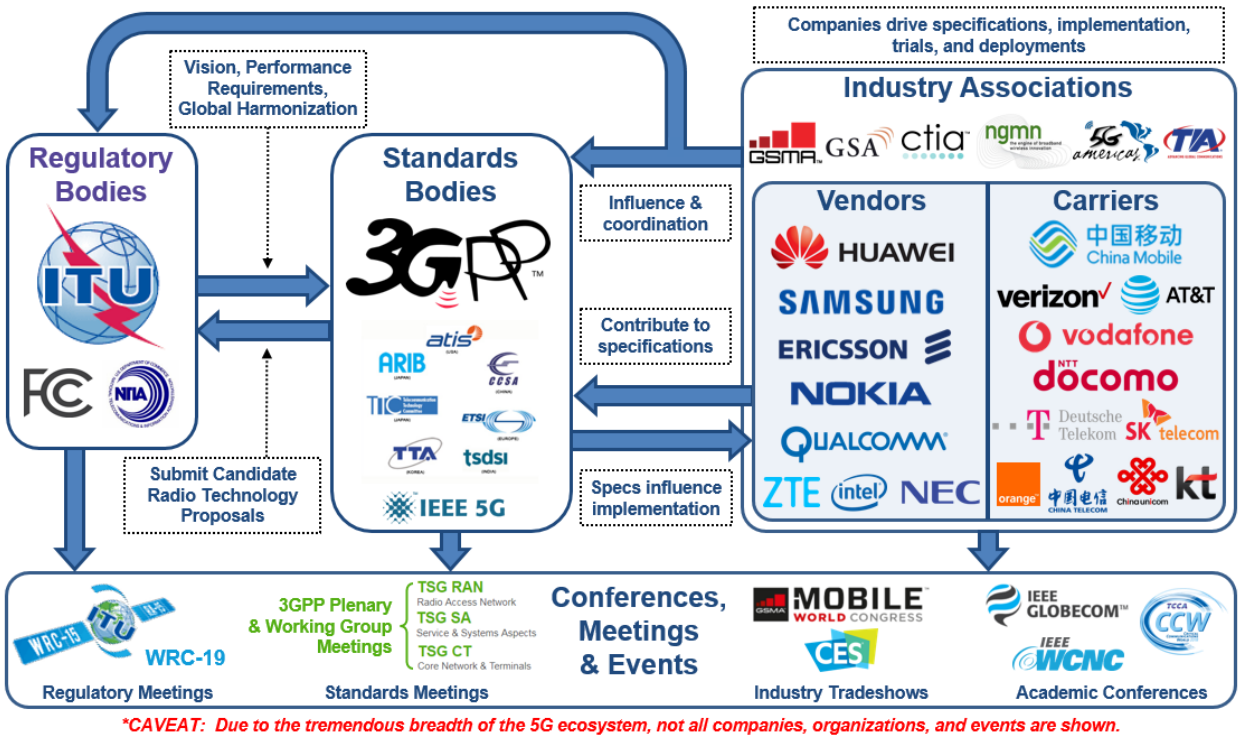


Figure 8 – 5G Standards Ecosystem

3GPP develops standards through Technical Specification Groups (TSGs) and Working Groups (WGs). Among the working groups, the Radio Access Network (RAN) specifies all physical layer and link layer radio resource control, the CN and Core Terminals (CT) specifies all user equipment, interworking functions, and APIs, and the Service and Systems Aspects (SA) specifics the service requirements and the architecture related to 3GPP systems[26].

The 3GPP specifications follow a "release" schedule where relevant concepts are set forth as agenda items following past studies performed in working groups. The technologies relevant to that release are then discussed and agreed upon by all contributing 3GPP members. The 4G/LTE specifications were introduced as Release 8 in 2008 and continued to evolve in current releases to ensure backwards compatibility. The 5G specifications were first introduced in Release 15 completed in 2019. Release 16 was completed in 2020 and release 17 is under development now. Some of the features associated with each release are shown in Figure 9. It should be noted that most mobility networks deploying 5G today are only compliant with Release 15 specification and it will likely be years before advanced features of Release 16 and 17 are deployed operationally.

[26] Note: there are numerous 3GPP Technical Standards (TS) and Technical Reports (TR) which describe the 5G systems, interoperability, security, use cases, etc. The TS23.501 is however the primary systems architecture specifications. For a complete list, follow the specification numbering guideline: https://www.3gpp.org/specifications/specification-numbering

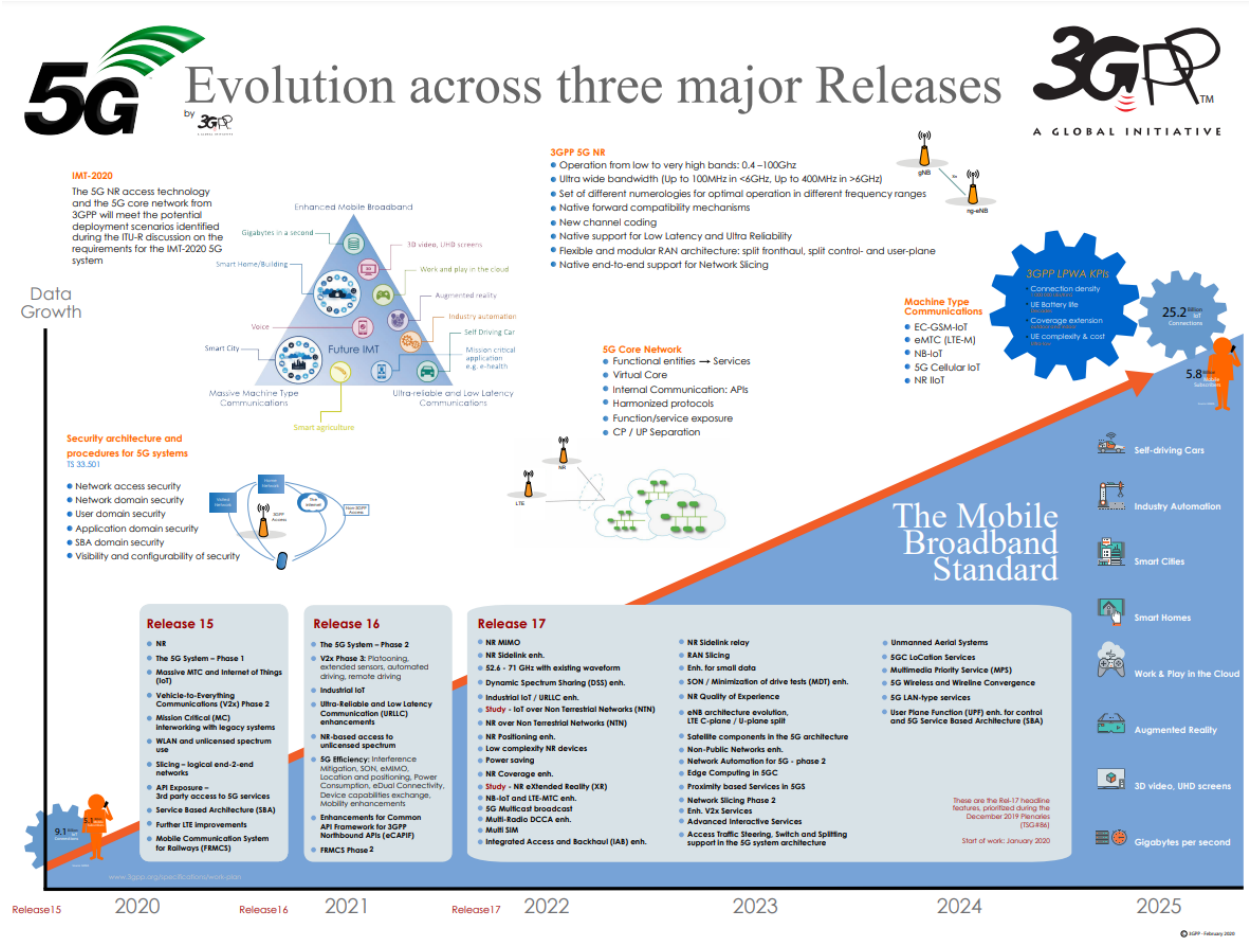


Figure 9 – Evolution of 5G across three major Releases[27]

The ETSI group has developed use cases and specifications for several important aspects of 5G, namely the NFV[28], MANO, and MEC[29]. The specifications for NFV and MANO have long been leveraged by enterprise data centers and cloud computing environments to develop more robust, secure, and resilient network services. As data centers evolved from tens of servers to hundreds of thousands of servers and virtualization was embraced to ensure high availability and dynamic flexibility, so did network functions. The NFV and MANO specifications provide the terminology and main concepts for virtualization of network functions along with various use cases, proof of concepts, and an overarching architectural framework. They further define how virtual network functions are defined as service descriptors using common programming languages, how they are instantiated and managed, and how they interact with the underlying physical hardware. The NFV and MANO concepts will be key to enabling the 5G service-based architecture. To enable improved support for 5G, the ETSI specifications are developing new standards which describe interoperability with network slicing and other resilient networks.

The ETSI MEC specifications describe how enterprises and cloud computing environments should approach edge computing in general, and similar to the NFV and MANO specifications, provide the

[27] https://www.3gpp.org/about-3gpp
[28] https://www.etsi.org/technologies/nfv
[29] https://www.etsi.org/technologies/multi-access-edge-computing

terminology and main concepts along with various use cases, proof of concepts, and the overarching architectural framework. Some of the very important aspects of MEC include the application enablement and service APIs which allow for automation and lifecycle management of applications. With relation to 5G, new MEC specifications further describe integration with a business enabled, service orchestration and network slicing.

As noted previously, there are many other SDOs which play a role in the larger 5G ecosystem. The IEEE SA has developed solutions for both wired and wireless networking access methods as well as security mechanisms, which will play a crucial role in access to 5G networks from non-3GPP network types such as Wi-Fi. The ONF has developed many specifications and reference designs for Software Defined Networks (SDNs) which will be crucial for advanced routing and transport of information through the 5G networks. The IETF has developed for years many aspects which govern modern networks, enterprise datacenters, and the internet at large. With regards to 5G, the IETF is developing specifications which describe autonomic networks, virtualization, and the various data models and descriptor languages for defining virtual network functions. The MEF is developing a large set of reference points and APIs to enable complete service lifecycle orchestration, which will be leveraged by both NFV and MEC applications.

The 5G standards ecosystem is broad and complex and goes well beyond just 3GPP in order to enable the vision of eMBB, mMTC, and URLLC use cases. As 5G evolves, it will be necessary to track these organizations to ensure interoperable solutions follow strict adherence to specifications. Table 1 includes a list of the most relevant SDOs and their corresponding technologies.

Table 1 – Standards Development Organizations relevant technologies and specification identification.

Standards Development Organization	Technologies
3rd Generation Partnership Project (3GPP)	5G Core and Radio Access Networks, Service-Based Architecture (SBA), Network Slicing, Non-Public Networks (NPN)
European Telecommunication Specification Institute (ETSI)	Network Function Virtualization (NFV), Management and Orchestration (MANO), Multi-access Edge Computing
Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)	802.x Local Area Networks (LAN), Personal Area Networks (PAN), Metropolitan Area Networks (MAN), Wireless Local Area Networks (WLAN) and Security[30]
Internet Engineering Task Force (IETF)	Network Descriptor Data Models including NetConf and Yang
Open Network Foundation (ONF)	Software-Defined Networking
Open-Radio Access Network (O-RAN) Alliance	Virtualized Radio Access Networks (vRAN) Solutions
MEF	Lifecycle Service Orchestration (LSO)

[30] Common IEEE 802.x standards include 802.1 for secure network access control and authentication, 802.3 for LAN Ethernet, 802.11 for WLAN including Wi-Fi, and 802.15 for PAN technologies such as Bluetooth and ZigBee. Some of the more recent 802.11x WLAN standards that will play a large role in 5G interoperability include 802.11ax (Wi-Fi 6), 802.11ay (WiGig), and 802.11be Extremely High Throughput (EHT) of Wi-Fi 7.

3.1 5G ARCHITECTURE

3.1.1 5G SERVICE BASED ARCHITECTURE

5G brings a transformational change to its core architecture. 5G introduces a new Service-Based Architecture (SBA) that defines all new NFs as offering their services over common standardized interfaces. The original CN elements in 4G have been reorganized into NFs and designed with control plane and user plane separation. This new architecture is defined in the 3GPP Technical Specification (TS) 23.501 and depicted in Figure 10 (Reference [10]). The cloud-native approach of SBA allows NFs to operate flexibly in virtualized environments transforming the way networks are deployed and orchestrated. Now carriers can move away from a one-size-fits-all network to a set of customizable networks that are dynamically instantiated for distinct use cases. For more details on 5G SBA, as well as options for roaming architecture, see Appendix B.1

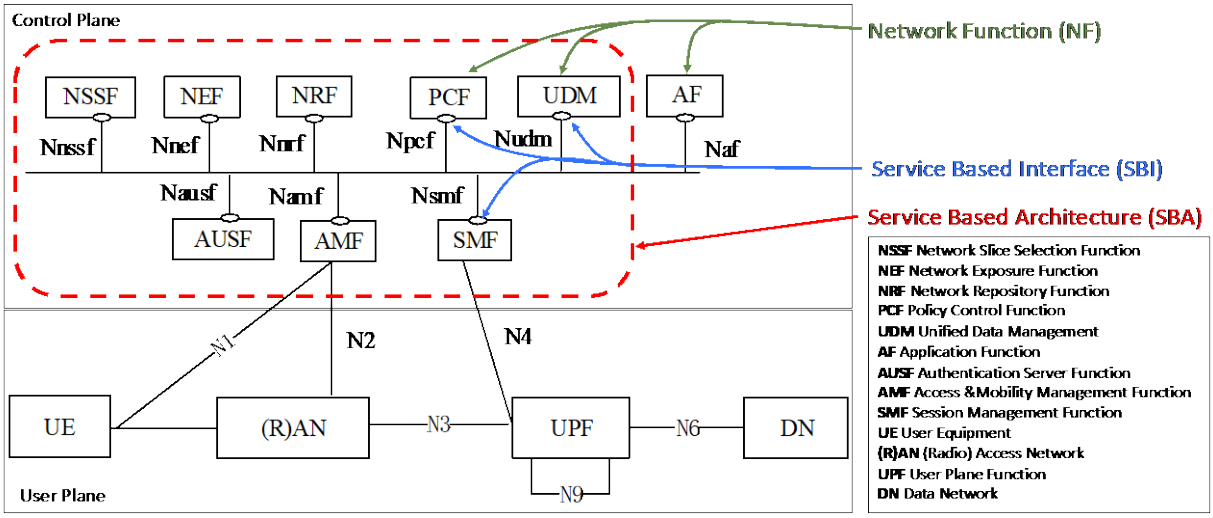


Figure 10 – 5G System Architecture (non-roaming reference architecture)

The 5G SBA utilizes microservice technology. Microservice technology refers to an architectural design pattern which breaks down a system into small granular, highly cohesive, and loosely coupled services. These self-isolated services each provide a specific function to the system as a whole and together comprise the 5G system. The interfaces among these microservices are lightweight and utilize common Application Programming Interfaces (APIs). 5G NFs are broken down into services, which each have their own specific Service-Based Interface (SBI). Service functions have to register as producer or consumer of a given service. Now the CN can use messaging protocols (e.g. HTTP/2, TLS, etc.) commonly adopted in the cloud community to communicate over the SBIs. The benefits of a microservice design for 5G is that it provides flexibility, granularity, and independent scaling. Additionally the independence of NFs means that services can be easily changed or upgraded following common "agile" cloud-native principles, including Security Development Operations (SecDevOps), and Continuous Integration/Continuous Delivery (CI/CD) to drive innovation and agility across the network infrastructure.

The 5G System Architecture (5GSA) is designed with control plane and user plane separation (CUPS) as shown in Figure 10. This allows NFs responsible for control plane signaling and NFs responsible for user applications to be deployed independent of each other. In turn, deployment models can be more flexible.

For instance, user plane functions can be pushed closer to the edge of the network for traffic steering purposes, while control plane functions can remain more centralized. It also provides the option to isolate network resources to meet demand of user applications independent of the control plane resources that may be shared.

For context, the user plane data in Figure 10 traverses four main elements within the 5G system, the User Equipment (UE), Radio Access Network (RAN), User Plane Function (UPF) and Data Network (DN). The UE represents 5G devices connecting to the network. The RAN consists of a Next Generation NodeB (gNB), the 5G base stations that serve as the wireless access points to the 5G network. The UPF is the core NF that connects the user plane flows from the UE to the DN. The DN represents the data network that provides the subscriber's desired service and application. The UPF provides the flexibility to steer traffic to the most optimal DN including any edge cloud resources, and further applies any traffic filtering or quality of services parameters. Multiple UPFs can be deployed by the 5G control plane to achieve very dynamic end-to-end information transport.

Two key control plane functions are the Access and Mobility Management Function (AMF) and the Session Management Function (SMF). The AMF receives control plane messaging from a UE and manages connectivity, registration, authentication, and authorization to the 5G network. The SMF manages the data session between UEs and DN including policy control. The SMF sets configuration parameters in the UPFs that provide traffic steering for a UE to an edge DN. In the CUPS architecture, the SMF and AMF can be independently scaled as well as the UPFs as needed. They can also be placed in geographically different locations to improve performance and resilience. For more details on the 5G UP and CP NFs shown in Figure 10, see Appendix B.2.

The 5G SBA is a key pillar for all 5G functionality and enables many of the new features of 5G including multi-access edge computing, non-public networks, network slicing, and business driven management and orchestration. The NGMN Alliance highlights four key features about the SBA that are critical to realizing the other 5G enablers (Reference [11]).

1. Operational – the cloud-native approach of SBA and the decoupling of NFs allow operators to leverage cloud delivery models like continuous integration and orchestration to build and change production networks more quickly and with automation
2. Extensibility – common standardized interfaces (e.g. SBI) and messaging protocols (e.g. HTTP/2) allow plug-and-play of NFs as new features/services are added or as resources need to be scaled
3. Modularity – the independence and virtualization of NFs enables on-demand and flexible deployment models (e.g. edge computing, network slicing) customizable for different use cases
4. Openness – the service-based registration and authorization framework facilitates observability into the core functions and seamless integration of 3rd party applications with 5G core to enable next-gen use cases

3.1.2 5G Radio Access Network Disaggregation

Another important aspect of 5GSA is the disaggregation of the 5G Radio Access Network (RAN) as illustrated in Figure 11 (Reference [12]).

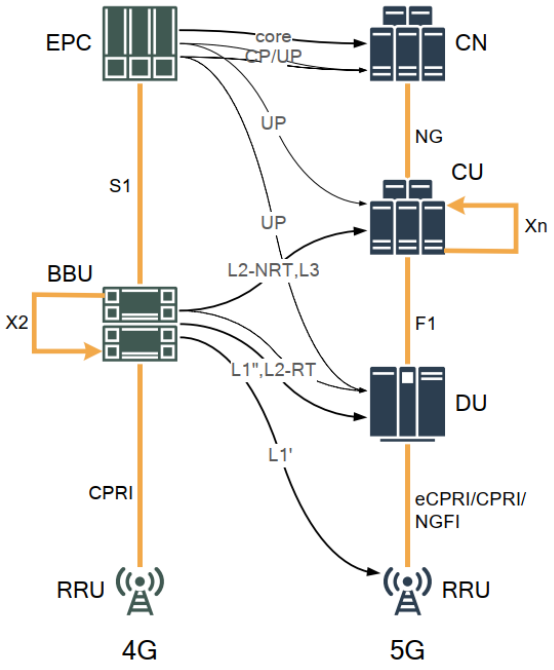


Figure 11 – Evolution from single purpose 4G Evolved Packet Core (EPC) to a split 5G infrastructure

This figure illustrates the core components of the 4G/LTE network on the left, including the Evolved Packet Core (EPC), Base Band Unit (BBU), and Remote Radio Unit (RRU), being disaggregated to new 5G components on the right, namely the CN, Central Unit (CU), Distributed Unit (DU), and RRU.

The CU will perform the upper Layer 2 and above processing and routing and the DU will perform the lower Layer 2 and PHY layer processing traditionally performed by the BBU. The DU will support tens of Remote Radio Units (RRUs) at a single facility and the CU will support tens of DUs, and thus hundreds of RRUs. It is likely that the DUs in 5G architecture will be hosted in what looks like traditional base stations today, located only a few kilometers from the RRUs. However, the CU will likely be hosted at distributed datacenters throughout a metropolitan area, and thus very close to additional compute and storage resources that will enable edge computing.

In the 4G/LTE networks, traffic was tunneled back to the EPC before it would route to the internet. This resulted in often long delays. While the DU serves primarily as a PHY layer processor, handling both Control Plane (CP) and User Plane (UP) traffic, the CU now can host virtualized 5G UP NFs such as the UPF providing the flexibility for dynamic steering and load balancing of user traffic to edge computing centers. This speaks directly to the 5G SBA architecture's CP/UP split functionality and is expected to greatly improve the latency and quality of experience.

3.1.3 5G Mission Critical Services

The 5G SDOs are actively engaged in developing the capabilities to enable mission critical services within the networks. The SA WG6 (SA6) is specifically responsible for the coordination of Mission-critical applications related to 3GPP standards. 3GPP developed a comprehensive set of specifications for next generation mobility networks that standardized Mission Critical (MC) Service specifications in 2013. Since then, the MC Service specifications were continuously developed and refined to support greater

capabilities. FirstNet and other dedicated 3GPP Public Safety networks will use these specifications to provide MC Services to public safety.

Early 3GPP work defined the requirements for High Power User Equipment (HPUE) in order to improve the operational characteristics and to support longer communication range, specifically in FirstNet's private Band 14 spectrum. In Release 12, Device to Device (D2D) Proximity Based Services (ProSe) and Group Communications System Enablers (GCSE) were defined to support public safety communications.

The initial specifications for Mission Critical Push-to-Talk (MCPTT) standardized with Release 13. In Release 14, MCPTT was supplemented with additional enhancements and standardized Mission Critical Data (MCData) and Mission Critical Video (MCVideo). In Release 15, the first release of 5G systems, additional MC Services were further developed supporting interworking between legacy radios systems such as P25 and additional MCservice requirements for non-public safety entities. Release 16 further refines the specifications set in Release 15 but also introduces Mission Critical Multimedia Broadcast Multicast Service (MCMBMS) for mission critical applications and sets the stage to port 5G mission critical requirements from 4G. Additionally, the study of Mission Critical services support in the Isolated Operation for Public Safety mode of operation (MCIOPS) began, allowing public safety users the ability to maintain a level of communications from an isolated Evolved NodeB (eNB) that is not connected to a CN. Release 17 scheduled for the end of 2021 refines specifications for non-first responder entities, targets the specifications for MCIOPS and continues the study of MCOver5G.

Table 2 lists the various standards associated with mission critical services over mobile broadband networks:

Table 2 – 3GPP Standardized 5G Mission Critical Services

Specification ID	Name
TS22.179	Mission Critical Push to Talk (MCPTT); Stage 1 (Rel 16 2019)
TS22.280	Mission Critical Services Common Requirements (MCCoRe); Stage 1 (Rel 16 2020)
TS22.281	Mission Critical Video (Rel 16 2018)
TS22.282	Mission Critical Data (Rel 16 2018)
TS23.280	Common functional architecture to support mission critical services; Stage 2 (Rel 16 2019)
TS23.281	Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2 (Rel 14 2016)
TS23.282	Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2 (Rel 14 2016)
TS23.379	Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2 (Rel 14 2016)
TR23.783	Study on Mission Critical (MC) services support over the 5G System (5GS) (Rel 17 2021 Draft)
TS29.582	Mission Critical Data (MCData) interworking with Land Mobile Radio (LMR) systems; Stage 3 (Rel 16 2020)

3.1.4 IMPACT TO PUBLIC SAFETY

Unlike previous generations, the 5G architecture is not a one-size-fit-all solution for data and services, rather it is a paradigm shift in its underlying design providing the ability to optimize for varying use cases such as eMBB, URLLC, and mMTC. 5G SBA and network disaggregation enables the ability for public safety and first responders to utilize concepts like MEC, network slicing, and non-public (private) networks which will be explained in the coming sections. An architecture that is operational, extensible, modular, open, and disaggregated enable use cases like information sharing for an active shooter scenario. It will further enable the quality of experience that is characterized by reliable, real-time, and efficient mission driven transport.

3.2 NETWORK FUNCTION VIRTUALIZATION AND MANAGEMENT AND ORCHESTRATION

The concepts of virtualization and cloudification, will play a vital role in the 5G architecture and its ability to heal, scale, and ensure robust and resilient operations with guaranteed quality of service[31]. Although not directly under the scope of the 5G 3GPP SDO, they are discussed here for clarity. The 5G community has universally adopted Network Function Virtualization (NFV) as a means to simplify and automate deployments of both 5G SBA and RAN, as well as third-party services offered throughout the 5G network. NFV involves separating NFs from the hardware they run on using virtual infrastructure such as cloud computing and hypervisors. This means a common computing and storage platform can host a plethora of NFs avoiding single purpose vendor locked hardware. Additionally this promotes ease of deployments and upgradability. The cloud environments that host Virtual Network Functions (VNFs) is known as NFV Infrastructure (NFVI) and includes all physical resources such as compute, storage, and networking components. The NFVI can be distributed which aligns well with network slicing, multi-access edge computing, and disaggregated 5G RAN architecture to meet locality and latency requirements.

3.2.1 NFV SPECIFICATIONS

The ETSI has played a major role over the last 10 years in developing the use cases, architectural framework, and common interfaces that will govern NFV and Management and Orchestration (MANO). The generic architecture of NFV and the supporting infrastructure and management systems as defined by ETSI are illustrated in Figure 12 (Reference [13]). The various functional blocks include the VNFs and supporting NFVI, the Element Management System[32], Operations Systems Support (OSS) / Business Systems Support (BSS), and the NFV Management and Orchestration (NFV-MANO). The element management system controls the state of individual VNFs, the OSS/BSS provides overarching guidance to meet service provider needs, and the NFV-MANO governs the overall state of the architecture. Each functional block is connected by well-defined interfaces, the reference points, which describe the structure and information that must pass to ensure monitoring and control.

[31] Note that Software Defined Networks (SDN) will also play a vital role in 5G architecture and will be a key enabler for 5G flexibility and virtualization of both network functions and edge applications.

[32] Shown as EMS in the figure

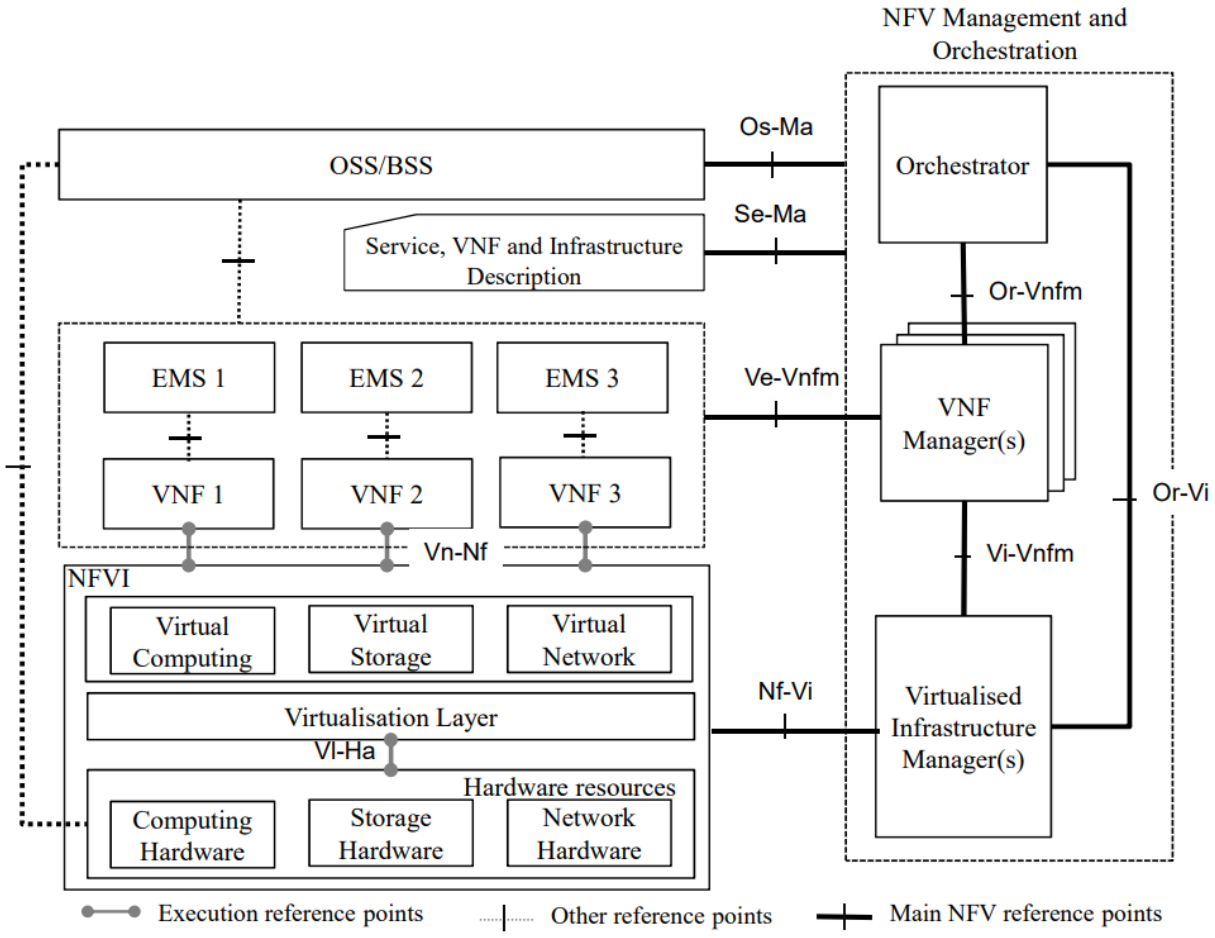


Figure 12 – NFV Reference Architectural Framework

The NFVI that hosts the VNFs is critical to its operation and is defined by ETSI (Reference [13]) and include both large scale commercial cloud infrastructure as well as on-premise private data-centers and hypervisors. The VNFs are dependent on the NFVI, and though they often support redundant and load balancing operations by default, they will experience disruption or outage if the underlying infrastructure experiences faults.

VNFs are designed to be rapidly deployed through automated controls and processes and monitored to meet defined Service Level Objectives (SLOs). The SLOs are described as either directly measurable objectives (e.g., guaranteed minimum capacity, minimum latency, maximum jitter, maximum packet loss, etc.) or indirectly measureable objects (e.g., security posture, path/node/network/geographic restrictions, maximum occupancy, etc.). VNF's configuration and functionality are defined entirely by a VNF Descriptor (VNFD) which are data models that describe the template configuration of the VNF, connectivity requirements, NFVI requirements, software or neighbor dependencies, and any SLOs. It can additionally include any artefacts necessary for the NS on-boarding and lifecycle management of its instances. Standardized data models include the Organization for the Advancement of Structured Information Standards (OASIS) Topology and Orchestration Specification for Cloud Applications (TOSCA) (Reference [14]), YANG (Reference [15] and Reference [16]), and NetConf (Reference [17] and [Reference

[18]). ETSI further defines the VNF packaging formats for vendor neutral delivery to service providers (Reference [19]) and various NFV descriptors based on YANG specification (Reference [20]).

3.2.2 MANO SPECIFICATIONS

VNFs alone come with a certain level of complexity and 5G networks will likely increase that through highly distributed deployments over large geographic regions. This complexity necessitates some form of automated management and control. This is provided by the Management and Orchestration (MANO) components standardized by ETSI (Reference [21]) and leverages many of the functional concepts and common interfaces defined by the MEF[33] Lifecycle Service Orchestration framework (Reference [22]). The 3GPP organization has further adopted these concepts and have begun to integrate into the larger 5G specifications as TS28.530 MANO Concepts (Reference [23]), TS28.531 MANO provisioning (Reference [24]), and TS28.533 MANO Architecture Framework (Reference [25]).

The MANO is responsible for the design, commissioning, real time monitoring and operations, and the decommissioning of a network service's lifecycle. This includes all policy management including the classical Fault, Configuration, Accounting, Performance, and Security (FCAPS) as well as the automated execution of internal and external operational aspects. The MANO further provides the end-user the location to configure these operations and business support systems (OSS/BSS) policies and controls.

The MANO architectural framework is illustrated in Figure 13 and includes the various functional blocks and data repositories as described in Table 3 . Both the VIM and VNFM expose northbound interfaces to the NFVO to allow global and coordinated control and delivery of NS.

[33] http://mef.net/

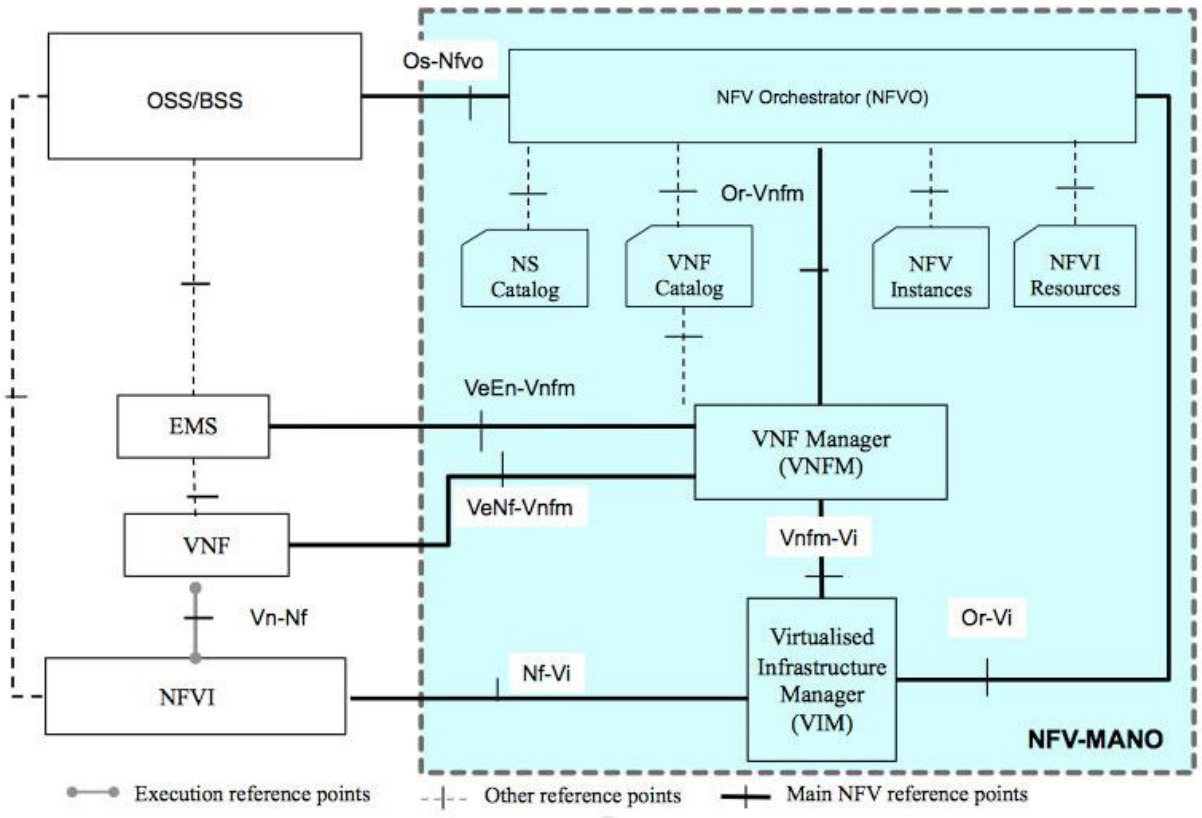


Figure 13 – ETSI Management and Orchestration (MANO) Architectural Framework (Reference [19])

Table 3 – MANO Functional Blocks and Data Repositories

Primary Functional Blocks	NFV Orchestrator (NFVO)	Orchestrates the lifecycle management of VNFs and their NS including capturing all health and state and triggering any scaling or recovery operations. Orchestrates actions for NFVI resources across multiple VIMs.
	VNF Manager (VNFM)	Executes the lifecycle management commands of VNF instances.
	Virtualized Infrastructure Manager (VIM)	Manages the NFVI hardware including compute, storage, and network resources.
Data Repositories	NS Catalogue	Repository for all on-boarded NS, supporting the creation and management of the NS deployment templates (Network Service Descriptor, Virtual Link Descriptor, Virtual Network Function Forwarding Graph Descriptor).
	VNF Catalogue	Repository of all on-boarded VNF packages, software images, manifest files, etc.
	NFV Instance Repository	Repository of VNF instances and NS instances represented by a VNF record and NS record. The records are continually updated by the state of the lifecycle.
	NFVI Resources Repository	Repository of available, reserved, and allocated NFVI resources supporting the reservation, allocation, and monitoring of the VNFs.

Common VIMs include enterprise cloud software such as Openstack[34], Kubernetes[35], or VMware[36], as well as commercial cloud environments including Amazon Web Services (AWS)[37], Google Cloud Computing Platform[38], or Microsoft Azure[39]. Numerous commercial and open source efforts exists to perform management and orchestration including ETSI's own Open Source Mano (OSM)[40] designed as a reference implementation of the various standards produced within its organization. One of the biggest proponents among the 5G community however is the Open Network Automation Platform (ONAP)[41], which includes a mix of the basic NFV and MANO components, but also includes features for control loop automation and advanced analytics supplemented via artificial intelligence as Illustrated in Figure 14.

[34] https://www.openstack.org/
[35] https://kubernetes.io/
[36] https://www.vmware.com/
[37] https://aws.amazon.com/
[38] https://cloud.google.com/
[39] https://azure.microsoft.com/en-us/
[40] https://osm.etsi.org/
[41] https://www.onap.org/

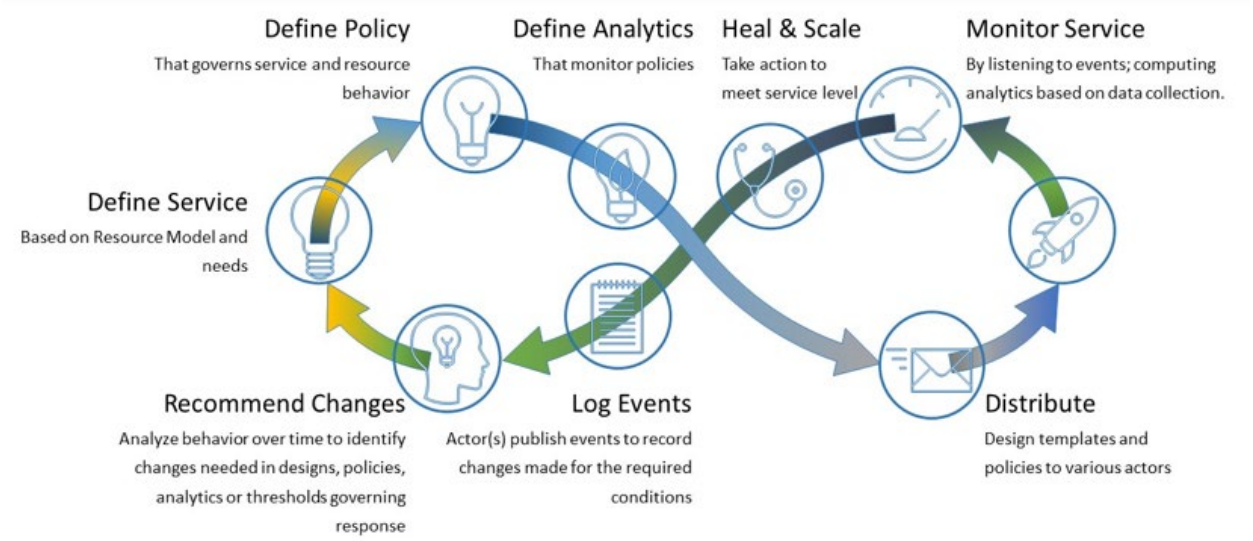


Figure 14 – Control loop automation with advanced analytics[42]

This aligns with the larger, long-term vision of 5G, which intends to leverage automation to deliver service-based, business driven functions to the end-user as described previously in Figure 5. While NFV itself is focused primarily on NFs (i.e., composable routers, firewalls, etc.), 5G MANO hopes to leverage the same concepts to drive edge applications and network slices described in the following sections.

3.2.3 IMPACT TO PUBLIC SAFETY

NFV technology virtualizes the network entities and functions found in previous mobile telecommunication architectures. The 5G architecture consisting of virtualized NFs running on virtualized infrastructure is the technology that specifically enables scaling up and down network services and deploying and removing these NF services in different locations with ease. Transparent white box virtualized infrastructure enables these virtualized functions to be deployed and removed while previous generations did not have that flexibility with opaque black box servers running proprietary hardware. MANO will provide the lifecycle management and control of these virtualized functions. Reemphasizing low latency, reliable, real-time 5G user experiences, the 5G network provides these characteristics through NFV and MANO technology. When a public safety incident occurs, the MANO will take initiative by deploying and allocating the proper network resources and network services to the users and in an edge location that can provide the experience desired. If network services go down, the MANO can self-heal by standing up new virtualized resources or functions and push back-up virtualized resources or functions into the primary role minimizing down time. The MANO can scale the resources at the scene as the event begins and can scale down as the scene is under control and the mission complete. MANO and NFV enables an efficient 5G system that only uses network function and services when needed.

3.3 MULTI-ACCESS EDGE COMPUTING (MEC)

Historically, accessing and sharing information on mobile broadband networks required traffic to travel to the carrier's CN before reaching the global internet where traffic would then route to the datacenter which was hosting the application content. This could result in latencies of up to seconds for information

[42] https://docs.onap.org/projects/onap-clamp/en/latest/

transport alone and cross many different systems and administrative boundaries, which reduces resiliency for mission critical services. MEC[43] is a concept that evolved from cloud computing where compute, storage, and networking services are placed closer to the edge of a network and closer to the user or application where the data is generated and consumed. MEC will play a significant role in 5G's ability to meet use case latency and ultra-reliability requirements by allowing application developers to place their services very close to the RAN. The enablers of edge computing include virtualization technologies, cloud infrastructure, and the ability for 5G networks to steer traffic to the most appropriate destination. MEC will further enable advanced analytics that drive the behaviors of the 5G network itself through tight integration with the 5GSA through exposed interfaces. These behaviors include:

- Optimization of network resources
- Automated lifecycle service orchestration
- Geographic and user centric control
- Policy and charging

Edge computing will provide the desired quality of service or quality of experience for these type of use cases. There is however, no "one-size-fits-all" deployment strategy for edge computing. Figure 15 shows an overview of the locations where edge computing may be deployed and ranges from regional and metropolitan data centers, to on premise local enterprise deployments, where users can access compute resources directly at the point of access (Reference [26]).

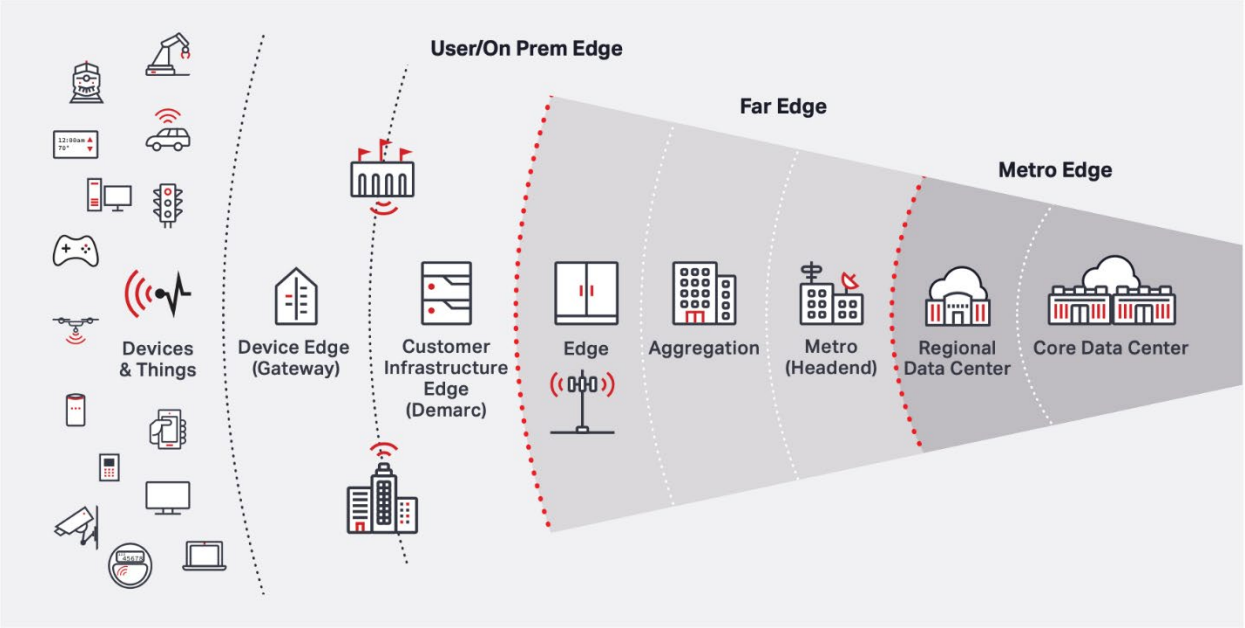


Figure 15 – Distribution of Edge Computing Implementation (Reference [26])

[43] Originally defined this as "mobile edge computing" but later changed the name to "multi-access edge computing" in 2017 to widen the access media and use of MEC to not only 3GPP networks but also WLAN networks like WiFi and other fixed-access technologies. For more information, see Appendix B.4.

3.3.1 MEC SPECIFICATIONS

While edge computing is a general concept, multi-access edge computing has been standardized by ETSI[44] as it relates to mobile broadband networks. The high-level framework of the MEC is described in GS MEC 003 and is shown in Figure 16 (Reference [27]). The framework includes three high-level layers as described in Table 4.

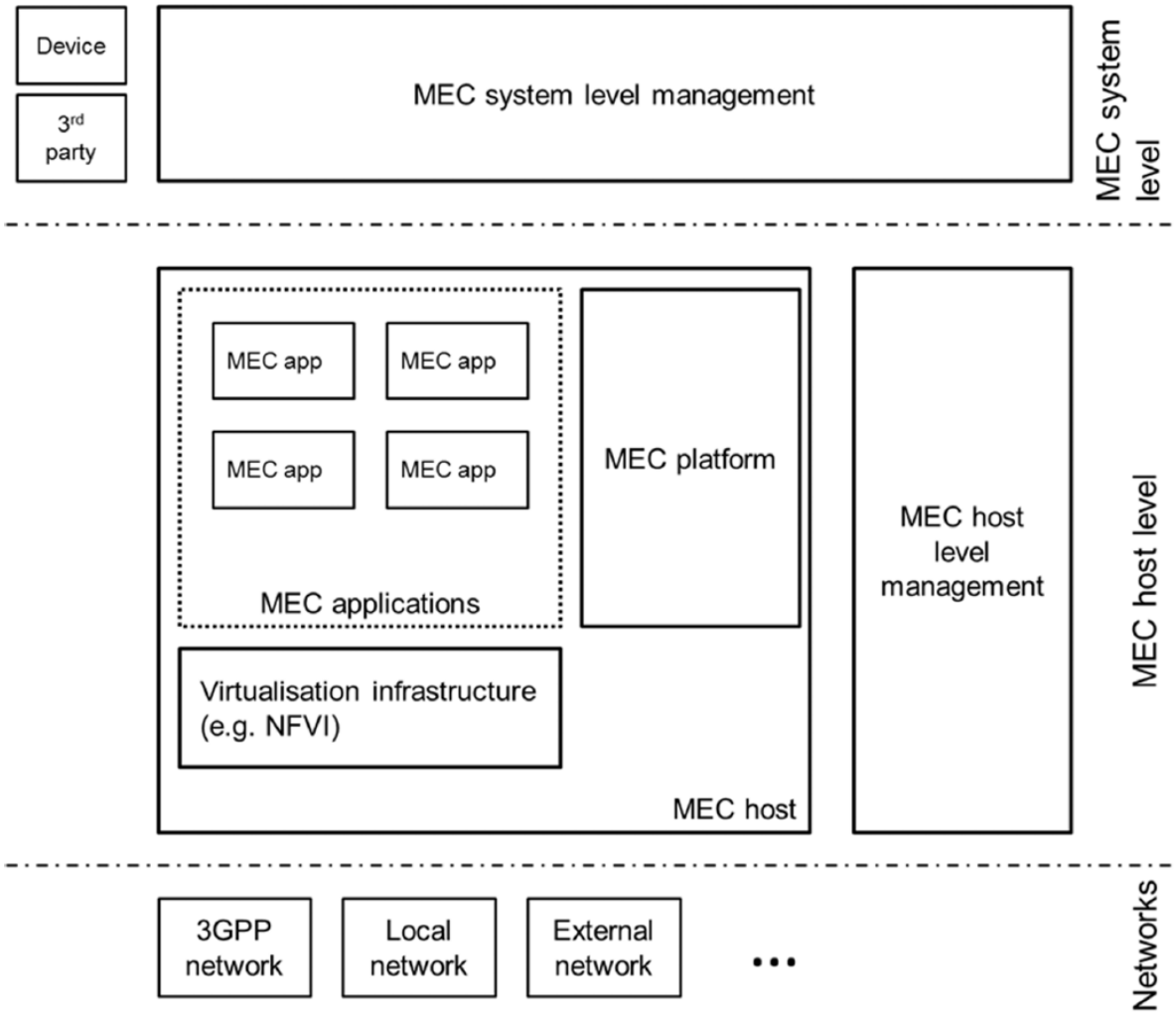


Figure 16 – ETSI MEC Framework (Reference [27])

[44] https://www.etsi.org/technologies/multi-access-edge-computing

Table 4 – MEC Framework Functional Layers

Layer	Function
System Level	Handles all MEC lifecycle management and orchestration of both applications and MEC infrastructure. Provides the user interface for OSS/BSS operations.
Host Level	Performs all management of the individual host that contains the MEC applications. Includes host level Virtualized Infrastructure Management (VIM) and application lifecycle management.
Networks	Serves as the attachment point to any access network providing users access to the MEC applications

MEC enables the implementation of applications as software-only entities that run on top of a virtualized infrastructure, which is located at or close to the edge of the network. Figure 17 shows the reference architecture which includes the functional elements of the MEC system and the reference points between them. The Mp reference points provide the MEC platform functionality. The Mx reference points lead to external entities. Lastly, the Mm reference points relate to management interfaces.

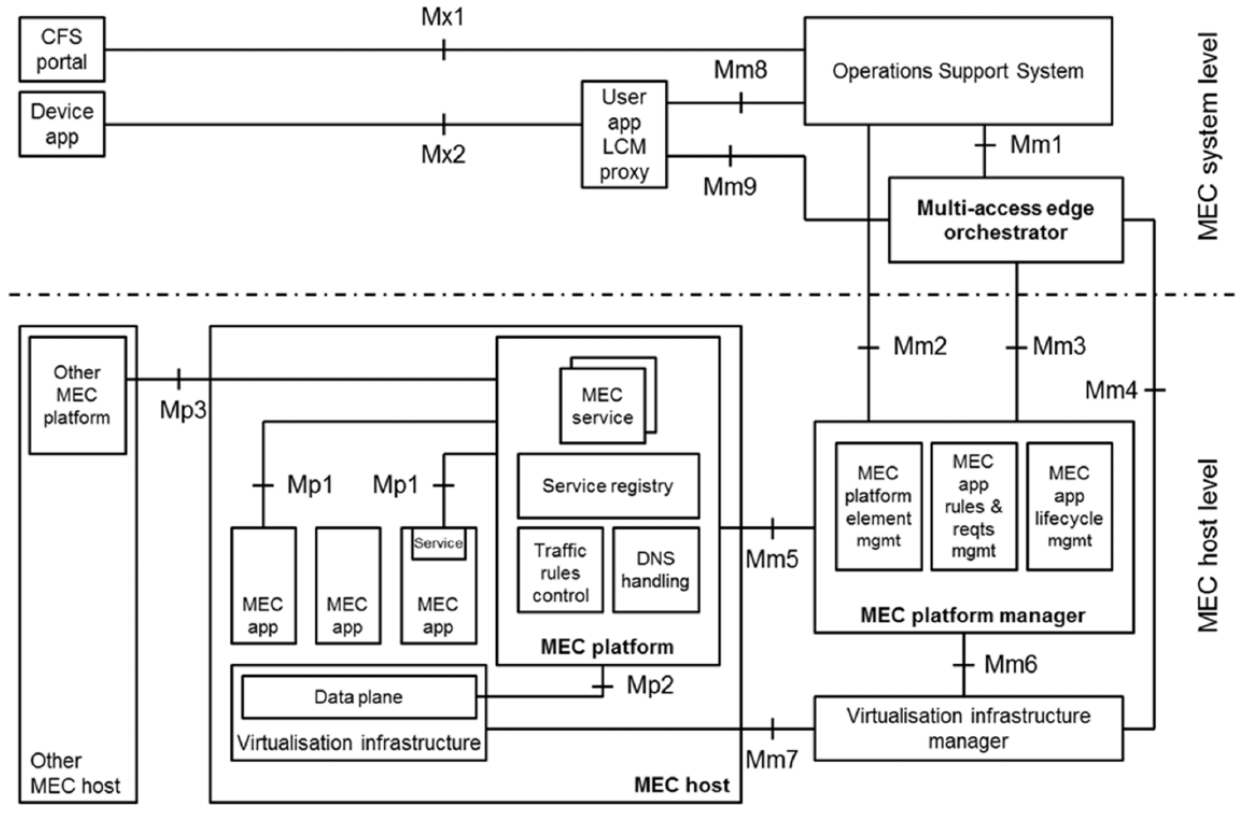


Figure 17 – ETSI MEC Architecture (Reference [27])

The MEC system consists of the MEC host and the MEC management necessary to run MEC applications within a network. The MEC host is an entity that contains an MEC platform and infrastructure consisting of compute, storage and networking resources that host virtualized applications. The MEC platform

facilitates all functionality of the applications including configuration, registration, and advertisement. MEC applications are instantiated on the virtualized infrastructure of the MEC host and are activated based on configuration and valid requests approved by MEC management.

MEC and NFV are complementary concepts. MEC architecture has been designed so that there are a variety of different deployments that are possible. The diagram below in Figure 18 shows a possible deployment where MEC applications and VNFs are deployed on shared infrastructure. It also shows re-use of the ETSI NFV MANO components fulfilling a part of the MEC management and orchestration tasks. The diagram shows that the MEC platform is deployed as a VNF and the MEC apps appear as VNFs toward the ETSI NFV MANO components. The virtualization infrastructure is deployed as an NFVI and is managed by a VIM defined by ETSI NFV architecture. The MEC Platform manager (MEPM) is replaced by the MEC Platform Manager-NFV (MEPM-V) and delegates the VNF lifecycle management to one or more VNF Managers. The MEC orchestrator (MEO) is replaced by a MEC application orchestrator (MEAO) that relies on the NFV Orchestrator (NFVO) for resource management.

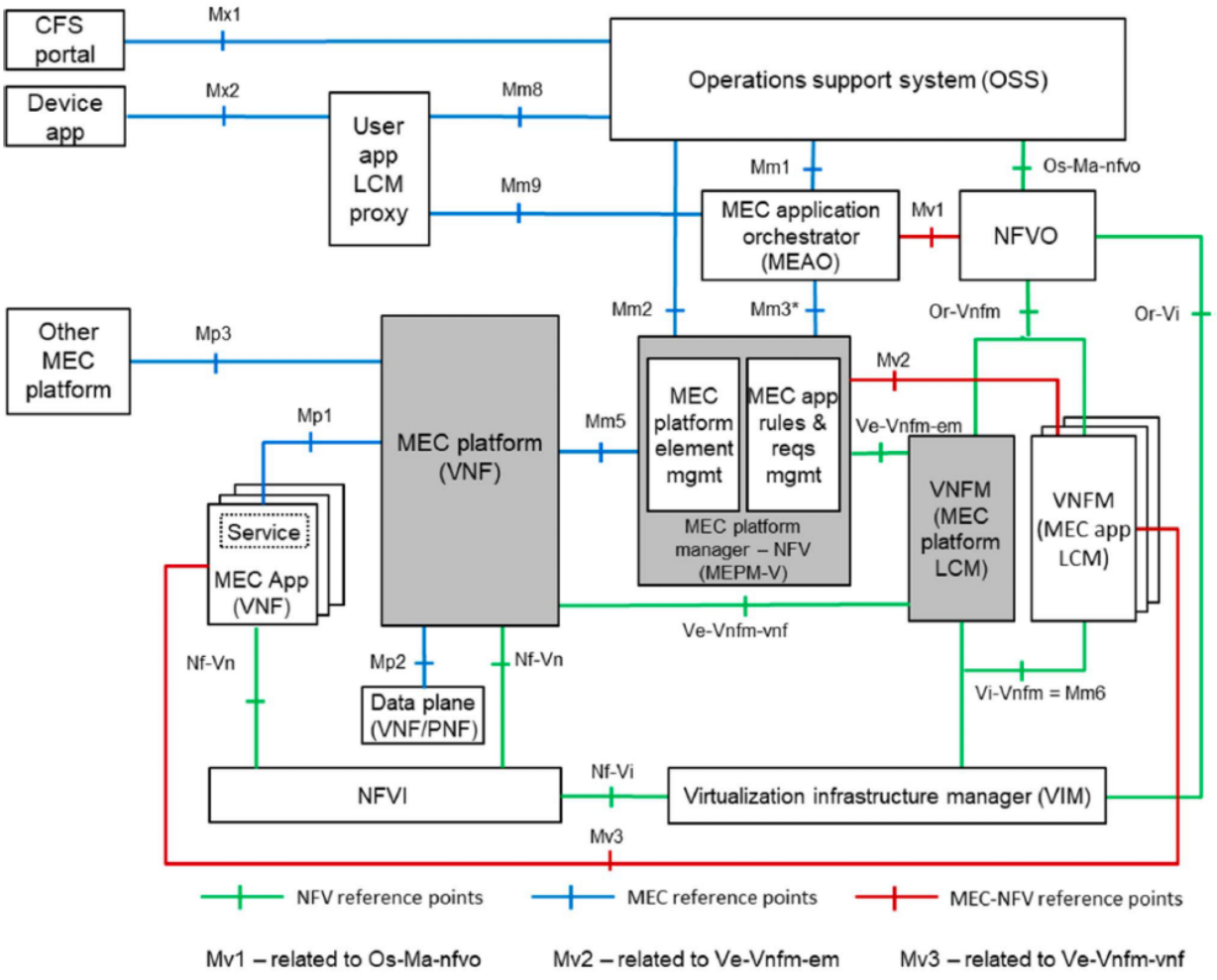


Figure 18 – Multi-access edge system reference architecture variant for MEC in NFV (Reference [27])

The 3GPP 5GSA and the ETSI MEC architectures are also complementary to each other. Integration of the MEC framework into the 5G systems architecture is described in ETSI GR 031 (Reference [29]). The 3GPP

5GSA specification describes how the MEC architecture integrates with the core SBA (Reference [10] and is shown in Figure 19 from an ETSI whitepaper on MEC in 5G networks (Reference [28]).

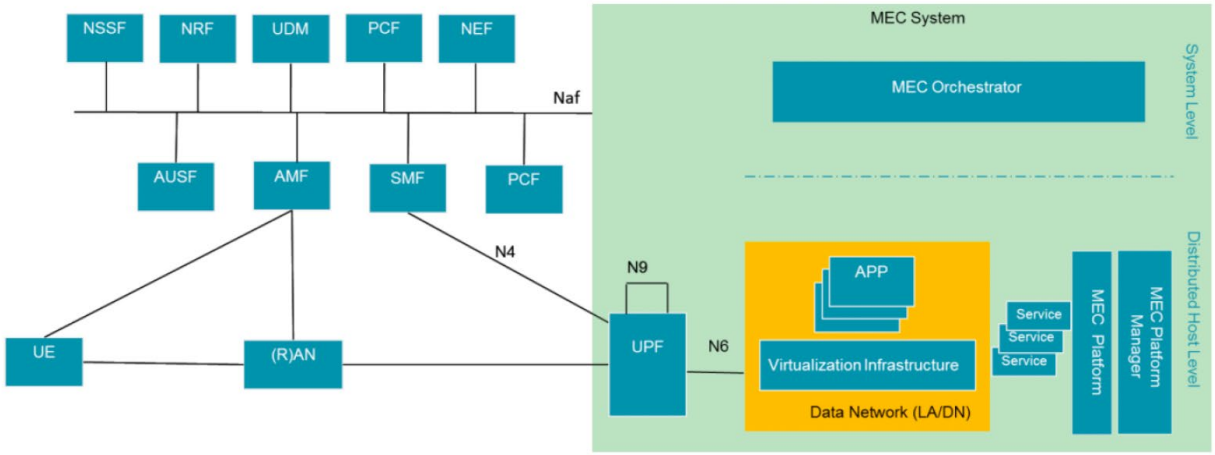


Figure 19 - Integrated MEC deployment in 5G Network

It should be noted here that the System Level MEC Orchestrator is separate from all user plane functionality and will likely be centrally located with the 5G CN. This allows for central management of disparate deployments of Host Level platforms that are located near the edge of the network. User plane traffic to an MEC application is accessed via the 5G UPF N6 interface to an external Data Network (DN). This is the same interface that the UPF would normally steer traffic to the internet in the CN, however for MEC the UPF is located closer to the user and thus steers traffic locally providing reduced latency. This speaks directly to the flexibility offered in a 5G SBA where the UPF may be deployed as a single element far away from the control elements, and very near to the RAN and MEC DN.

The MEC operating in a 5G network is viewed as an Application Function (AF) and thus has the ability to influence 5G CN behavior such as routing and resource selection. This is accomplished via the system level MEC components communicating with the 5G control plane functions. In a trusted AF scenario, the MEC has authority to interact directly with the 5G Policy Control Function (PCF) to request or trigger how user traffic is handled for the MEC application. In an untrusted AF scenario, adaptive behavior is limited as MEC applications must communicate through a proxy Network Exposure Function (NEF) to access services and capabilities provided by the 3GPP network. These NEF services can include the following capabilities:

- Monitoring
- Provisioning
- Policy and Charging
- Network Status Reporting
- Analytics Reporting

The tight integration between the 5G CN and the MEC will be very powerful to ensuring new services and capabilities are enabled within the 5G network and the vision of a business driven system is met. For more details on the various 5G enablers of MEC, see Appendix B.3.

3.3.2 MEC PHYSICAL DEPLOYMENT OPTIONS

The MEC system within 5G can be deployed in various locations as previously noted in Figure 15. It will be up to the carrier, carrier partners, or the enterprises themselves to deploy infrastructure based on their best judgement factoring in operational, performance, and security related requirements. Figure 20 shows four physical deployment options of MEC with 5G infrastructure. The MEC can be placed anywhere between the base station point of access and the 5G CN data center. The four deployment options are described as follows:

1. MEC and the local UPF collocated with the Base Station: farthest edge of the 5G network including enterprise on-premise deployment providing lowest latency and access to enterprise local network services
2. MEC collocated with a transmission node, possibly with a local UPF: far edge deployment with limited infrastructure, likely to collocated with the distributed unit as described in Section 3.1.2[45]
3. MEC and the local UPF collocated with a network aggregation point: far edge deployment likely to be collocated with the central unit as described in Section 3.1.2.
4. MEC collocated with the Core Network function (i.e., in the same data center): centralized deployment following existing mobile broadband networks providing limited latency improvement over existing models[46]

[45] Note this deployment scenario is unlikely as there will be limited hardware and management functionality to support the MEC at a distributed unit. Further the latency may not be improved as traffic would first travel to the UPF then steer back out to the MEC.

[46] The biggest improvement in this scenario will likely be seen as integrated resiliency including scaling and healing operation. Since the MEC will have AF integration with the core network, higher-level decisions can be made for selection and mapping of end users to MEC resources.

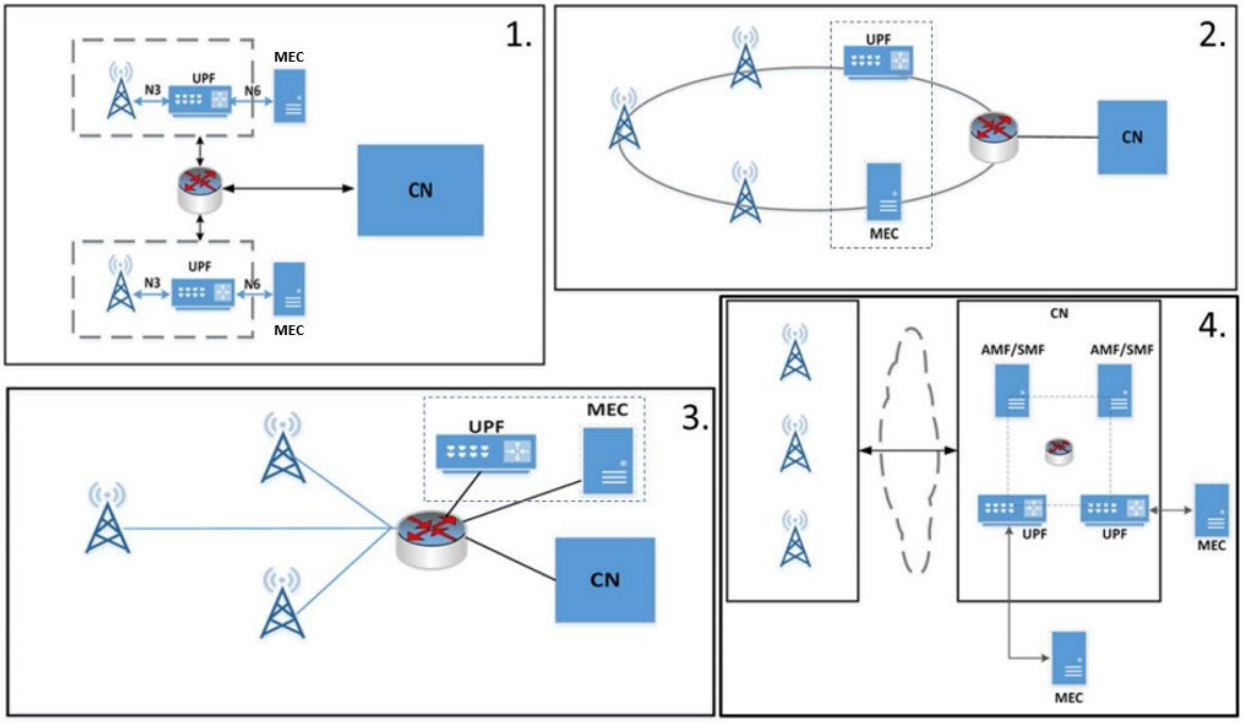


Figure 20 – MEC 5G Deployments (Reference [28])

3.3.3 IMPACT TO PUBLIC SAFETY

5G MEC is a key enabler for information sharing at the edge. This flexible, software-centric, virtualized, cloud native architecture standard provides the following benefits for the public safety and first responder:

1. It provides the standard to deploy virtualized infrastructure, functions and services needed to enable real-time, low latency, high-bandwidth applications at the edge
2. An efficient system at the edge that can scale up or down resources based on need
3. A system that can serve as an AF within the 5G architecture and dynamically influence traffic steering and 5G resource allocation to this edge system communicating with the 5G control plane
4. A system that can offload data sent over the transport backhaul
5. A system that can offload compute and storage from the UE

5G MEC and the 3GPP architecture are designed to be a "multi-access" architecture. As progress and breakthroughs in developments for non-3GPP access to the network are made, this will enable more interoperability and push MEC closer to the user by leveraging access media such as WLAN (i.e. Wi-Fi) technologies that are typically on-premise to access the 5G network. This will enable unified MEC deployments to support users on both mobile broadband and other network types.

5G MEC would provide the information sharing use case the ability to share high resolution video by placing the video application server within the MEC at the edge. It could push much of the compute and storage necessary for the use case whether on devices or vehicles to this edge server. Most importantly low latency is achieved by data being steered and processed at the edge server and not at the central

cloud location. Edge computing is important not only to 5G networks through 5G MEC but to all networks that desire to run applications that require low-latency and high bandwidth.

3.3.4 MEC CHALLENGES

5G MEC comes with many benefits as well as challenges to fully integrate, implement and deploy within the 5G system. ETSI currently lists multiple key issues with 5G and MEC integration and include the following (Reference [29]):

1. Traffic path update for mobility support
2. AF Influence on traffic routing
3. Information exposure for MEC Application Instances

Many of these relate to the integration between the 5GS and the MEC platforms and orchestrator. Because the 5G vision includes a very adaptive and hands-off approach to configuration and deployment, it will be necessary for each system to maintain a high level of knowledge of one another. This includes monitoring the health and state of each system, identifying and tracking connected UEs, and responding to real time requests of new service delivery. Many of the MEC deployments that exist today are still lacking in this tight integration among components.

A final challenge is the overall complexity and vendor interoperability. As the 5G network reaches further out close to the user, it requires coordination with third parties such as cloud providers and internet service providers. It requires technology innovations to implement these techniques according to the specification and the infrastructure that can support this design. This is not always possible as deployments often lag behind standards and vendors often make money from being first to market and offering “non-standard” features. This will remain challenging to the public safety community as they look to leverage MEC.

3.4 NETWORK SLICING

One of the most prominent features of 5G is network slicing. A Network Slice (NS) is formally defined as a logical network that provides specific network capabilities and network characteristics. Network slicing will permit operators to tailor the mobile network properties to a diverse range of vertical sectors, like healthcare, automotive, manufacturing, and public safety. Different verticals may have disparate service requirements in terms of attributes such as latency, data privacy, geolocation, and energy efficiency. Network slicing enables differentiated treatment per customer using multiple independent logical networks on top of a common shared physical infrastructure. Figure 21 illustrates an abstract example of the network slicing concept for three different vertical sectors.

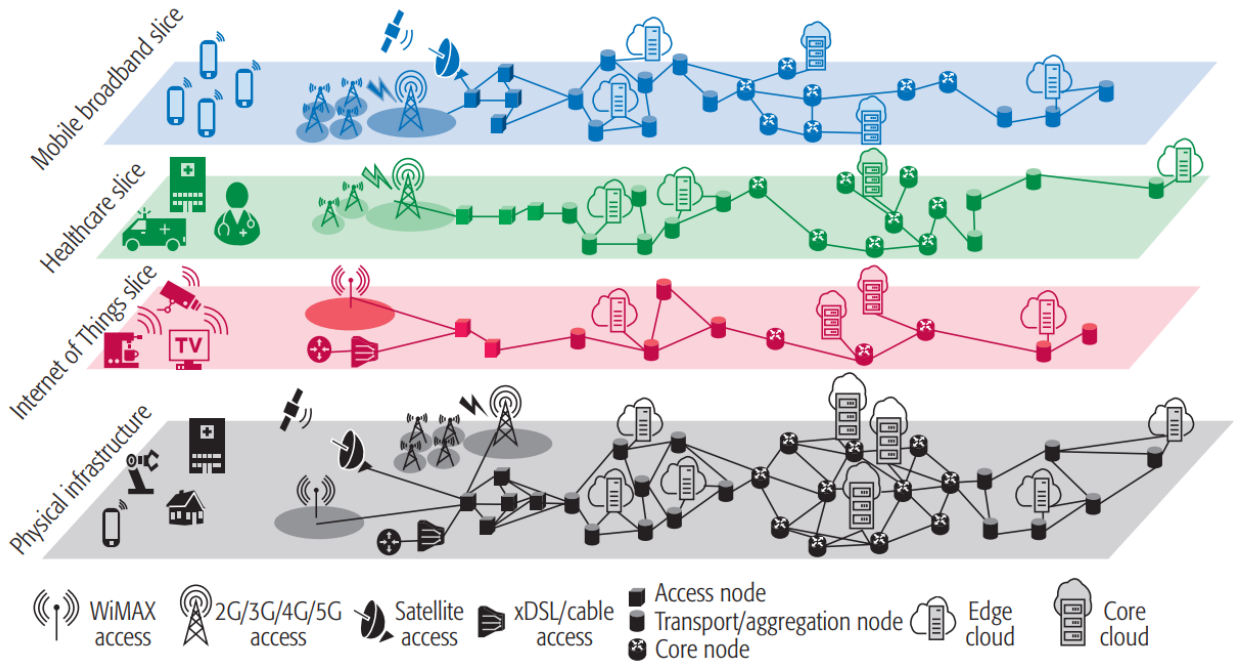


Figure 21 – 5G Network Slicing (Reference [30])

It is the 5G service based architecture and evolution of the CN and RAN that ultimately allow for 5G to be much more easily sliced than prior generations. Instances of virtualized NFs in the RAN, CN, and transport network can be independently deployed, scaled, and released with automated processes. Edge computing resources can be dynamically integrated into slices and traffic steered to those resources to reduce latency. This paradigm shift in slicing will present new opportunities for improving communication services for public safety.

3.4.1 Network Slicing Architecture

The system architecture and functional aspects of network slicing are defined in the 3GPP Technical Specification 23.501[47] . A Network Slice Instance (NSI) is a set of NF instances and the required resources (e.g. compute, storage, and networking resources) which form a deployed network slice. A network slice instance is defined within a Public Land Mobile Network (PLMN) and includes the User Equipment (UE), 5G Access Network (AN), Transport Network, and the 5G CN[48].

The logical architecture for network slicing is depicted in Figure 22 showing the relationship between the shared NFs and NFs dedicated to specific network slices (Reference [31]). A UE can connect up to 8 slices. Each slice is identified by a Single Network Slice Selection Assistance Information (S-NSSAI) identifier. The Access and Mobility Management Function (AMF) is the control anchor and common to all slices used by the UE. The AMF queries the Network Slice Selection Function (NSSF). The NSSF selects the network slice instance to serve the UE based on permitted S-NSSAIs, UE's current tracking area, load level, and other

[47] Other standards organizations are involved in defining network slicing, including IEEE, IETF, MEF, and ONF
[48] The 5G AN may be the Next Generation Radio Access Network (NG-RAN) or the Non-3GPP Interworking Function (N3IWF) to a non-3GPP AN (e.g. Wi-Fi).

information. The Session Management Function (SMF) is specific to each slice and is selected via the Network Repository Function (NRF) that maintains the availability of NF instances specific to the slice. The NRFs and SMFs can be different administrative domains from the AMF. SMFs are responsible for selecting and controlling the User Plane Function (UPF). The Policy Control Function (PCF) retrieves the slice security control policy applicable to the UE and returns it to the SMF upon request.

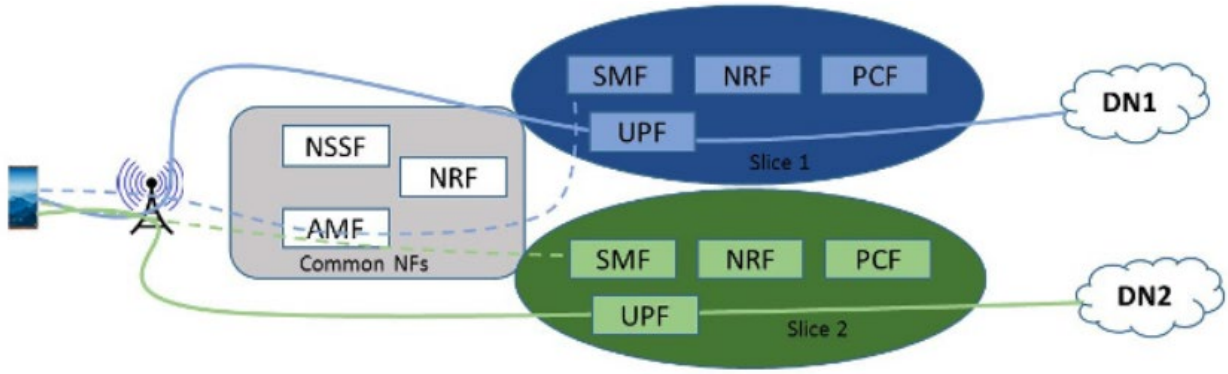


Figure 22 – Network Slicing Architecture (logical example)

3.4.1.1 SLICE IDENTITY

A slice is uniquely identified across the core, RAN, and UE by a Single Network Slice Selection Assistance Information (S-NSSAI) identifier. This identifier is used in network procedures to help select and activate/deactivate a slice for user applications. Once the slice is operational, the S-NSSAI is used to direct the user's data packets across the resources specific to its slice.

The value assigned to the S-NSSAI represents a set of communication service requirements which dictate what resources (i.e., NF instances, compute, storage, etc.) get provisioned to the slice. The S-NSSAI is a combination of the Slice/Service Type (SST) field and an optional Slice Differentiator (SD) field. The SST refers to the expected Network Slice behavior in terms of features and services, whereas the SD differentiates amongst multiple slices of the same SST. The SST is customizable, but TS 23.501 has defined a set of standardized SSTs as a way for establishing global interoperability for slice profiles that are expected to be common. Support for these SST values is not mandatory. However, the goal is to enable PLMNs to support roaming use cases more efficiently for the most commonly used SSTs. Table 5 shows the standardized SSTs. For more details on defining a customized slice see Section 3.4.2.

Table 5 – Standardized Slice Service Types

Slice/Service type	SST value	Characteristics
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband. (e.g. streaming high-quality video, fast large-file transfer, real-time gaming)
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications. (e.g. autonomous driving, UAS, augmented/virtual reality, public safety)
MIoT	3	Slice suitable for the handling of massive IoT. Slice Type has high density of heterogeneous devices with massive connectivity requirements. E.g. smart cities, smart grids, intelligent agriculture.
V2X	4	Slice suitable for the handling of V2X services.

3.4.1.2 SELECTING A NETWORK SLICE

The CN is responsible for selecting the network slice instance (NSI) to serve a UE, which will include the control plane and user plane NFs. Selection of a network slice for a UE is normally triggered as part of the UE registration procedure. The UE can request slices by optionally including the Requested NSSAI listing up to 8 network slices in its Registration Request message. Depending on slice availability and subscription parameters, the network may accept the registration for all, some, or none of the requested S-NSSAIs. If the UE's registration request does not include a Requested NSSAI, the network assigns the UE default slices based on subscription information. To select the appropriate NSI, the first contacted AMF instance serving the UE interacts with the NSSF to retrieve information for the Allowed NSSAI based on the UE's current tracking area and the Configured NSSAI of the serving PLMN. The AMF conveys the network decision back to the UE in a Registration Accept message including the Allowed NSSAI and/or Rejected NSSAI.

3.4.1.3 ESTABLISHING A PDU SESSION IN A NETWORK SLICE

A Protocol Data Unit (PDU) session connects a UE to a network. A PDU session is associated to one S-NSSAI and one Data Network Name (DNN) and allows data transmission in a NSI to a Data Network (DN). When an application needs communication services, the UE initiates the PDU Session Establishment Request message. According to the rules in the UE Route Selection Policy, the UE indicates the desired S-NSSAI (from the Allowed NSSAI list assigned during the registration procedure) in the request. The AMF queries the appropriate NRF to select the SMF instance for the specific NSI. The selected SMF selects the UPF and establishes a PDU session based on S-NSSAI and DNN. When the PDU session for a given S-NSSAI is established using a specific NSI, the CN provides the S-NSSAI corresponding to the NSI to enable the Radio Access Network (RAN) to perform access specific functions.

3.4.2 Defining a Network Slice

The Global Systems for Mobile Communications Association (GSMA) has defined a Generic network Slice Template (GST) to provide a standardized list of attributes that can characterize a type of network slice (Reference [32]). A GST is intended for operators, vendors, and slice customers to communicate the characteristics of a slice efficiently. The customer provides requirements for their use case and the slice provider would map those requirements into attributes of the GST filled with suitable values. In the context of network slice lifecycle management (see Section 3.4.3), the GST serves as input to the Preparation Phase and then further translated into 5G system configuration parameters for the RAN, CN, and transport subnets. An example process flow is shown in Figure 23 to illustrate the utility of the GST.

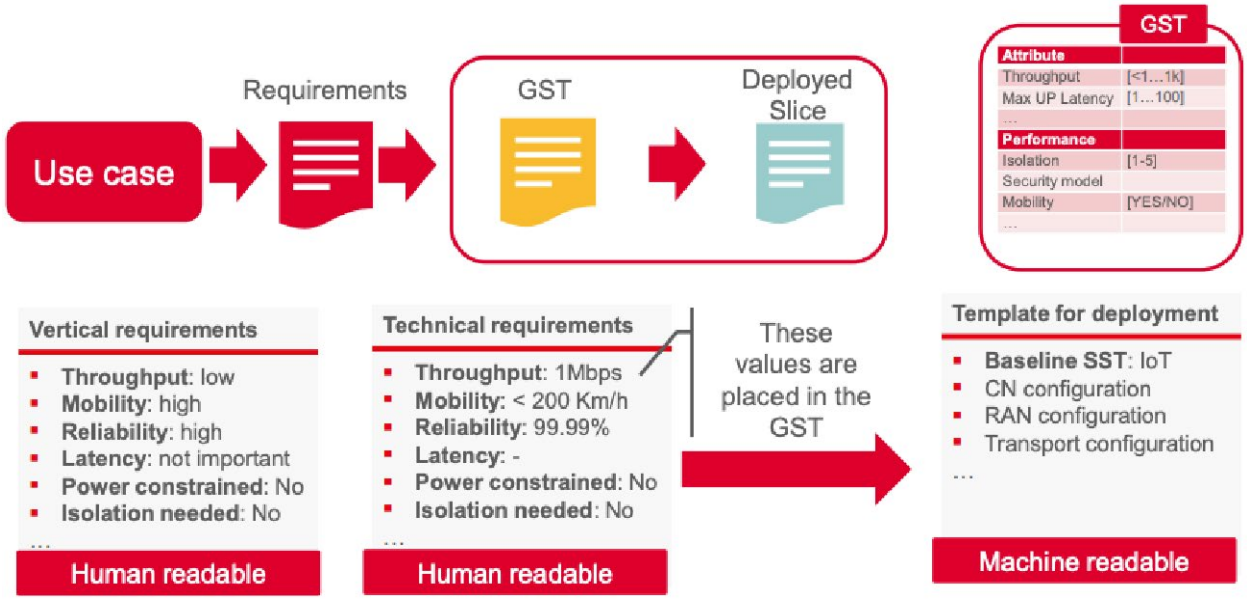


Figure 23 – Example configuration of a slice using GST (Reference [33])

The GSMA-defined attributes are based on open and published 3GPP specifications. In general the attributes are categorized into:

- Character attributes – characterize a slice based on performance, functionality, and operational methods for controlling and managing slice
- Scalability attributes – provide information about scalability of slice (e.g. number of UEs)
- Exposure Attributes – attributes that provide a way for the slice customer to access the slice capabilities (e.g. KPIs, API)

Figure 24 lists example attributes for each of the categories. Some attributes like Deterministic Communication Parameters have several sub-attributes. Additionally, many of the attributes can be listed across multiple categories. For a complete list of over 30 attributes defined for GST see Global System for Mobile Communications website (Reference [34]).

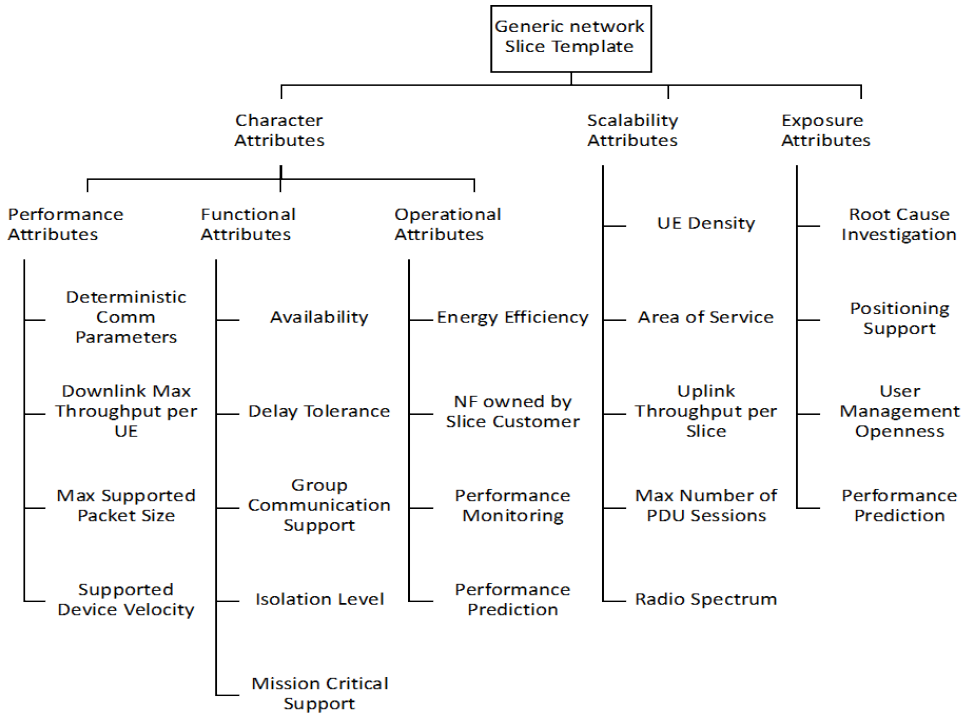


Figure 24 – Examples of attributes defined for the GSMA Generic network slice templates (GST)

Given the flexibility and granularity of customization, the public safety community will need an efficient method at the design phase to identify what network characteristics and service offerings are required and delivered by the Mobile Network Operators (MNOs). Requirements beyond the typical performance parameters like latency, throughput, and mobility will need to be considered. For instance, the level of physical or software isolation will also need to be considered for security and reliability. The public safety community may also want to exercise the option to manage its own slice, once Network Slice as a Service (NSaaS) is available. NSaaS will expose management capabilities to the slice customer for which it can offer their own services on top of the network slice instance. The flexibility in configuration will have to be weighed against the cost and the level of self-management the public safety community wants to own.

3.4.3 Network Slice Management and Orchestration

The 3GPP Technical Specification 28.530 defines management and orchestration concepts for network slicing and borrows heavily from concepts developed by ETSI for NFV MANO (Reference [23]). The lifecycle management of a network slice instance is depicted in Figure 25 and described by 4 phases (Reference [35]).

1. Preparation: In the preparation phase the network slice instance does not exist. The preparation phase includes network slice template design, network slice capacity planning, on-boarding and evaluation of the network slice requirements, preparing the network environment and other necessary preparations required to be done before the creation of a network slice instance.
2. Commissioning: Provisioning in the commissioning phase includes creation of the network slice instance. During network slice instance creation all needed resources are allocated and configured to satisfy the network slice requirements. The creation of a network slice instance can include creation and/or modification of the network slice instance constituents.

3. Operation: Includes the activation, supervision, performance reporting (e.g. for KPI monitoring), resource capacity planning, modification, and de-activation of a network slice instance. Provisioning in the operation phase involves activation, modification and de-activation of a network slice instance.
4. Decommissioning: Network slice instance provisioning in the decommissioning phase includes decommissioning of non-shared constituents if required and removing the network slice instance specific configuration from the shared constituents. After the decommissioning phase, the network slice instance is terminated and does not exist anymore.

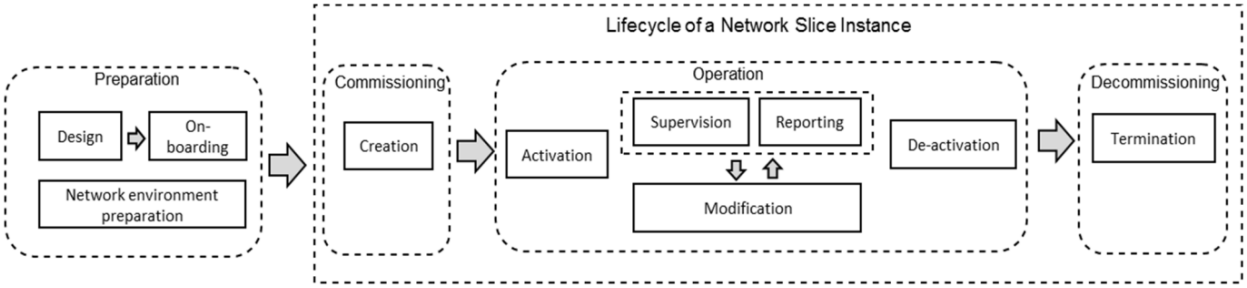


Figure 25 – Network Slice Lifecycle (Reference [23])

Additionally, it should be noted that end-to-end slicing will require management and orchestration of all technologies that comprise the 5G network, including the 5G New Radio (NR) RAN, edge cloud, transport xHaul, and the 5G CN, as well as the business enablement layer. This will require management functions, and likely different software solutions, for each component. The 3GPP has defined specific roles for each and include:

- Communications Service Management Function (CSMF): higher-layer OSS/BSS that performs customer order management and applies defined policies to meet end-user service level objectives
- Network Slice Management Function (NSMF): Cross-domain network slice orchestration using the domain-level slice management functions
- Network Slice Subnet Management Function (NSSMF): Application-level and domain [footnote: domains also referred to as subnets] specific management of NFs including instantiation, scaling, and termination

This is illustrated in Figure 26.

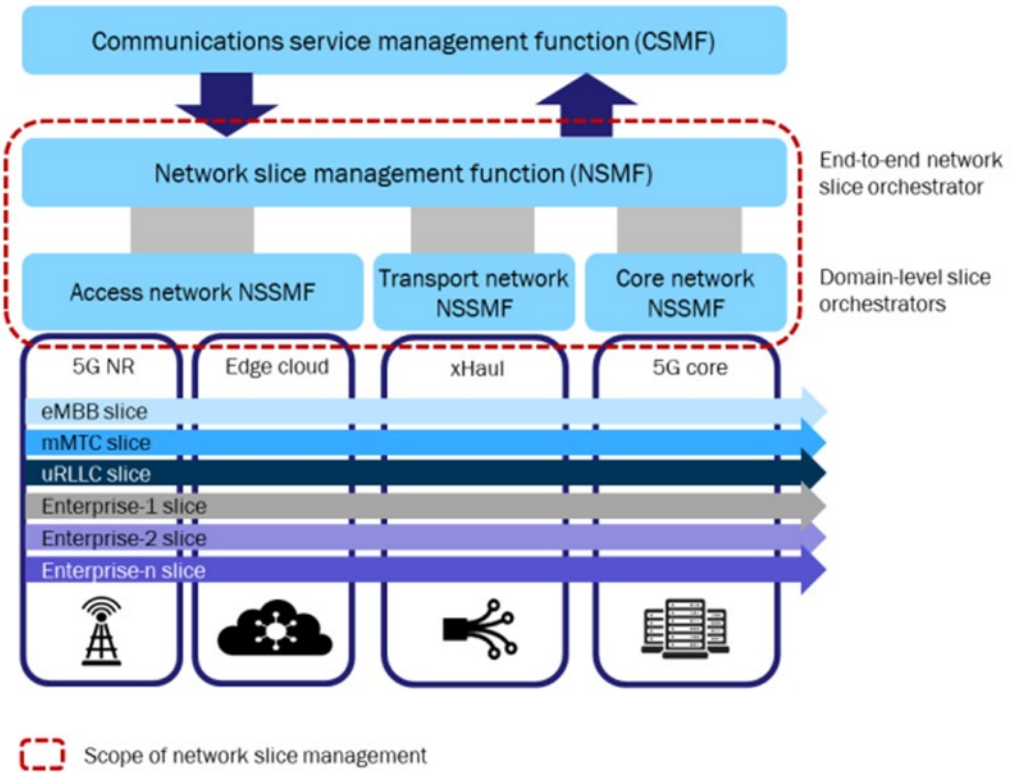


Figure 26 – Domain orchestration (Reference [36])

3.4.4 IMPACT TO PUBLIC SAFETY

The concept of having a customized mobile network for public safety is not new. FirstNet established a dedicated network for First Responders providing guaranteed priority and access to communicate during crisis on band 14. However, service offerings will need to evolve within and outside of FirstNet to allow the public safety community to act faster and more efficiently.

With network slicing, capabilities can be brought in for specific missions and then removed when finished. The network can be sliced and configured as required without needing to set up a new network. Slicing can leverage MEC resources bringing compute power closer to the first responders to improve situational awareness with analytics. Slicing can enable advanced routing, transmitting pertinent information to the right users. Network slicing presents an opportunity to realize a wide set of use cases for mission critical operations.

While the higher capacity and lower latency in 5G will provide advances to public safety applications, slicing will enable quick deployment of "Public Safety" slices that can be tailored – assigned more spectrum, positioning support, or group communication support – and adjusted to specific tasks. This is illustrated in Figure 27.

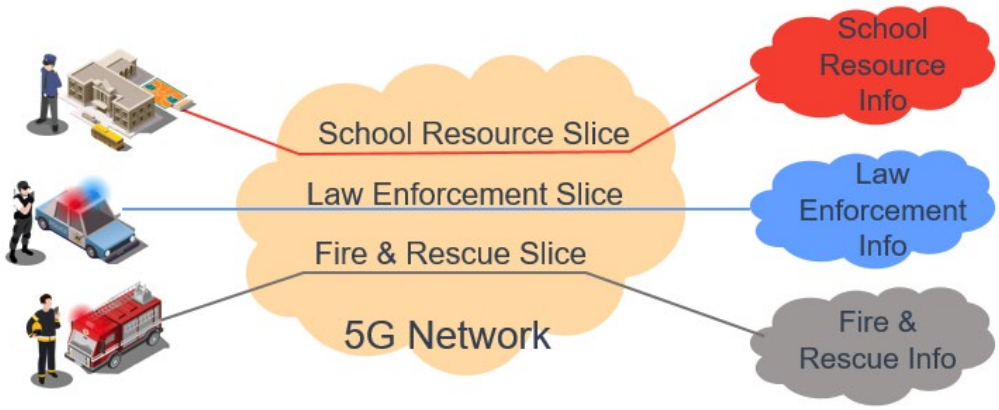


Figure 27 – Exemplary concept of "Public Safety Slices"

Take for example an emergency response to a school shooting requiring intensive voice and video communication to coordinate between teams. Slicing allows communication resources to be instantiated on demand in the precise area of the school during this operation. Additionally, slicing can help ensure the right information is sent, to the right person, at the right time. For instance, the position and vital sign information from first responders requiring low bandwidth, low loss, and the highest level of data privacy can operate under one slice. Simultaneously, surveillance information from UAS and Body Worn Camera (BWC) requiring high bandwidth can run on another slice to share across agencies and jurisdictions and to route data to a regional data center for facial recognition analysis.

3.5 NON-PUBLIC NETWORKS

Starting with 3GPP Release 16 specifications TS 22.261 (Reference [37]), the concept "private networks" was extended to *Non-Public Networks* (NPNs) to enable more deployment models. While NPN is not specifically an enabler of 5G technologies, it is considered an enabler of new envisioned vertical use cases. NPNs are intended for the sole use of a private organization, typically an industry vertical (e.g. automotive, manufacturing, and government) and help ensure data privacy and security, continuity of service when public networks fail, and reliable access to local resources with improved quality of service. The NPN provides coverage and private network services that are within the organization's premises. 5G NPNs are divided into two categories:

- Standalone NPN (S-NPN) – physically isolated from and do not rely on NFs provided by the Public Land Mobile Network (PLMN). An S-NPN operator could be the organization itself or a 3rd party. An S-NPN operator has full control and management capability.
- Public network integrated NPN (PNI-NPN) – hosted completely or in part on PLMN infrastructure, relying on NFs controlled and managed by the MNO.

Table 6 (Reference [38]) provides a comparison between SNPN and PNI-NPN. Each category is discussed in more detail below.

Table 6 – Comparison between Standalone NPN and Public Network Integrated NPN

	Standalone NPN	Public Network Integrated NPN
Isolation from Public Network	Complete physical isolation	Hosted completely or in part on public network
RAN Cell Selection	Broadcast PLMN ID and Network ID (self-assigned or coordinated)	Broadcast PLMN ID specific to PNI-NPN and Closed Access Group (CAG) ID
Spectrum	Private, unlicensed, licensed	Unlicensed, Licensed, shared
Roaming	No	Yes
Network Maintenance	Private organization, 3rd party integrator, or MNO	MNO
Investment	High Capex (upfront equipment cost) Low Opex (no subscription & license fee)	Low Capex (no upfront cost, MNO deploys equipment) High Opex (MNO charges subscription & maintenance fees)

3.5.1 STANDALONE NPN

SNPNs deploy the full 5G system on-premise not relying on any network functionality from a mobile network operator (MNO). Plus it is isolated from any interaction with the public network. Figure 28 illustrates an SNPN (Reference [39]). This setup provides complete data security and privacy, because all subscription information, data, and network services are stored and managed on-premise. Additionally, if the MNO's network fails, the SNPN will continue to work. A SNPN can be built by the private organization or 3rd party using unlicensed spectrum (e.g., NR-U, CBRS bands) or licensed spectrum sub-leased from a MNO. One trade-off for SNPNS is high capital expenses for hardware, software, and licensing fees.

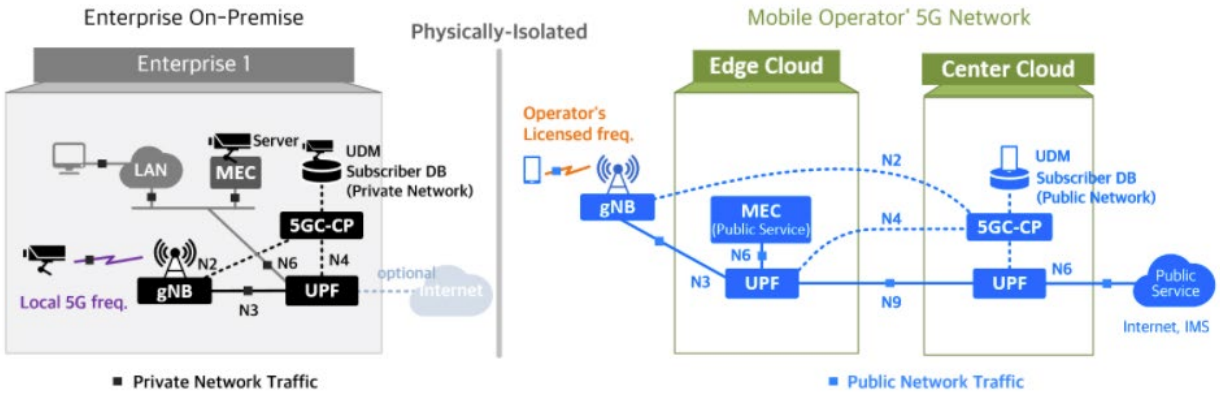


Figure 28 – Standalone NPN (Reference [39])

3.5.2 PUBLIC NETWORK INTEGRATED NPN

PNI-NPN deployments function as private networks, but can vary in terms of the degree of interaction and sharing of infrastructure with a public network. Here we present 3 scenarios for deploying PNI-NPNs: 1) shared RAN, 2) shared RAN and control plane, and 3) shared RAN and CN. When the full 5G system (RAN and CN) in the public network is shared and logically segregated to host a private network this is often referred to as an end-to-end 5G network slice.

3.5.2.1 RAN SHARING

RAN sharing between a private and public network is depicted in Figure 29. In this configuration, the full 5G system is deployed on-premise. However, the 5G base stations are shared between the public and private network. Traffic from devices belonging to the private enterprise is routed to the on-premise private network. Whereas traffic from devices belonging to the public network are routed to the mobile operator's CN. Network slicing can be implemented to provide segregation of traffic at the RAN. Although not completely isolated from public network and subscribers, subscription information and enterprise data are stored and managed on-premise providing data security and privacy. Additionally, quality of service of the private network is still fairly independent of the public network if it were to fail.

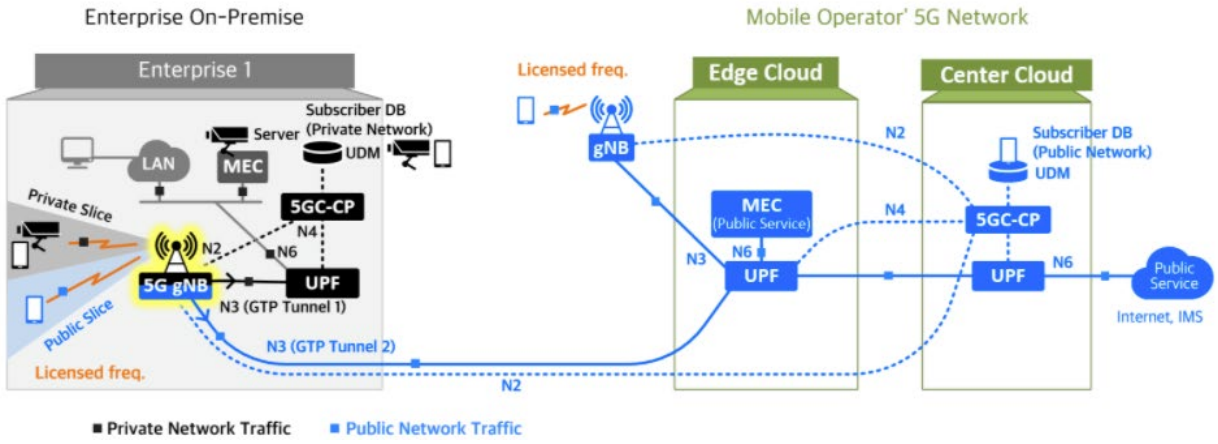


Figure 29 – PNI-NPN: RAN sharing between private network and public network (Reference [39])

3.5.2.2 RAN AND CONTROL PLANE SHARING

When sharing the RAN and control plane, the private network relies on the mobile operator's public network to handle control plane procedures (e.g. authentication, mobility management, etc.). This means subscription information is stored in the operator's domain, rather than the enterprise. The user plane functions and private services (e.g. UPF and MEC) are physically isolated and deployed on premise. Network slicing can be implemented to provide segregation of traffic at the RAN and control plane. Figure 30 shows a shared RAN and control plane configuration for a private network.

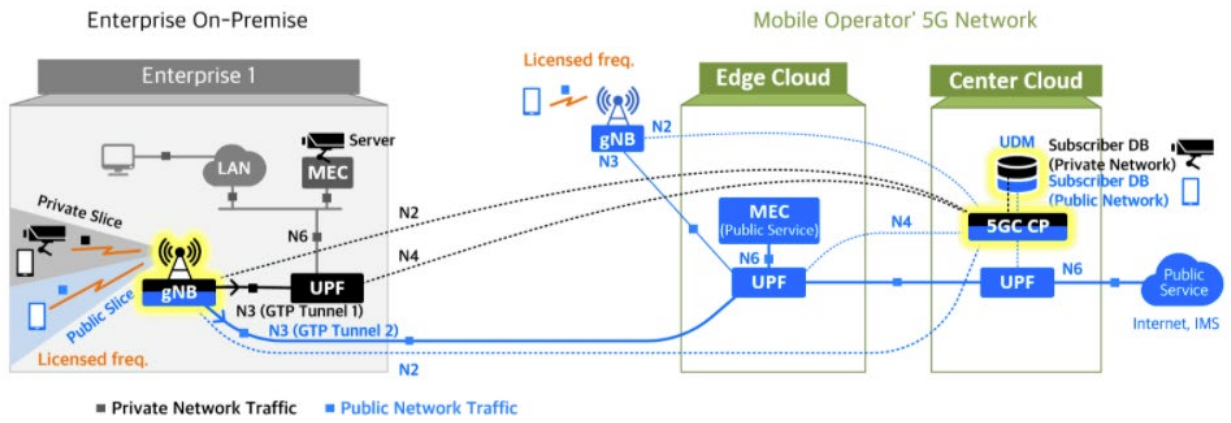


Figure 30 – PNI-NPN: RAN and control plane sharing between private network and public network (Reference [39])

3.5.2.3 RAN AND CORE SHARING

When sharing the RAN and core, there is no physical separation from the public network. The separation is only logical and the RAN is the only component on-premise. User's operational data and subscriber information are stored in the operator's network. The private network is dependent on the mobile operator for control signaling and providing application services. Since traffic of the private network is transferred over the mobile operator's network, there is concern for security and quality of service. End-to-end network slicing can be used to implement this deployment strategy. Figure 31 shows a shared RAN and core deployed for a private network.

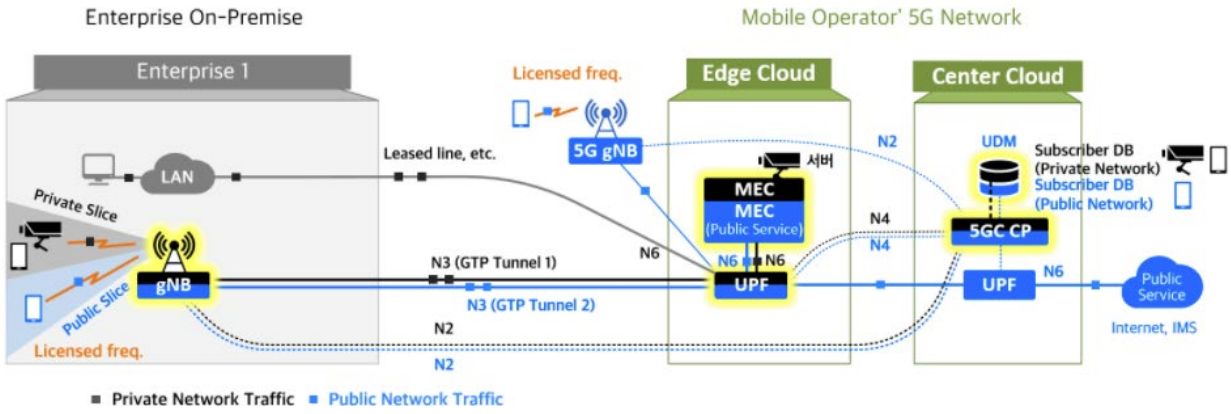


Figure 31 – PNI-NPN: RAN and core sharing between private network and public network (Reference [39])

3.5.3 IMPACT TO PUBLIC SAFETY

5G non-public networks offer different deployment models to provide 5G wireless access and private network services that are within an organization's premises. When first responders arrive on scene where a private 5G network has been deployed, configurations (e.g. UE Route Selection Policy, PLMN ID, CAG ID, etc.) can be pushed to their 5G devices to allow them access to local networks, applications, and services via 5G access. The private indoor 5G base stations will extend RF coverage for first responders and provide local access to data-heavy applications, like surveillance video.

Though it is highly unlikely due to the cost, the public safety community could also have their own private 5G networks. This could range from a standalone NPN, for example, on a first responder vehicle (e.g. fire truck) to a private network completely hosted on the public infrastructure using network slicing (Section 3.4). With the proper configurations, a first responder can access multiple private 5G networks from a single device. When deploying their own private 5G network, the public safety community should consider the level of responsibility for the different deployment models. Table 7 describes each approach discussed above showing the customer or mobile operator role for non-public networks.

Table 7 – Customer versus Mobile Network Operator Role for Different Types of Non-Private Networks

	Standalone NPN	**Public Network Integrated NPN**		
		RAN Sharing	RAN + Control Plane Sharing	RAN + Core Sharing (E2E slicing)
Applications	Customer	Customer	Customer	Customer
Data Security	Customer	Customer	Customer	MNO
Spectrum	Customer or MNO	MNO (Customer optional)	MNO (Customer optional)	MNO
Infrastructure	Customer	Customer & MNO	Customer & MNO	MNO
Management	Customer	Customer & MNO	MNO	MNO
Devices	Customer	Customer	Customer	Customer
Subscriptions, SIMs	Customer	Customer	MNO	MNO

4 ACTIVE SHOOTER SYSTEMS VIEW

An active shooter event ranks high on the NPSTC incident scale. As a result, the incident will involve multi-service, multi-jurisdictional responders among local and state public safety entities. Federal agencies may also work with the lead agency to support post event investigations and provide other on scene support functions.

While active shooter events are very dynamic and situations can quickly change, certain key actions are required for the response. Among these are to neutralize the threat and to treat and evacuate the injured. To this end, the International Association of Chiefs of Police (IACP)'s active shooter model policy guideline (Reference [40]) has been developed to assist law enforcement agencies to develop an active shooter incident response plan. According to the policy guideline, there are seven (7) specific roles and responsibilities that need to be considered for an active shooter. The following is a summary of those roles and responsibilities.

1. Situational Assessment whether from 911 call through the Public Safety Answering Power (PSAP) or dispatch, witnesses or by other means
2. Intervention by law enforcement (e.g., school resource officer), whether on duty/off duty in uniform or civilian clothes, taking immediate action necessary and reasonable to stop the threat
3. Law enforcement officer or team response (first Officer(s) at the scene) tasked with the locating the suspect(s) and stopping the threat. Contact Officer or team should not render aid to victims, unless the location of the suspect is known and any immediate threat is eliminated and the area is cleared.
4. Rescue Task Force (RTF): After the initial response is deployed and additional resources arrive at the incident scene, the Incident Commander may request support from the RTF team, which is organized under a team leader consisting of fire/EMS personnel paired with law enforcement officers. The RTF team is tasked with locating wounded and injured persons based on initial location notification. This rescue and recovery operations shall continue until the Incident Commander has declared the scene clear and safe.
5. Unified Command: Incident command system where more than one agency with jurisdiction work together. Incident commander ensures unified interagency communication(s). The Incident Commander is also the individual responsible for all incident activities and resources, establish inner and outer perimeters, establish staging areas for; responding officers and other emergency personnel, treatment of the injured and evacuation by EMS or medevac, evacuation area for individuals without injuries for identification and debriefing, notification center for arriving family members, and an area for the media. The IC will also request mutual aid if needed, establish traffic control and management, among other tasks.
6. Community notifications are handled by the Public Information Officer (PIO) or other designated individual(s) who ensures that appropriate information is distributed in a timely manner to the community
7. Debriefing by all essential personnel involved in the incident by the lead agency.

Law enforcement typically has jurisdiction over an active shooter incident but a significant number of fire and rescue, and emergency medical services resources will also be involved in the response. Law enforcement from other jurisdictions may also be dispatched or self-dispatched. The need for interoperable communications and data sharing is thus critical from start to finish in a complex response

such as an active shooter incident. Each individual involved in the incident will have access to a set of voice and data communication capabilities. These capabilities can be linked to a person with a set of communication resources immediately available to them and to a vehicle or facility that may take time to access. These on-body/off-body capabilities are referred to as the "capability stack" in this document.

As an example, Figure 32 represents the capability stack for a LEO. Figure 33 provides a legend for the systems view including app capability stacks. The LEO will typically have immediate access to their portable LMR, cellular phone, and BWC. Figure 32 illustrates location and physio sensors, however this technology has not matured enough to be considered standard equipment among the law enforcement community. In the future, these sensors may be linked to a communication hub that is connected to a mobility network, or directly to a mobility network themselves to share data such as heart rate, temperature, or interior location and elevation. The LEO will also have access to a vehicle-based set of communication capabilities. This could include the LMR, camera system, mobile data computer and a modem that connects these technologies to a mobile broadband data network.

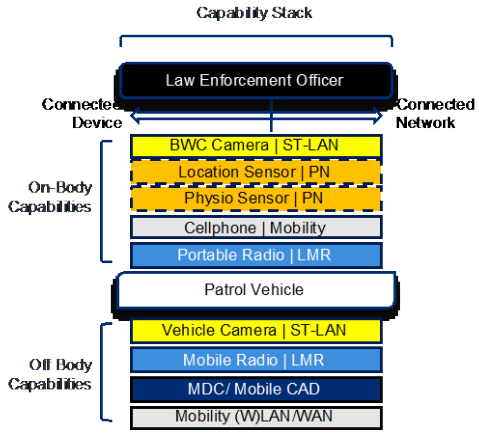


Figure 32 – Law Enforcement Officer Capability Stack

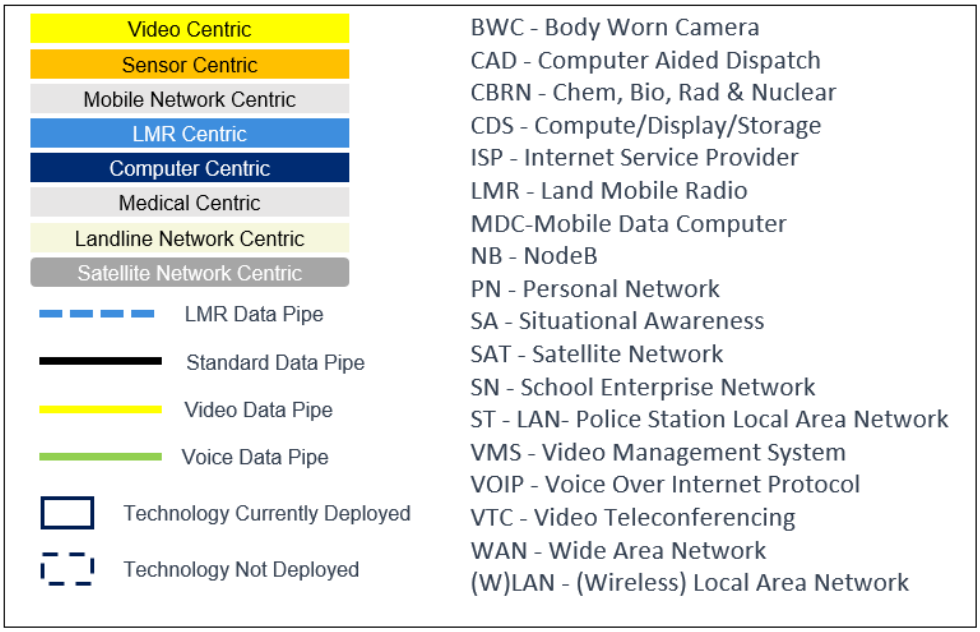


Figure 33 – Legend for systems view diagrams

These communication capabilities are then connected to different networks. As shown in Figure 34, the devices providing voice and data communication are connected to the mobility network. The device that provides LMR voice communication is connected to the LMR network. Within the vehicle, the cellular gateway/router device that connects to the mobile broadband Wide Area Network (WAN) may also provide Wireless Local Area Network (WLAN) or Local Area Network (LAN) connectivity for other devices, such as the Mobile Data Computer, allowing access to the internet.

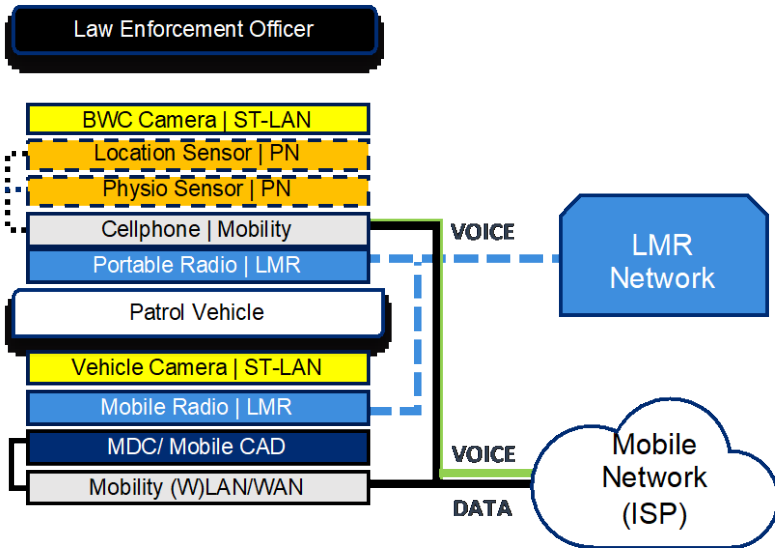


Figure 34 – Law Enforcement Officer Capability Stack Connections

These capability stacks are then inter-linked to various networks that may include:

- Mobile network ISP
- Fixed network ISP
- Satellite ISP
- LMR network

Figure 35 below provides an overview of the current system view for an active shooter incident[49]. It places individual(s), first responders and their systems, and supporting facilities within the incident area that includes the Operational Area, Incident Command/Unified Command Area, and remote stakeholders outside of the response area.

It is intended to represent the typical systems and networks that an individual(s) or groups may use to communicate during the response. The actual systems and networks that are utilized for a real-life active shooter incident may be different. The network connection view illustrates the capability stacks for individuals, first responders, and other stakeholders connected by separate networks through which voice and data communication is enabled. It also identifies the responders having roles and responsibilities as described in the IACP policy guideline combined with other stakeholders. This includes the following entities and their respective capability stack:

- Civilians/School Personnel
- On-scene first responders including the SRO, LEO, EMS, Fire & Rescue as well as Incident Command/Unified Command
- Remote stakeholders including the PSAP, emergency management agencies, and local hospitals

Additionally, the sources of information to be shared at the scene include:

- School Cameras
- Body Worn Cameras
- UAS Cameras

[49] Note that this systems view is notional and does not describe the systems and first responders that would be present at all active shooter incidents, nor all networks and configurations that may exist. These systems and first responders were selected to illustrate the interoperability required at the scene including both operational and incident command area, as well as any remote supporting entities. The networks illustrated are designed to demonstrate the complexity in communications options.

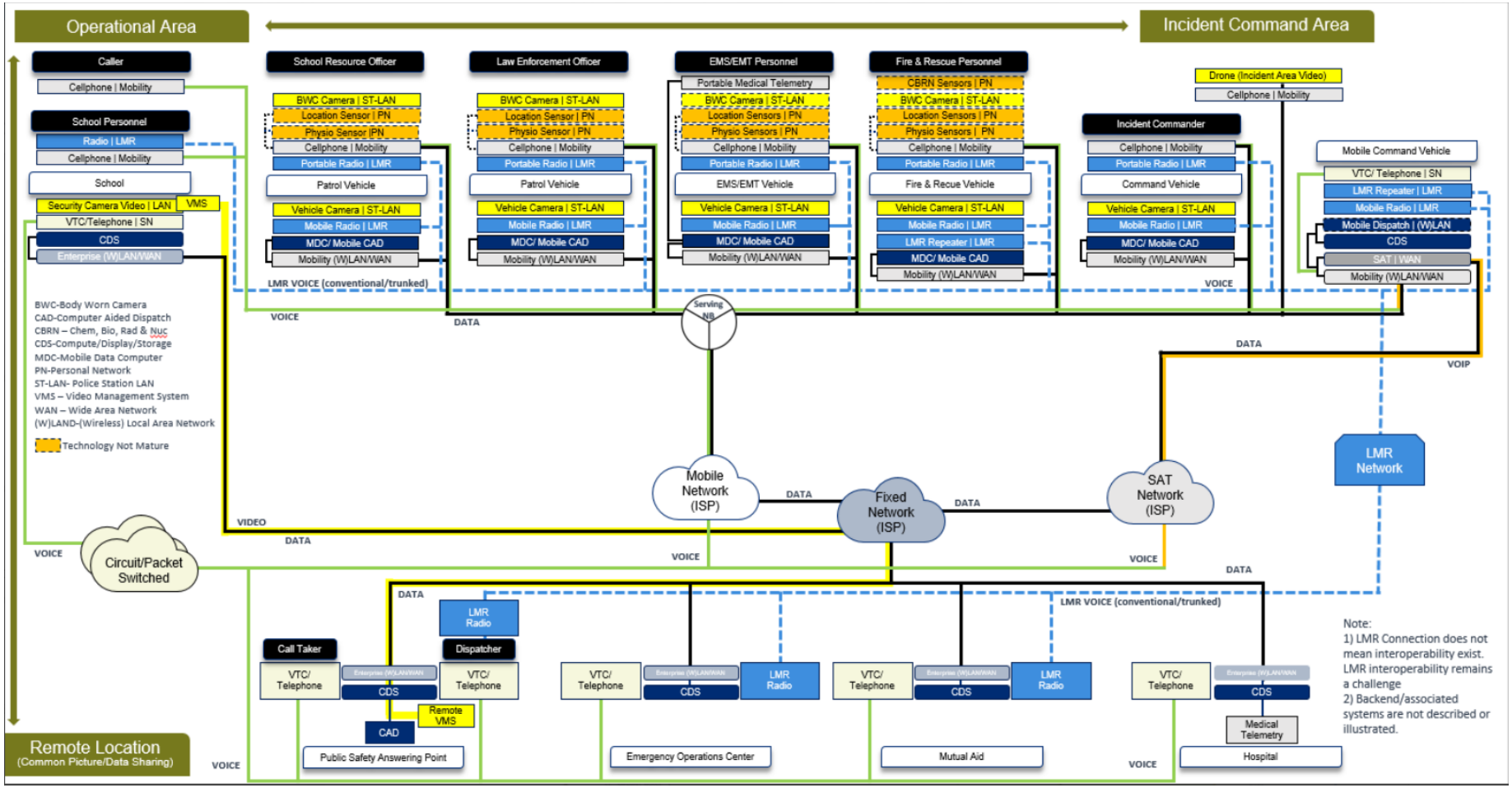


Figure 35 – Incident area network Emergency Response operational systems view

As described in the IACP policy guide, the Incident Commander is responsible for all activities and resources during the incident. Therefore, a key objective of information sharing activities should be to ensure the incident commander has real-time critical information for decision support needs. Figure 36, illustrates the sharing of video information to the Incident Commander obtained from the school cameras, BWCs, and UAS.

Figure 36 – Video dissemination at the incident area network

4.1 Lessons Learned from Real World Events and Exercises

In order to better understand the challenges imposed by information sharing of video at the incident area network, two exemplar events were reviewed for the purposes of this study. These include the after action report generated for the active shooter response at the Marjory Stoneman Douglas (MSD) High School, and an DHS S&T active shooter operational exercise at an area school in Adams County, Indiana. The lessons learned can be summarized as follows:

- Limited capacity
- Limited coverage
- Unacceptable latency
- Lack of interoperability
- Lack of automated access to information
- Limited situational awareness

4.1.1 Marjory Stoneman Douglas High School

The MSD school shooter provides a representative real-world use-case that demonstrates the critical need to get the right information to the right people at the right time. On February 14, 2018 an active shooter entered the High School, leading to the death of 17 individuals and causing injuries to 17 other people. An

initial report by the High School's Public Safety Commission (Reference [41]) detailed the events leading up to the event and subsequent arrest. The report provides detailed timelines, relevant contextual interviews, and collaborated accounts by BWCs and surveillance cameras mapping a comprehensive picture of the operational response. The commission found multiple factors which contributed to the breakdown of the response. For the purposes of this report, focus is placed on key elements of video information sharing and communication which hindered decisions.

In its report, the Commission concluded that had the Broward County Public School system given authorization to law enforcement for direct access to the camera system, locating the perpetrator and victim rescue efforts would not have been hampered. They stated, "The Broward County Public School's decision not to allow law enforcement live and real time direct access to the school camera systems in Broward County, including the system at MSDHS, adversely affected law enforcement efforts to locate Cruz and it hampered victim rescue efforts."

It was also later discovered that once the video from the school camera was finally accessed, it was severely delayed, giving first responders a false impression that the perpetrator was still in the building. This video feed was monitored for over nine (9) minutes until the delay was realized. As a result, rescue and recovery efforts for the injured was delayed.

This report stresses the need to access real time video at the incident edge and ensure interoperability among responding emergency responder components. For more details on the decomposed video centric timelines of the MSD-PSC report, refer to Appendix A.

4.1.2 DHS S&T Activate Shooter Operational Exercise

Mitigating communication challenges and the importance of video data sharing was further validated through an operational exercise conducted in Indiana on October 24, 2018 by APL on behalf of DHS S&T. The exercise simulated an active shooter event at an area school in Adams County Indiana with a primary goal of assessing the value of video data in supporting critical decision-making needs. This event included the participation from 15 agencies and multiple public safety disciplines including law enforcement, fire rescue, emergency medical services, public safety answering points, local and state emergency management agencies, school personnel and resource officer.

The exercise integrated live streaming video data that allowed decision makers to access and view video from the school's fixed camera system, live stream from the SRO's BWC, and live stream video from a UAS. Results demonstrated that if the appropriate video data can be provided to the decision-making personnel in a timely manner, response operations and responder safety could be improved. For example, remotely located personnel, such as the bomb squad, can have their "eyes on" a suspicious device and plan for specific mitigation action in advance of their arrival on scene as well as advise on-scene personnel accordingly. Outcomes also revealed that efforts are needed to bring the use of video data to the level of integration and dependability that LMR currently provides for voice. Exercise participants acknowledged that video data enhanced overall response by providing improved situational awareness, especially for areas where video can supplement voice communications and where LMR communications may be limited.

Public safety personnel's need for access to real-time video and reliable communications cannot be understated, but the lessons learned from the MSD incident and Adams County active shooter exercise

demonstrate gaps still exist for these communities. While the added capability of video data has been determined to be beneficial, there are also common concerns primarily in the areas of planning/procedures, as well as the technical and human resources required to manage video data. Public safety personnel have provided feedback in recent video integration testing, conducted by APL on behalf of DHS S&T and included:

- Video data could help to align initial tactical decision making
- Video data could enhance the recovery of injured persons in a timely manner when incident command can see victim locations in relationship to cleared or controlled threat areas. (It) Would help in selection of entry points to achieve the maximum benefit (e.g., safety and timeliness of response) for emergency responders such as a RTF's (Rescue Task Force).
- Information was shared between response partners almost as soon as the video was connected. It was a great asset for unified command.
- To add video data for the purposes of enhanced decision-making, the mission needs and readiness levels of the public safety agency must first be well understood.
- Any time additional information is added for situational awareness needs, extensive consideration must be given to ensuring the right information is available at the right time for the right mission.
- First responder operations and communication related needs will continue to be a challenge when it involves processing large amounts of data.

4.2 THREE VIEWS – A 5G PROGRESSION IN TIME

Mobility networks continue to evolve from earlier generation mobility standards to the next generation of mobility standards supporting more capacity, lower latencies, and other attributes progressively improving the Quality of Experience for the end user. Whether on commercial mobile broadband networks or FirstNet, the underlying mobility technologies that support the data communication needs of the public safety community will continue to improve.

The following section describes the capability stack and underlying systems and networks facilitating information sharing from current state (non 5G), to the mid-term state and to a future state integrating many of the 5G enablers. It describes the gaps and areas of opportunities as the underlying networks transition from earlier mobility standards to 5G. The goal is to provide knowledge of how the current state of systems and networks could evolve to potentially improve interoperability, improve access to information through automation, provide instant access to real-time video, and improve overall communication through the 5G enablers and systems.

4.2.1 CURRENT OPERATIONAL VIEW

As the MSD incident demonstrates, first responders often rely on a variety of information sources, to include video data when it's available, during their response to locate the suspect, the victims and any potential secondary devices. Having access to multiple video sources could improve their ability to locate the perpetrator(s) more quickly. For example, real-time footage from the school cameras can be used to scan the hallways or rooms, live video from the BWC can provide supplemental information for decision

makers to help mitigate the threat, and UAS video could be used to monitor the perimeter for threats. However, it is also important to note that while technology advancements such as integration live video streams can enhance response capabilities, these same advancements also provide for a more complex information sharing environment that can be overwhelming.

There may be policy reasons constraining access to the necessary data, but technology also plays a central role. Today, different systems from disparate networks remain disconnected from one another, inhibiting the ability to support instant access to critical interoperable data and to improve overall communication for enhanced situational awareness. Figure 37, illustrates this by aligning the capability stack to its network connections in order to examine the flow of data, in this case video, to gain insight on the limitations and challenges that public safety encounters from a data sharing perspective.

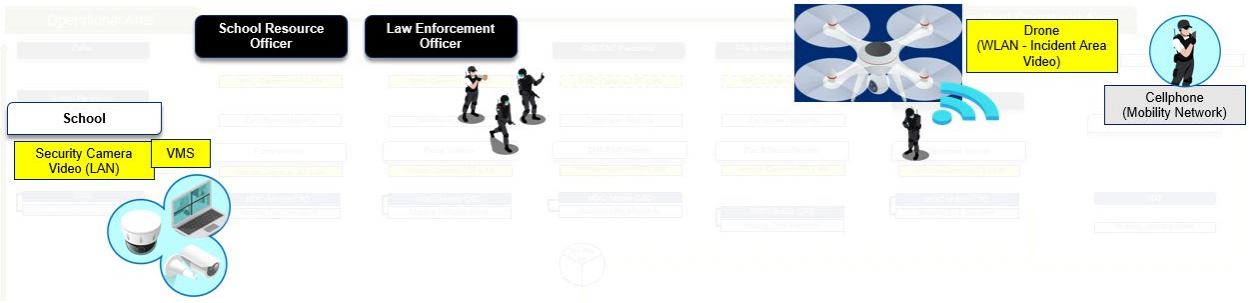


Figure 37 – Active Shooter Scenario - Current Operational View

As shown in Figure 37, there are three (3) video data sources identified; the school video camera, BWC, and UAS-based camera. Gaining access to these video sources will be instrumental to responders, however, these sources are disconnected and getting access requires manual requests.

The school camera system operates on its own, closed loop enterprise network that may not be immediately accessible to responders. The typical BWC on the SRO and LEO is not equipped to stream live video to key decision makers. The video footage from the UAS is typically only seen by the pilot unless the video is distributed locally or uploaded to a website using 4G LTE. If response personnel needs to view the video, they must go to the specific location where the video is being collected. For the school camera, that might be in the security office with the video management system. For the UAS footage, that might be where the UAS pilot operator is flying the drone. For the on-scene incident command team, quickly getting access to real-time high-quality video is not generally possible today.

Additionally, the on-scene responders are in the field, so having access to wireless networks/services for data sharing is paramount. The current mobility standard first responders are using for data sharing and voice conversation is predominately based on 4G/LTE. First responder's also rely on LMR for mission critical voice communication. Since the communication channels are wireless, it is subject to coverage and performance problems that is impaired by terrain, environment and many other factors. This could result in poor results when attempting to use an LTE device or LMR radio.

In summary, some of the areas that limit first responders' situational awareness for an active shooter type of event include the following:

1. No sharing of school camera data directly with key decision makers
2. No real-time sharing of UAS data to key decision makers

3. BWC are self-contained standalone devices preventing sharing of video data
4. Various transport networks must be used to share data, potentially causing unwanted latency
5. Existing mobility networks are congested at the RF air interface under extreme loading conditions, as more users start to connect, the quality of experience for all will decrease
6. Secure access to information and sharing the data is not instant and mostly a manual process

4.2.2 Mid-term Operational View

The mid-term operational view describes a scenario in the near future[50] where 5G networks are becoming the predominant mobile broadband solution, the 5G Core SBA and disaggregated RAN are fully deployed, and additional use cases such as mMTC and URLLC are operational.

The mid-term 5G evolution incorporates the potential to improve coverage inside the building using small cells connected to the carrier's core. The incident commander launched UAS connects directly to the outdoor 5G network, allowing all command, control, and video feeds to be accessed via the mobility networks. This stage also integrates the MEC at the edge of the network and closer to the end users allowing applications-based solutions that enhance the data sharing capabilities at the scene of the incident. The school camera systems still operate on its own, closed loop enterprise network at this stage, thus direct access to the school camera system will still be limited. Similarly, the BWC is still a standalone device, so data sharing from this video source is not possible. This is represented in Figure 38.

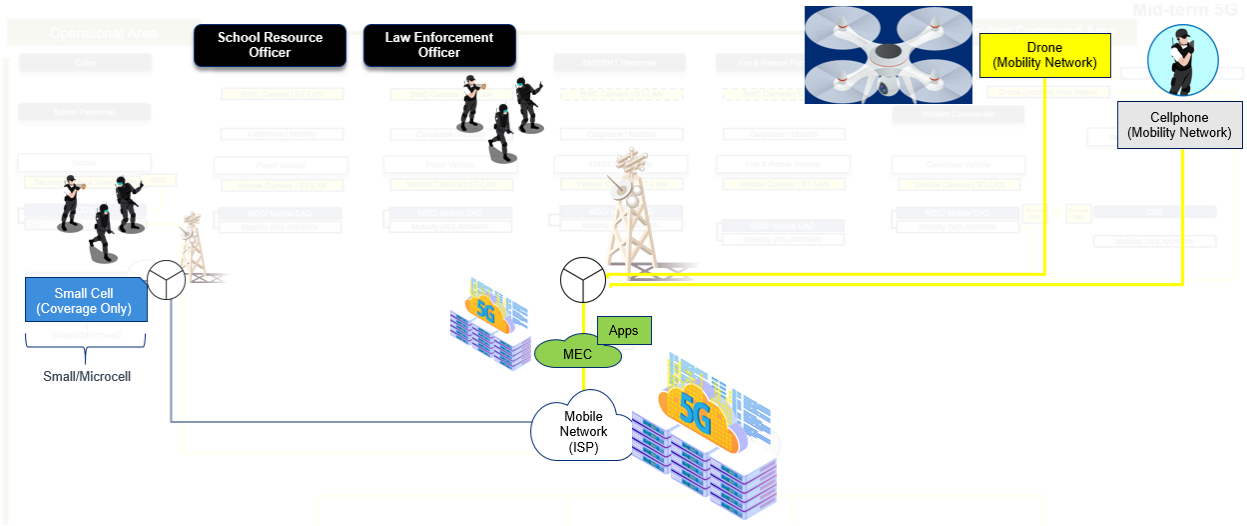


Figure 38 – Active Shooter Scenario - 5G Mid-Term Operational View

The 5G technology in this mid-term scenario will provide improved coverage, lower-latency, and automated application deployment for information sharing at the scene. It applies a flexible, dynamic, cloud-native, micro-service based architecture to the telecommunication network which differs from the static, bare-metal implementations found in 4G/LTE and previous generations of mobile networks. The 5G technologies highlighted in this scenario are the 5G Core SBA and disaggregated RAN, MEC application functions, virtualization, MANO, and small cells.

[50] Note: It is hard to predict a specific date for this scenario as 5G networks are being deployed today, however in many cases, they are yet to fully integrate the SBA and disaggregated RAN. One however may expect to see this view within the next 5 years in various markets as these are solutions currently being advertised by different vendors.

Small cells have been deployed by carriers for indoor and outdoor settings such as buildings, venues and campuses using minicells, microcells, picocells and femtocells to supplement macrocell coverage and/or capacity. These small cells are connected to various antenna configurations such as a distribution antenna system, leaky RF cables or a set of antennas that is determined by the deployment coverage and capacity objectives. They are also backhauled to the carrier's network using various transports methods that could include dedicated connections or internet grade connections. In 5G, small cells will fill the same role as in earlier generation with several added advantages including flexible radio and network topologies as well as supporting additional spectrum designed for coverage and/or capacity. This includes Low-band for expanded coverage, Mid-band for capacity and High-band (mmWave) supporting significant capacity and bandwidth in various sizes.

The indoor small cell in the mid-term view is installed and managed by the carrier to provide 5G service in degraded indoor coverage areas to its customers (e.g., staff, faculty, students, guests and first responders). First responders can access the microcell to use voice and data services as if they are on an out-door 5G public site.

For shared situational awareness and improved video dissemination at the scene, an incident commander UAS is launched that connects directly to the 5G network. The UAS in this case has been developed to operate using tight integration with both the carrier network and the MEC, where the deployment of the UAS will trigger a series of events that dynamically loads an application at the edge for video dissemination. The end result is to enable the key decision makers with direct access to the information with minimal delay. This process is further described below.

To achieve lower latency and observe a real-time video experience, it requires the video to be processed and re-distributed closer to the video source. This minimizes the transmission, propagation, queuing or processing delays that occur when data traverses back to the central cloud. MEC as a 5G enabler provides the standardized architecture that enables access to virtualized software solutions at the network edge[51]. The 5G virtualized and disaggregated SBA allows dynamic traffic steering and user plane functions to be pushed close to the active shooter scene. The virtualized architecture further provides the flexibility to scale network resources up or down to meet the real-time demand.

Once the UAS is powered on, it connects to the network and makes a query to a central cloud to establish an application to receive, process, and disseminate video, as well as provide all command and control. This query will trigger a previously established service within the 5G BSS architecture to identify the best location and deploy the application close to the edge. Following the service based rules and policies defined, the commissioning and run-time operation phases of the lifecycle orchestration of an MEC application is thus executed by a MANO. This involves deploying an application image from a central repository to edge NFVI, configuring for run-time access and control, and consistently monitoring to ensure all SLOs are met. If any SLOs fail to meet the expected behavior, the services can be autonomously scaled to meet demand.

Once the MEC application has been deployed near the incident, it will coordinate as an AF to dynamically steer both the uplink of UAS video to the virtual instance, as well as all downlink access for the end users

[51] This could be either a metropolitan or regional datacenter such as those hosted by Amazon Web Services or Microsoft Azure

similarly connected at the edge. A more detailed architectural diagram of how traffic steering to the MEC would operate can be seen in Figure 39.

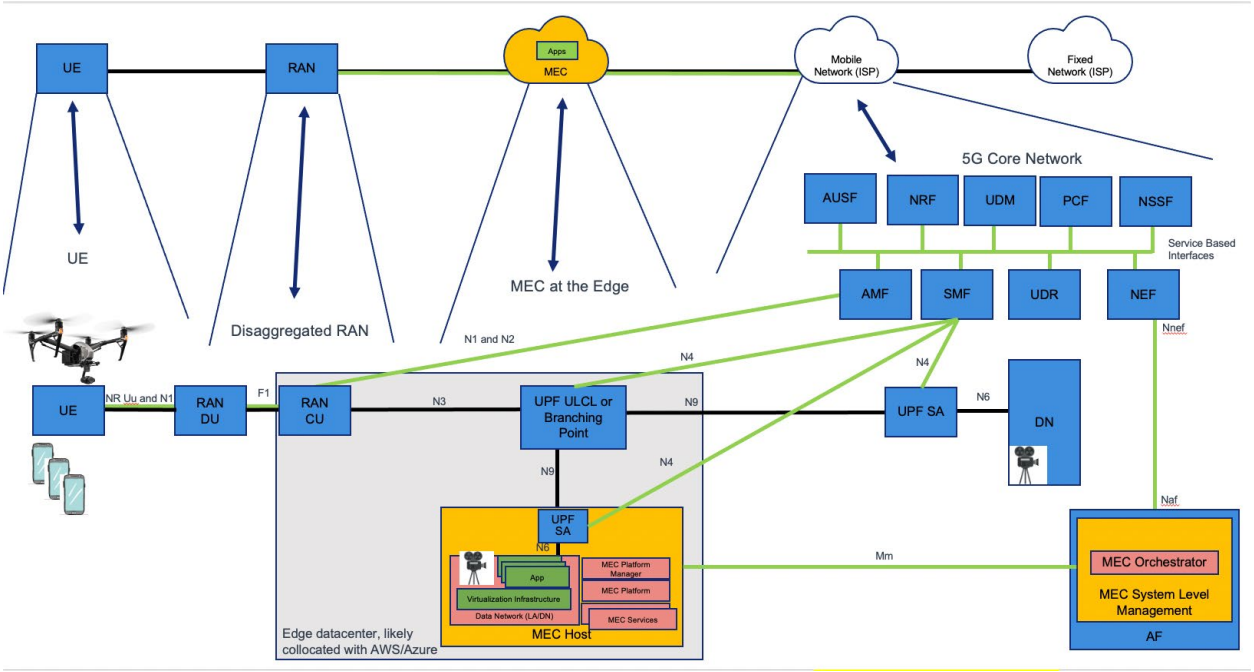


Figure 39 – Active Shooter Scenario - 5G Mid-Term Architecture View for Traffic Steering

The diagram shows 5G UEs including the UAS connecting to the 5G core and accessing the video server at the edge. The UAS establishes a data session with the video server application. The video server serving as an AF and running on an MEC within the 5G network can influence traffic steering through the 5G Core SBA Network Exposure Function (NEF). The NEF serves as a proxy for communication between untrusted AFs and the 5G control plane. If the AF is trusted and an agreement is established with the carrier, the AF can communicate with the 5G control plane directly. AF influence deploys the UPFs and the proper filtering and configurations to steer video traffic to the edge video server at the MEC. Decision makers can then establish a data session with the MEC video server and obtain live video that has improved in terms of latency in comparison to receiving a live video stream served in the central cloud.

The figure further illustrates a disaggregated RAN architecture and a 5G Core SBA. The Core SBA provides all control plane functionality and serves as the central orchestrator for both the 5G core and business enabled services, as well as the MEC application functions. All user plane traffic follows the DU/CU/UPF path. The CU is expected to be located much closer to the access location and incident edge, and further likely to be collocated in a metropolitan or regional datacenter, it has the capability to host the 5G user plane functions for traffic steering as well as the MEC applications for enabling video dissemination.

The UAS video server deployed near the edge is seen by the 5G core as an application function and has the ability to influence the traffic routing and steering. The 3GPP defines two methods for traffic steering and they are the:

1. Up Link Classifier (UL CL)
2. IPv6 Multihoming

The 5G control plane deploys and configures a UPF at the edge which will implement these methods. In order to filter and identify traffic to steer, the UL CL generally uses configured IP and Port combination provided by the SMF while IPv6 multihoming uses IPv6 prefixes [footnote: Note IPv6 multihoming control through SMF is only compatible with IPv6 addressing]. The UL CL method deploys a UPF with "UL CL functionality" while the IPv6 multihoming method deploys a UPF with "branching point functionality." Both methods use UPF session anchors (SA) to affix the traffic flow to the appropriately steered path. These features are unique to 5G and allow the matching of user plane traffic to custom flow rules thus enabling MEC at large. For additional details, see Appendix B.3.

In summary, the mid-term 5G evolution improves wireless data connectivity in degraded environments and moves the edge computing capability closer to the incident area. As a result, following challenges are improved:

1. Coverage is improved inside the school supporting both public community and first responder access to networks
2. UAS video is live streamed and processed at an edge data center closer to the incident area improving local access and latency
3. Automated 5G Core SBA and MEC application function LSO to provide optimized network resources that can support resilient information sharing at the edge, including scaling and healing of virtualized functions
4. Dynamic configuration of routing and traffic steering rules triggered by MEC AF improving access to edge services or driven by the network operator or orchestrators

While there are indeed improvements offered in this solution, it comes with the challenge of complexity and monetary costs to the public safety community. A fully automated environment where 5G NFs and MEC applications are deployed dynamically based on trigger conditions requires that the service orchestration systems were properly configured. Further it requires that systems be aware of the complete health and state of the network and all underlying physical infrastructure which must host the services. These parts will be hard and complex and thus any public safety community system which depends on it must be tested for end-to-end operation under varying loads and conditions.

Regarding the monetary costs, these solutions will likely impose fees well beyond those encountered for traditional access to a mobility network. Carriers are likely to charge for access to services, and features such as lifecycle management. Applications hosted in the cloud are likely to incur additional costs to cloud vendors and long term OPEX to maintain the solutions.

Regardless of the improvements offered by 5G in the mid-term scenario, operational gaps remain for the first responder community in the following ways:

1. School cameras remain attached only to school enterprise LAN
2. BWCs lack connectivity options
3. Access to video data is highly dependent on carrier managed service policies and partnerships with cloud computing environments for hosting MEC applications

4.2.3 Future Operational View

The operational view for the future envisions a 5G use case utilizing features and technologies from various specifications that exist or are under study today, but will likely take years to be deployed. The future scenario is an exemplary use case to discuss how the public safety can leverage future 5G capabilities to meet demanding mission needs like those required for a school shooting incident.

The future scenario includes a full-featured 5G network able to support quality of service performance guarantees for eMBB, mMTC, and URLLC services to ensure real-time access to information sharing. The 5G network uses MEC technology to enable processing and dissemination of data as it is being created at the scene of the incident. This leads to greater performance and new possibilities for situational awareness applications (e.g. augmented reality). Network slicing is used to aid delivery of the right information to the right set of users. This allows information sharing for operational interoperability (e.g. inter-agency/inter-jurisdiction information sharing), while also allowing the separation of information for delivery specific to a first responder's role. The 5G network is fully automated to provide and adapt MEC and slicing capabilities on demand at the edge as the mission evolves. As carriers will likely partner with vendors to deploy 5G connectivity and local services within enterprise networks, this scenario also envisions the school having its own 5G enterprise PNI-NPN. In which case, there is 5G access and MEC deployed on school premises and managed by the carrier. Through integrated access and automation, first responder devices are intelligently routed to access the on-premise MEC to share the schools information (e.g. surveillance video) in real time, further enhancing performance and situational awareness. This view is illustrated in Figure 40.

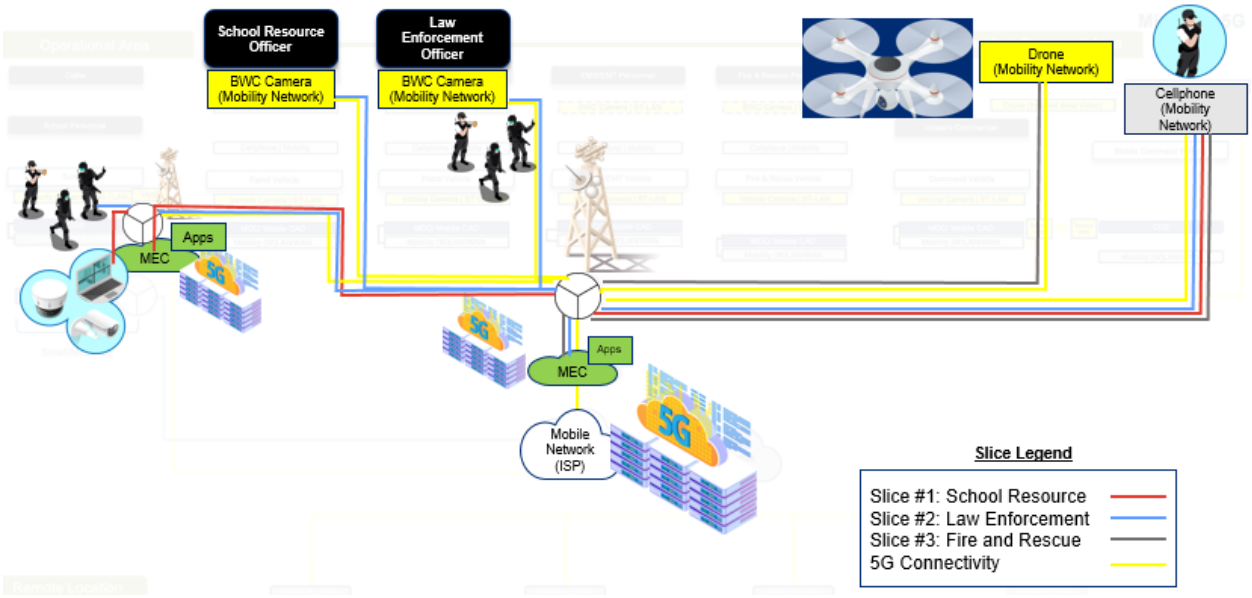


Figure 40 - Future operational view

There are many different architectures which could realize the future scenario. Further it should be expected that specifications and architecture designs will evolve over time and therefore it is not possible to predict how these features will ultimately be deployed. Therefore, different views are presented for consideration.

In the future scenario, the school's 5G enterprise network is deployed as an PNI-NPN, using carrier-deployed MEC and indoor microcells on the premises. Based on the RAN and control plane sharing NPN model, the indoor microcells are shared with access to the carrier's public network and network control tasks are also performed by the carrier. The NPN and public network are separated using slicing. Using this deployment allows local traffic paths between enterprise NPN 5G devices and the on-premise MEC. Secondly, with the carrier managing control tasks, like the subscription database, configurations for access to the NPN can be pushed to the 5G devices of first responders at the scene of the incident. When the first responder is in the coverage area of the indoor microcells, there devices can join the private slice and have a local path to the school's video surveillance data, sensor data, etc. Adding an on-premise MEC and using a private 5G network in conjunction with the public network allows data sharing between a private organization and first responders that are on the premises, providing URLLC and eMBB services. Moreover, because the indoor microcell is shared with the public network, a first responder can simultaneously connect to the public safety slices accessible via the public network, extending coverage for access to other slices. Figure 41 shows the deployment of the schools 5G NPN, represented by the black network components that form the "private" slice. The publicly shared infrastructure is represented by the blue network components and form the "public" slice.

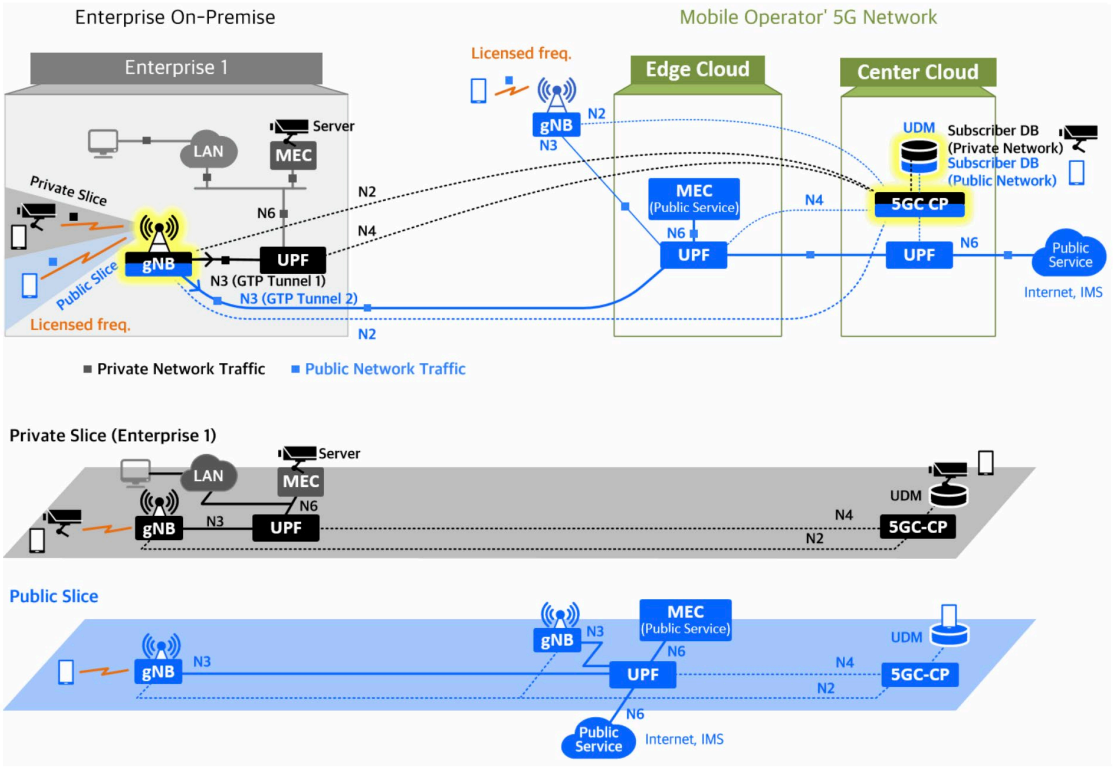


Figure 41 – Example deployment of the school's NPN, where the RAN and control plane are shared with the public network. The network slices show the separation between the private and public network. (Reference [39])

Another option is to provide first responders with access to the on-premise MEC from base stations outside of school premises where the incident commander and other responders are positioned during the event. To support this configuration there are multiple configuration options and it is hard to predict

what will be offered by the carriers. As illustrated in Figure 42, the UPF at the edge can have a leased line connection via the N6 interface into the school's LAN ideally through a firewall. For a more dynamic option shown in Figure 43, the NPN has been extended to outside the school[52]. A new, NPN uplink classifier UPF has been dynamically instantiated near the outdoor gNB, likely housed in the same datacenter hosting the public UPF, and an N9 interface is established for this new UPF to the on-premise UPF. In this case, similar to access within the school, the carrier managing control tasks, like the subscription database, configurations for access to the NPN can be pushed to the 5G devices of first responders at the scene of the incident to provide dual connectivity to both slices. In any case, there would need to be an agreement between the carrier and school to allow such connection for first responders.

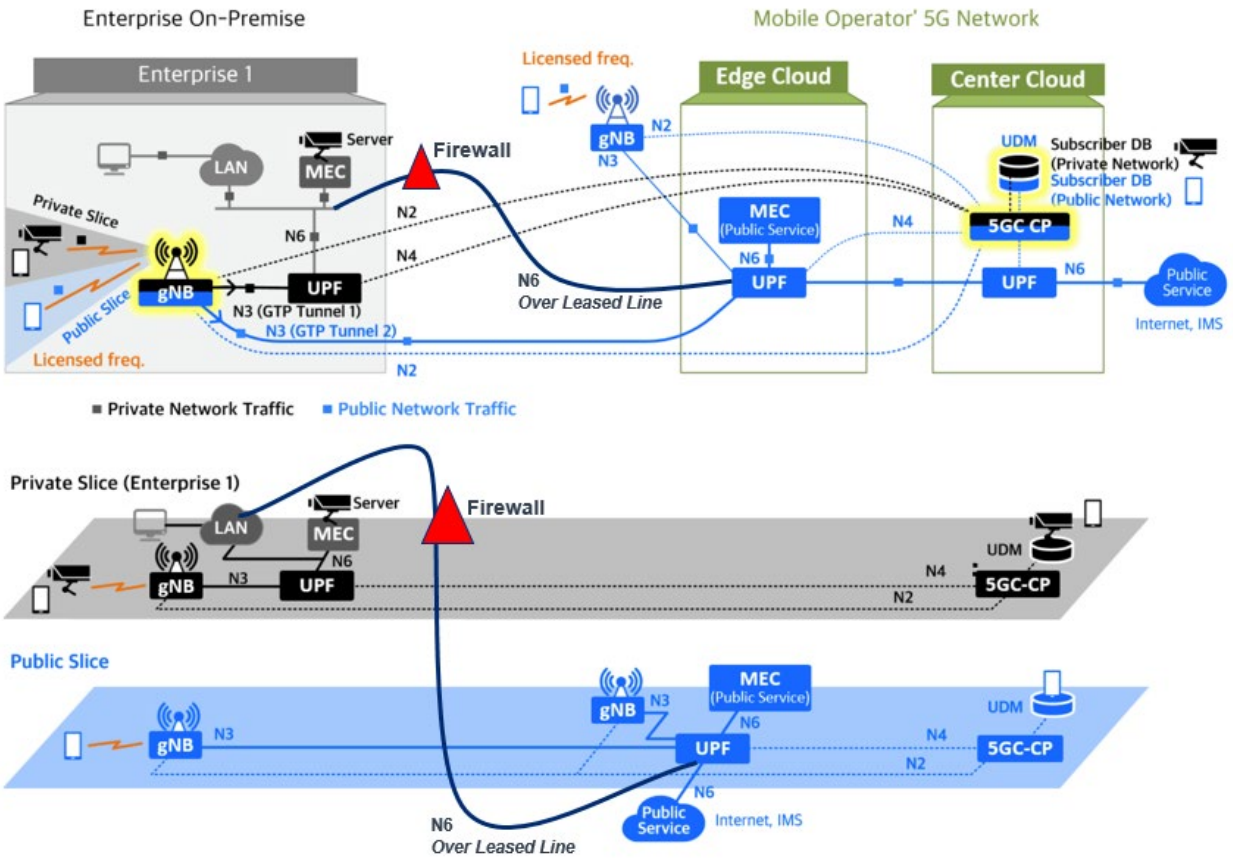


Figure 42 – Example deployment allowing publicly connected network users to access the on-premise enterprise MEC via internet provisioned leased line

[52] Note: these figures have been adapted from (Reference [38])

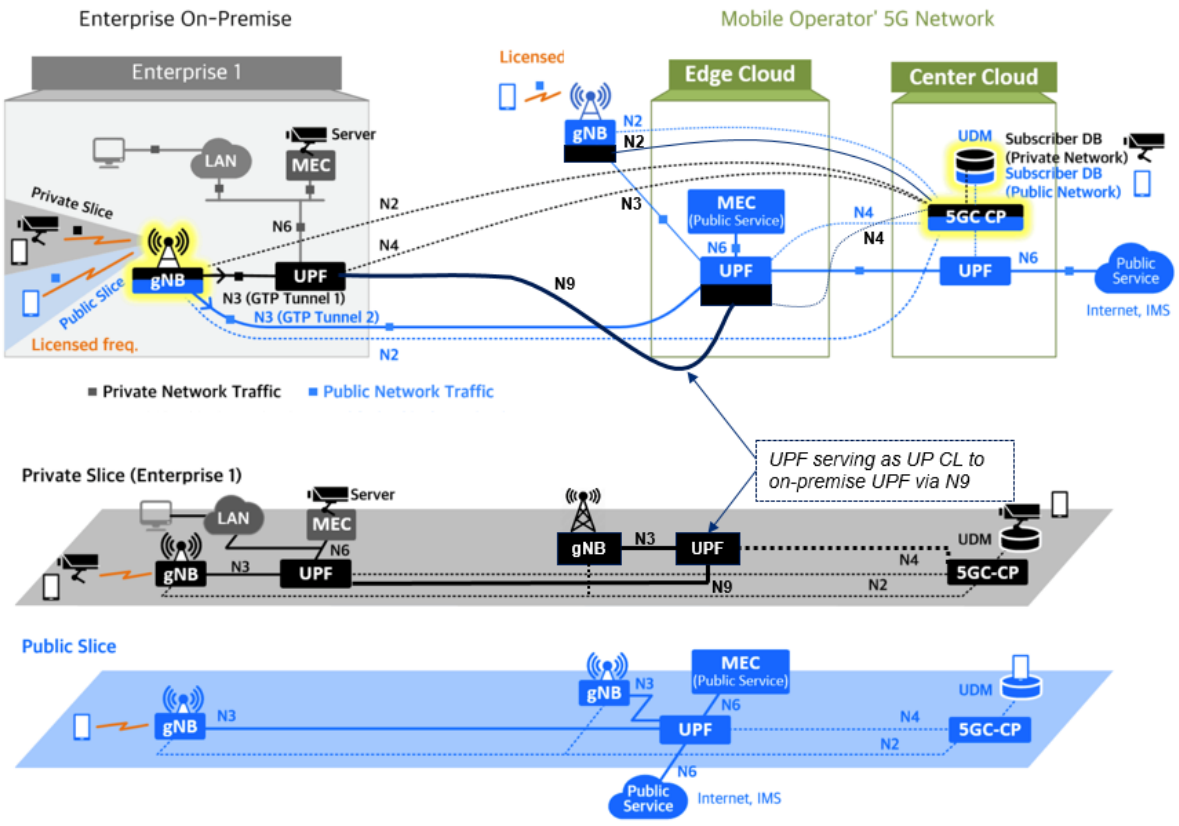


Figure 43 – Example deployment of dynamic instantiation of private network UPF for outdoor access to on-premise video

The Future 5G scenario also includes a MEC deployed at the edge, similar to the mid-term scenario. In this case, data from both the UAS and BWC are streamed to the MEC at the edge to allow access to the camera feeds and any analysis from the edge. As in the mid-term scenario, having the edge close to the first responders improves latency and throughput for data-heavy, real-time communication. Unlike the mid-term case, the future scenario also instantiates several network slice instances to the edge MEC as described in section 3.4.4, to manage information sharing. For example, one slice instance can be set up to only allow information suitable for multi-jurisdictional sharing. Additional slice instances can be set up for each first responder discipline (e.g., law enforcement, fire and rescue, EMS, etc.) to isolate traffic shared within a team. Alternatively, the slices could be based on traffic types. Video traffic can be assigned to one slice, while vital signs data from body worn sensors are assigned to a different slice. In any case, the slices are made available on demand and accessible in the cellular tracking areas of both the macrocells outside the school and the indoor microcells. Recall that the indoor microcells are shared infrastructure and therefore can allow access to other slices. The 5G network will assign the 5G devices (e.g., UAS, BWC, cell phones, etc.) slices based on subscription information. The 5G carrier can configure new slices for devices through the user equipment route selection policy (URSP) feature to allow dynamic configuration of slice selection policies. Moreover, a single device, such as those used by the incident commander, can be configured to access multiple (up to 8) slices simultaneously for full situational awareness. Figure 44 illustrates an example of multiple public safety slices (e.g. Slice 1 = School Resource Slice, Slice 2 = Law Enforcement Slice, and Slice 3 = Fire and Rescue Slice) to the edge MEC deployed along

with the private slice to the on-premise MEC[53]. This aligns with the operational view shown in Figure 40 at the beginning of this section.

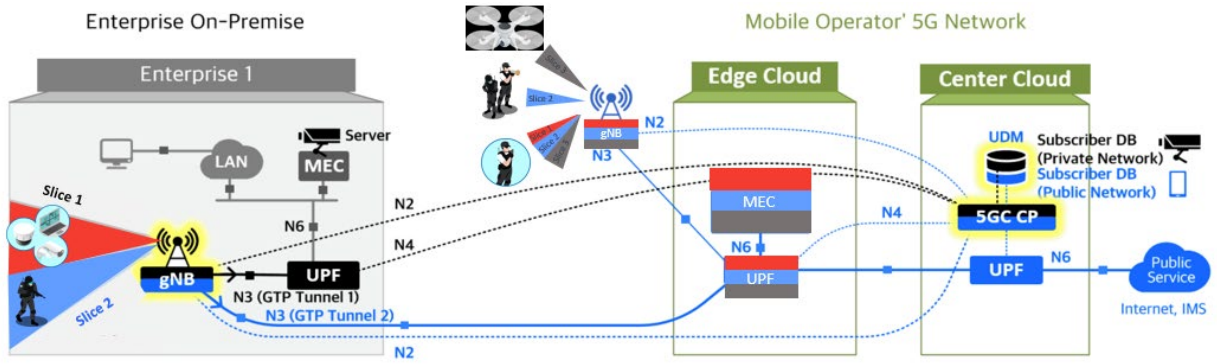


Figure 44 – Multiple public safety slices deployed for communication to the MEC at the edge

Similarly to the mid-term case, 5G's micro-service based, cloud-native, virtualized, infrastructure will continue to be developed and improved to provide a more seamless experience for optimizing network resources and steering traffic to the desired MEC application and location for the future scenario. SBA provides an architecture that allows for new features and functions to be seamlessly added which opens up 5G to provide benefits not yet defined. As MEC capabilities improve and availability of cloud services increase, there will more deployment options for MECs on-premise, far edge, and metro edge to improve quality of experience for users. The ability to bridge 5G enterprise networks with public infrastructure on-demand has the potential to significantly improve interoperability between the two different network domains allowing immediate access to data at the source with less latency and of higher quality.

From the enhanced capabilities of the future 5G scenario, the following improvements could be realized:

1. Coverage is improved in degraded areas so that data sharing can be more consistent
2. UAS footage can be live streamed and processed at an edge data center closer to the incident area improving latency and providing the means to centralize the collection and distribution of video.
3. Video data from the school can be live streamed and processed at on-premise MEC closer to the incident area improving latency and providing the means to centralize the collection and distribution of video.
4. BWCs can be 5G enabled and video footage could be live streamed and processed at an edge data center closer to the incident area, improving latency and providing the means to centralize the collection and distribution of video.
5. Instead of multiple transport networks, video data can be collected, processed and distributed on a common network
6. Different network slices can be activated to handle different information sharing needs for operational interoperability
7. By leveraging the policies and services defined at the business enablement layer, access to information could potentially be automated

[53] Note: this figure has been adapted from (Reference [38])

8. Optimized network resources at the user on premise edge, far edge and metro edge for 5G connected devices
9. A secure 5G architecture that provides a more seamless way to add additional features more easily to the network and so features and capabilities of 5G that have not yet been defined are a possibility for the future.

Note: The application-level capabilities described are not available today. All necessary end-to-end data management systems, and applications supporting the ingestion, processing and sharing of video data at from the source and out to the end users need to be already developed and available for the public safety community.

4.3 IMPACT TO PUBLIC SAFETY

The future systems view described here offers a view of a fully enabled 5G scenario where the network and services have been optimized to meet the public safety requirements. MEC is able to host applications that support improved access to information with reduced latency at the incident area network. Virtualization and business driven service automation allows for automated deployment of applications and functions based on defined trigger conditions configured within the network. Dynamic network slicing allows for connecting the right people to the right information at the right time, while simultaneously filtering access to information both improving security and operational effectiveness. Together, these various solutions will likely improve the operational quality of experience during an incident and further improve multi-jurisdiction and multi-agency interoperability.

While this report focused on information sharing of video at the incident area network, the same 5G technologies could be applied to enable an array of other public safety solutions. These could include hosting of building blueprints, first responder biometric monitoring applications, or even edge analytics which will enable many of the next generation first responder use cases. Through automated controls, systems within the network could identify buildings, end users, and systems within the vicinity, and self-configure to advertise these services as they are instantiated, alleviating the burden from operators at the scene.

With all this said, the future system view represents an idealistic view of 5G networks where technologies and enablers have been deployed as they are envisioned by futurists, marketers, and SDOs. As 5G will evolve over time, it is extremely challenging to predict how 5G technologies will be deployed and implemented. For simplicity of concept and scenario building, authors of this paper made scenario-based assumptions for use case building purposes. In an ideal scenario, the public safety community fully embraced 5G technologies and all systems and first responders are connected to the same network. While this is extremely unlikely even in the long term, it is necessary to scope this use case merely as an example of what 5G could enable. As designers and the public safety community look to further research these technologies, some additional considerations are noted below:

- NPN challenges:
    - Public safety community access to standalone NPN with private subscriber identity databases will be impossible
    - For PNI-NPN, roaming is a likely solution, however this requires roaming agreements between the local enterprise and the public networks. Further, solutions such as edge computing traffic steering and UPF selection, as well as application function influence

over 5G NF behavior, is only supported in one of the two 5G roaming architecture. (See Appendix B.3 for more details.)
    - Both standalone and PNI-NPN will likely use unlicensed spectrum (e.g., CBRS or ISM bands). This means access may be device dependent and further, provided in a contention based environment with limited mission critical guarantees.
- Network Slicing
    - Network slicing is designed to provide strict isolation between slices and the only supported way to transport or receive information on different slices is to attach to each. The 3GPP specifications only allow for connecting to 8 slices simultaneously which may limit some options for interoperability in the future.
    - Application support for attaching to multiple slices has yet to be demonstrated as network slicing is still being standardized. Further it is unclear how common MEC and NFV infrastructure will be integrated with network slicing, and will likely be highly dependent on vendor implementation.
- MEC
    - There are many flavors of edge computing today and this will remain true in the future. Carriers will partner with one or more cloud vendors who will each deploy different edge computing resources, with different software controls and interfaces.
    - MEC will be complicated by the locality of deployment, with large metropolitan centers likely having access to one or more of the primary market cloud environments, however rural locations having few options or still being a great distance away.

5 5G IMPACTS, OPPORTUNITIES, AND CHALLENGES

The goal of this study was to investigate the various impacts, opportunities, and challenges that 5G mobile broadband networks will bring to the first responder community. Several of the key 5G enablers have been discussed to investigate their capabilities, characteristics, and architecture according to the specifications. As a general takeaway, it should be obvious that 5G will likely impact the first responder community in many ways. The 5G networks are expected to bring a wide range of new use cases enabling integrated sensors and Internet of Things (IoT), increased capacity, and advanced routing and access to information. It is further likely to enable more futuristic use cases such as autonomous vehicles and drones, self-adapting networks, and edge analytics. However, it should also be noted that the public safety communication space is becoming increasingly complex with more and more data, tools and transport pathways than ever before. This is both a welcomed change as well as one that poses a number of challenges for end-users and operational personnel. While technology advancements bring new capabilities that are greatly needed, they also provide for a more complex data and information sharing environment that can be overwhelming.

As the public safety community looks to embrace 5G technologies, it is important to differentiate the vision of 5G versus the reality of 5G. Much like all previous versions of mobile broadband networks, the 5G will be an evolution. As noted in Section 3, the standards follow a release cycle with deployments lagging behind standards by 1-3 years on average and many of the advanced features of 5G will take even longer. Some may never even come to fruition unless there is a clear monetization strategy for carriers. Many of the use cases and marketing promotions that are seen today describe the vision of 5G. The reality is much different and the future is hard to predict. This results in a perception of what 5G can offer being incorrect, and the terms and technologies used to describe 5G not being consistent and clear. This is true even for both the mid-term and future 5G systems view described in this report.

It is important to note that in order for 5G to enable these new use cases, many technologies are being absorbed by the carriers and SDOs. This means 5G comes with increased complexity, a larger footprint, and many new vendors and partnerships. The conversation to enable specific features or leverage the 5G vision will involve partnerships beyond just the carriers, including companies and standards organizations with less proven record of success. This could result in increased costs and time to market for new technologies. In addition, many of the existing legacy infrastructure in use in public safety today were not designed for the integration and interoperability of these advanced technologies and transport mechanisms.

The takeaways from this report are summarized below and categorized as impacts, opportunities, and challenges. The impacts describe expected positive improvements that 5G will bring to the public safety community. The opportunities describe areas where the public safety community should invest and continue research to determine how best to leverage 5G technologies. Lastly, the challenges describes areas of concern as the public safety community approaches the full deployment of 5G technologies.

5.1 IMPACTS

1. New emergency responder use cases: 5G expected to enable three pillar use cases including eMBB, mMTC, and URLLC that will depend heavily on key enablers including 5G Core SBA, disaggregated RAN, MEC, and Network Slicing. Services offered will be tailored more to the end

user needs and provide increased quality of service and quality of experience. For the public safety community this means new systems and methods to access a network and better control for moving the right information to the right place at the right time.

2. Improved network and radio access resilience: 5G networks are being designed following a microservices architecture built on virtualization technologies with robust management and orchestration to ensure automated lifecycle management and self-healing and self-scaling capabilities. This translates to improved resilience and will play a key role in delivery of mission critical services such as voice and data information transport.
3. Cloud-based interoperable solutions: 5G networks and especially the capabilities such as multi-access edge computing, traffic steering, and business driven policies and controls will provide new locations to develop and deploy interoperable solutions for the first responders. The 5G networks are standardizing procedures to support interoperability among multiple access technologies and allows for placing applications for information fusion, processing, and dissemination near the end user. The business driven services will allow for monitoring of trigger conditions to enact these services automatically. It may be possible for 5G services to even advertise its capabilities to arriving first responders using disparate devices and networks thus facilitating operational interoperability.

5.2 OPPORTUNITIES

1. Business and mission driven network services: 5G networks will enable the end users to assert far more control over the services they need than previous generation networks. This comes in the form of both initial configuration of service policies within the network as well as from the tight integration from Application Functions (AFs) which can influence the real-time behavior of 5G networks through exposed interfaces. This has the opportunity to enable many new features and capabilities for the public safety community.
2. Faster to market first responder solutions through agile software development methodologies: 5G will enable cloud-enabled software solutions all throughout the network including on-premise, far edge, and core network locations. Application vendors and mobile broadband carriers will both promote rapid development of software solutions following the agile cloud-native principles including SecDevOps, and Continuous Integration, Continuous delivery (CI/CD) to drive innovation and agility across the network infrastructure. For the public safety community, this allows for new solutions to be prototyped and improvements to be added over time.
3. Integration with next generation first responder solutions and 911: As noted throughout the report, the public safety community is embracing the digital revolution in various ways including promoting advanced capabilities for the next generation first responder and improved public safety access and information sharing with 911 services. Many of the new use cases and features envisioned for 5G has the potential to enable both.

5.3 CHALLENGES

1. Complexity of 5G systems and enablers: The 5G network as noted throughout this report includes far more complexity than previous generation networks and goes well beyond radio access base stations, voice communications, and wide area network internet access to data. It will include many new technologies such as virtualized cloud-native architecture, services deployed to the edge, and highly dynamic network slices. While these solutions will likely be the pathway to

previously noted impacts and opportunities, it comes with many challenges. These include public safety coordination with new vendors and a large set of SDOs. Increased complexity is also likely to impact resilience of end-to-end solutions. If the public safety depends on an edge application or automated controls, but some component in the path fails, then access to the service at large may be impacted. Lastly, autonomous solutions driven by artificial intelligence will require a great deal of trust from the operators. While this will be necessary over time to enable truly robust, resilient, and adaptive communications networks and software solutions, it speaks to the timescale for when to expect some of these features.

2. Variability in 5G deployments: While mobile broadband networks and even the enablers such as multi-access edge computing follow standards, these are often limited to architecture, core functions, and exposed interfaces. This means the carriers and solution vendors have the flexibility to deploy many of their own functions and capabilities. Further due to the complexity and scale of future 5G networks, there remains many degrees of freedom for deployment options. This is especially true for solutions that leverage the cloud or dynamic network solutions such as network slicing. Even among the same carrier, solutions and configurations available will likely be dependent on locality and supporting systems like access to edge computing datacenters. This will challenge any solutions that claim to be interoperable
3. End-to-end mission critical services: The 5G SDOs have developed several standards for definition and approach to mission critical services including MCPTT, MCVideo, and MCData. While carriers are incentivized to make this work, there may be service and functionality limitations imposed to ensure resilience and quality guarantees are met. This could be especially true for services that depend on the MEC or dynamic network slicing enablers. The challenge will be approaching these solutions offered to the public such that they meet the end-to-end mission critical service delivery required by the public safety community.
4. Information Security: Information security, while not discussed in this report, is a continuous challenge and moving target as technologies and security protocols evolve. This chiefly includes data integrity and availability (reliability). As 5G solutions look to automate service delivery and access to information, special care must be taken to ensure the security of all systems and information are maintained.

6 PATH FORWARD

For the public safety community to successfully leverage advanced 5G technologies as they are introduced to market, DHS S&T and their operational components must continue to understand the impact of technological advancements, track the various standards organizations, and plan for where and how to focus their efforts. An approach to this, previously authored by APL, includes a set of seven tenants for addressing 5G RDT&E (Reference [42]). These are shown below.

Tenants of the Process Model

- Environmental Scan and Analysis of the 5G Impact to the DHS S&T Customer Components
- Adapt/Develop Use Cases that Demonstrate Adaption and Integration of 5G Technologies Relevant to DHS S&T Customer Components
- Map 5G efforts to DHS S&T Operational Components' Requirements
- Leverage Existing Efforts to Contribute to Optimization and Deployment
- Leverage Opportunities for Standards Contribution
- Support Testing and Evaluation Efforts and Provide Recommendations and Feedback from the End-User Communities
- Support Transition for Operational Deployment

In addition to these tenants, the public safety community will need new first responder focused solutions including hardware, software, and AI/ML for supporting interoperability and automated information sharing. APL offers a set of recommendations for any first responders looking for an approach to 5G enabled information sharing at the incident area edge network. These recommendations should further serve to remediate some of the challenges previously discussed.

6.1 RECOMMENDATIONS

1. DHS S&T should levy 5G mobile broadband network requirements from the public safety community that intends to leverage edge computing and network slicing to identify any quality requirements, performance expectations, security controls, and functional capabilities required. Clearly identify how the solutions will be used, which systems and users would access the solutions, and who would maintain administrative control over the solutions. For driving the autonomous behavior of the solutions, define how and where key performance indicators will be monitored and identify the various trigger conditions which would execute the lifecycle instantiation. These answers will directly influence how developers and systems engineers will approach solutions and inform the conversations with mobile network operators and other vendors.
2. Develop an information generation, processing, and sharing framework to identify the various information sources and destinations along with the information characteristics and requirements. Identify the sources of information critical to first responder incident management and develop the requirements for hardware and software that captures and collects the data. These will inform both the hardware and software solutions as well as the policies and controls, which govern any first responder mission dependent autonomous behavior within the 5G network.
3. Develop new first responder processes and procedures to validate end-to-end systems posture, standards conformity, and ability to meet the mission critical quality and resilience requirements.

Because many systems may be involved in the ultimate solution, including overlap of multiple standards organizations, it will be necessarily to validate each component in the end-to-end path. This includes RAN loading, edge compute infrastructure validation, software solutions unit testing, and validation of business level automation controls under many different conditions. Special care should also be taken to continually monitor, test, and version control all cloud based software solutions following the agile CI/CD workflow. Require that all solutions generated clearly define which standards were leveraged for information the solution design and define all interfaces leveraged or exposed.

4. Approach the entire 5G ecosystem concerning requirements and standards influence. While the 3GPP SDO remains the primary organization for the 5G network, it will lean heavily on the ETSI, ONF, IETF, MEF, and others for their area of expertise. This is especially true for solutions which leverage virtualized technology on common infrastructure resources or the business driven service and lifecycle orchestration. It is likely the public safety community will demand additional requirements on commercial solutions not identified by generic use cases. The public safety requirements will help scope and define the ultimate frameworks and exposed interfaces that remain in standardized solutions.

This report has focused on information sharing at the edge and included various 5G SA technologies including SBA and RAN disaggregation, and various 5G enablers including virtualization, MEC, network slicing, and NPNs. However, these are only a few pieces of the larger 5G technology roadmap. In order to continue assessing the impact of 5G technologies onto the public safety community or other DHS S&T operational customer components, it will be necessary to research additional enablers including:

- Flexible RAN technologies including the New Radio, Massive-Multiple Input Multiple Output (MIMO), Multi-user MIMO, mmWave, beam steering, scalable numerology, etc.
- New waveforms for mMTC use cases including Narrow Band IoT (NB-IoT) and Category-M (Cat-M)
- Software-defined Transport networks for intelligent traffic engineering and path aware routing
- Proximity Services (ProSe) for enabling device-to-device communication
- Integration with non-3GPP network types such as LMR to LTE/5G
- Open architecture solutions including Open-RAN
- AI/ML integration, service orchestration, and zero-touch automation

7 CONCLUSION

This report concludes by acknowledging the complexity of the overall 5G networks and systems described herewith. The 5G networks expand well outside the bounds of historical mobile broadband networks that focused primarily on voice communications and standards around radio access. To ensure business and mission driven services that will impact the public safety community and improve interoperability among various jurisdictions and agencies at all levels of government, it will be necessary to adopt many of the virtualized, service-based features of 5G. It will also be necessary to leverage edge computing and network slicing functionality in order to reduce latency and processing time to information at the edge and ensure the information is securely filtered and distributed to the right people at the right time.

Adoption of these features will be greatly enabled by incremental proof-of-concepts and trial deployments, leveraging partnerships among both industry and academia. While there may exist opportunities to leverage complete 5G networks from either commercial mobile network operators or other Department of Defense (DoD) experimentation efforts, developing and prototyping solutions should take a stepwise approach. Once use cases and requirements have been captured, and the specific 5G technology enablers identified, engineers can develop scoped prototype solutions which focus on algorithms and common interfaces. During this phase, solutions can be tracked for standards adherence and any required deviations shall provide for opportunities to engage and influence the SDOs. There are many experimental testbeds for advanced networking and radio technologies which can serve as a stepping stone for public safety community 5G research and development.

To reiterate, 5G is an evolution of technologies and any end-to-end solution will involve a mix of different vendors and SDOs. Thus, anyone in the public safety community looking to leverage 5G in the future will need to approach the SDOs and technologies as a fully integrated ecosystem in order to be successful.

8 ACRONYMS

4G	4th generation
5G	5th generation
5G RG	5G Residential Gateway
5GS	5G System
5GSA	5G System Architecture
AF	Application Function
AKA	Authentication Key Agreement
AMF	Access and Mobility Management Function
AN	Access Network
API	Application Programming Interface
AR	Augmented Reality
AUSF	Authentication Server Function
BBU	Base Band Unit
BSO	Broward Sheriff's Office
BSS	Business Systems Support
BWC	Body Worn Camera
CBRS	Citizens Broadband Radio Service
CN	Core Network
CP	Control Plane
CSfC	Commercial Solutions for Classified
CSPD	Coral Springs Police Department
CU	Central Unit
D2D	Device to Device
DHS	Department of Homeland Security
DN	Data Network
DNAI	Data Network Assistance Information
DoD	Department of Defense
DU	Distributed Unit
E2E	End-to-End
eMBB	Enhanced Mobile Broadband
eNB	Enhanced NodeB
EMS	Emergency Medical Service
EOC	Emergency Operation Center
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FN-RG	Fixed Network Residential Gateway
gNB	Next Generation NodeB
HPLMN	Home Public Land Mobile Network
IACP	International Association of Chiefs of Police
IETF	Internet Engineering Task Force

IC	Incident Command
IMS	IP Multimedia System
IoT	Internet of Things
ITU	International Telecommunication Union
KPI	Key Performance Indicators
LAN	Local Area Network
L2	Layer 2
L3	Layer 3
LBO	Local Break-Out
LEO	Law Enforcement Officer
LMR	Land Mobile Radio
MANO	Management and Orchestration
MCMBMS	Multimedia Broadcast Multicast Service
MEAO	MEC Application Orchestrator
MEC	Multi-access Edge Computing
MEO	MEC Orchestrator
MEPM	MEC Platform Manager
MCTn	Mission, Content, Transport Network
mMTC	Massive Machine Type Communications
MIMO	Multiple Input Multiple Output
MSD	Marjory Stoneman Douglas
MSDHS	Marjory Stoneman Douglas High School
MSD-PSC	Marjory Stoneman Douglas High School Public Safety Commission
NAS	Non-Access Stratum
NB	Narrow-Band
NEF	Network Exposure Function
NECP	National Emergency Communications Plan
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
NFV-MANO	NFV Management and Orchestration
NGFR	Next Generation First Responder
NS	Network Slice
NIMS	National Incident Management System
NPN	Non-Public Networks
NPSTC	National Public Safety Telecommunications Council
NRF	Network Repository Function
NRT	Non-Real Time
NR-U	New Radio Unlicensed
NSSAI	Network Slice Selection Assistance Information
NSSAAF	Network Slice Specific Authentication and Authorization Function
NSSF	Network Slice Selection Function
OIC	Office for Interoperability and Compatibility
ONAP	Open Network Automation Platform

ONF	Open Networking Foundation
OSM	Open Source Mano
OSS	Operations Systems Support
PCC	Policy Control and Charging
PCF	Policy Control Function
PIO	Public Information Officer
PLMN	Public Land Mobile Network
PNI-NPN	Public network integrated NPN
ProSe	Proximity Based Services
PSA	PDU Session Anchors
PSAP	Public Safety Answering Point
QoS	Quality of Service
RAN	Radio Access Network
RRU	Remote Radio Unit
RTF	Rescue Task Force
S&T	Science and Technology Directorate
SBA	Service-based Architecture
SBI	Service-based Interface
SCP	Service Communications Proxy
SDN	Software Defined Network
SDO	Standards Development Organization
SEPP	Security Edge Protection Proxy
SLO	Service Level Objective
SMF	Session Management Function
SNS	SAFECOM Nationwide Survey
S-NSSAI	Single Network Slice Selection Assistance Information
SRO	School Resource Officer
SSC	Session and Service Continuity
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscriber Permanent Identifier
TC	Technology Center
3GPP	Third Generation Partnership Project
UAS	Unmanned Aerial System
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UL- CL	Up Link Classifier
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communications
USIM	Universal Subscriber Identity Module
VPLMN	Visited Public Land Mobile Network
VR	Virtual Reality

WAN	Wide Area Network
WG	Working Group
WLAN	Wireless Local Area Network

9 REFERENCES

[1] DHS S&T First Responders Group, "Advanced Communications Video Over LTE: Efficient Network Utilization Research," December 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/VQiPS_T3X3_2%206%209%202_EfficientUtilization_MemorandumReport_Final_Draft_v4-508.pdf. [Accessed April 2021].

[2] DHS S&T Next Generation First Responder APEX Program, "Next Generation First Responder Case Study: Enhanced Situational Awareness," January 2020. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/enhanced_situational_awareness_ngfr_case_study_harris_county_01.30.2020-508.pdf. [Accessed April 2021].

[3] Defining Public Safety Grade Systems and Facilities. Littleton: NPSTC; 2014:24

[4] CTIA, "The 4G Decade: Quantifying the Benefits," July 2020. [Online]. Available: https://api.ctia.org/wp-content/uploads/2020/07/The-4G-Decade.pdf. [Accessed April 2021].

[5] Federal Communications Commission, "2020 Communications Marketplace Report," December 2020. [Online]. Available: https://docs.fcc.gov/public/attachments/FCC-20-188A1.pdf. [Accessed April 2021].

[6] Cybersecurity and Infrastructure Security Agency (CISA), "NECP Webinar: 5G Is Here: How Will This Impact Emergency Communications?," December 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/NECP%20Webinar_Technology%205G_%28December%202020%29%20Slide%20Presentation_508C.pdf. [Accessed April 2021].

[7] International Telecommunication Union, "IMT Vision - Framework and overall objectives for the future development of IMT for 2020 and beyond. Recommendation ITU-R 2083-0," 2015

[8] Next Generation Mobile Network (NGMN) Alliance, "5G White Paper," February 2015. [Online]. Available: https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf. [Accessed April 2021].

[9] National Public Safety Telecommunications Council, "Public Safety Internet of Things (IoT): Use Case Report and Assessment Attributes," June 2019. [Online]. Available: https://www.npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf. [Accessed April 2021].

[10] 3GPP TS 23.501, System Architecture for the 5G System; Stage 2," Release 15, Version 15.7.0, September 2019

[11] Next Generation Mobile Network (NGMN) Alliance, "Service-Based Architecture in 5G," January 2018. [Online]. Available: https://www.ngmn.org/wp-content/uploads/Publications/2018/180119_NGMN_Service_Based_Architecture_in_5G_v1.0.pdf. [Accessed April 2021].

[12] International Telecommunication Union, "Transport Network Support of IMT-2020/5G, GSTR-TN5G," 2018

[13] European Telecommunications Standards Institute, "Network Function Virtualization (NFV); Infrastructure Overview, NFV-INF 001 v1.1.1," 2015

[14] TOSCA Simple Profile for Network Functions Virtualization (NFV) Version 1.0," 11 May 2017. [Online]. Available: http://docs.oasis-open.org/tosca/tosca-nfv/v1.0/tosca-nfv-v1.0.html.]

[15] M. Bjorklund, "RFC 7950: The YANG 1.1 Data Modeling Language," 21 January 2021. [Online]. Available: https://datatracker.ietf.org/doc/rfc7950/. [Accessed April 2021].

[16] A. Bierman, M. Bjorklund, J. Schonwalder, K. Watsen and R. Wilton, "RFC 8525: YANG Library," 16 March 2021. [Online]. Available: https://datatracker.ietf.org/doc/rfc8525/. [Accessed April 2021].

[17] R. Enns, M. Bjorklund, A. Bierman and J. Schonwalder, "RFC 6241: Network Configuration Protocol (NETCONF)," 21 January 2020. [Online]. Available: https://datatracker.ietf.org/doc/rfc6241/. [Accessed April 2021].

[18] M. Bjorklund, J. Schonwalder, P. Shafer, K. Watsen and R. Wilton, "RFC 8526: NETCONF Extensions to Support the Network Management Datastore Architecture," [Online].

[19] European Telecommunications Standards Institute, "Network Function Virtualization (NFV); Management and Orchestration; VNF Packaging Specification, NFV-IFA 011 v2.1.1," 2016

[20] European Telecommunications Standards Institute, "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; NFV descriptors based on YANG Specification, GS NFV-SOL 006 V2.7.1," 2019.

[21] European Telecommunications Standards Institute, "Network Function Virtualization (NFV); Management and Orchestration, NFV-MAN 001 v.1.1.1," 2014

[22] MEF Lifecycle Service Orchestration (LSO): Reference Architecture and Framework, Service Operations Specification MEF 55

[23] 3GPP, "5G Management and Orchestration; Concepts, Use Cases, and Requirements, TS 28.530 version 15.0.0," 2018

[24] 3GPP TS 28.531, "Management and orchestration; Provisioning," Release 16, Version 16.9.0," 2021

[25] 3GPP TS 28.532, "Management and orchestration; Architecture framework," Release 16, Version 16.7.0," 2021

[26] Ciena – The Adaptive Network White Paper “The Adaptive Network: A Framework for Understanding the Networking Implications of the Edge Cloud”, Ciena Corporation, 2020

[27] European Telecommunications Standards Institute, "Multi-access edge computing (MEC); Framework and Reference Architecture, GS MEC 003 v2.2.1, 2020

[28] "MEC in 5G networks," June 2018. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf. [Accessed April 2021].

[29] European Telecommunications Standards Institute, "Multi-access Edge Computing (MEC); MEC 5G Integration, GR MEC 031 V2.1.1 ," 2020

[30] J. Ordonex-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca and J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," IEEE Communications Magazine, no. May, pp. 80-87, 2017

[31] T. Saboorian and X. Amanda, "Network Slicing and 3GPP Service and Systems Aspects (SA) Standard," IEEE Software Defined Networks, Dec. 2017

[32] GSM Association, "Generic Network Slice Template, Version 4.0," 23 November 2020. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v4.0-1.pdf. [Accessed April 2021].

[33] W. Chen, "5G Network Slicing Seminar, Network Slicing Task Force (NEST) Summary of activity," June 2018. [Online]. Available: https://www.gsma.com/futurenetworks/wp-content/uploads/2018/07/1_2_GSMA-Progress-of-5G-Network-Slicing_GSMA-NEST_vice-chair.pdf. [Accessed April 2021].

[34] GSM Association, "Generic Network Slice Template, Version 4.0," 23 November 2020. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v4.0-1.pdf. [Accessed April 2021].

[35] T. Tovinger, "Management, Orchestration, and Charging for 5G networks," March 2018, https://www.3gpp.org/news-events/1951-sa5_5g

[36] A. Rao, "5G Network Slicing: Cross-Domain Orchestration and Management Will Drive Commercialization," September, 2020.

[37] 3GPP TS 22.261, "Service requirements for the 5G system", Release 16

[38] 3G4G.CO.UK, "Advanced: Private Networks & 5G Non-Public Networks," February 2020. [Online]. Available: https://www.slideshare.net/3G4GLtd/advanced-private-networks-5g-nonpublic-networks. [Accessed April 2021].

[39] H. J. Son, "7 Deployment Scenarios of Private 5G Networks," NETMANIAS, October 2019. [Online]. Available: https://www.netmanias.com/en/?m=view&id=blog&no=14500&xtag=5g-edge-kt-sk-telecom&xref=7-deployment-scenarios-of-private-5g-networks. [Accessed April 2021].

[40] Active Shooter Model Policy Concepts & Issues Paper Need to Know. Theiacp.org. https://www.theiacp.org/sites/default/files/2018-08/ActiveShooterBinder2018.pdf. Published 2018. Accessed April 12, 2021.

[41] 2019. Initial Report Submitted to the Governor, Speaker of the House of Representatives and Senate President. [online] Marjory Stoneman Douglas High School Public Safety Commission. Available at: <http://www.fdle.state.fl.us/MSDHS/Meetings/2018/December-Meeting-Documents/Marjory-Stoneman-Douglas-High-School-Public-Draft1.aspx>

[42] Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office for Interoperability and Compatibility Technology Center (OIC-TC), "5G Research and Development Roadmap for DHS S&T Operational Customer Components," 22 May 2020

Appendix A MARJORY STONEMAN DOUGLAS COMMUNICATIONS ASSESSMENT

A.1 VIDEO AND COMMUNICATION CHALLENGES AT THE MARJORY DOUGLAS STONEMAN HIGH SCHOOL

The Marjory Stoneman Douglas school shooter is a representative case for the critical need to get the right information to the right people at the right time. On February 14, 2018 an active shooter enters the Marjory Stoneman Douglas High School through Building 12 at 2:21:16 PM and exits the building at 2:27:54 PM, leading to the death of 17 individuals and causing injuries to 17 other people.

An initial report by the Marjory Stoneman Douglas High School Public Safety Commission (MSD-PSC) detailed the chain of events leading up to the school shooter event and his subsequent arrest (Reference [41]). The report provides detailed timelines and relevant contextual interview and collaborated by BWCs and surveillance cameras mapping a comprehensive picture of the operational response. The commission found multiple factors which contributed to the breakdown of the response picture. Focus will be placed on key elements of information sharing and communication which hampered the response posture related to this report which are radio coverage and video information sharing.

A.2 RADIO COVERAGE CHALLENGES

From a radio coverage standpoint, the report concluded that "the sporadic functioning of Broward Sheriff's Office (BSO's) radios undoubtedly hindered BSO's response. To an unknown extent, the school structure itself also hindered the radio functionally." This is observed thorough footage from the school's camera system as well as the BWC that the officers were wearing. For example, Officer Gonzalez stated "I can't key up here. There's no comms. I gotta go back outside", then Gonzalez ran down the west stairwell and out of the west door of building 12. The report further explained that the MSD-PSC investigators learned from BSO homicide detectives that due to radio failures BSO SWAT was forced to use a runner system to exchange information. When the investigators observed Gonzalez was frequently seen running up and down the stairwell when the investigators viewed the school surveillance video, leading to the conclusion that Gonzalez and another officer from the BSO SWAT were the primary compunction "runners".

While the Coral Springs Police Department (CSPD) didn't have congestion issues on their radio system, the BSO radio system encountered capability problems. Other communication problems were rooted in interoperability issues resulting from independent radio systems, patching and not leveraging the mutual aid radio channels that were already established.

A.3 VIDEO DATA CHALLENGES

The perpetrator entered Building 12 at 2:21:16 PM and exited Building 12, 6 minutes and 38 seconds later, at 2:27:54 PM. When reviewing the report an observation can be made that throughout the whole response timeline, including the time after the perpetrator left the premises, the suspect could not be reliably located. In reference to the school camera system, the MSD-PSC found that, "While not law enforcement's fault, the school's staff lacked adequate ability to operate the camera playback system. The fact that law enforcement erroneously believed for a considerable amount of time that Cruz was still in the building and was being watched on camera misled officers and deputies and adversely affected their decision-making and victim rescue efforts."

To give perspective on the challenges, the timeline has been decomposed to specifically highlight events surrounding problems related to sharing of video and its impact in deployed response at building 12 with the video sharing aspect of the timeline as shown in Table 8.

Table 8 – Decomposed Incident Timeline

Time	**Elapsed Time**	**Description**
2:19:00 PM	-0:02:38	Nikolas Cruz was dropped off by an Uber on Pine Island Road east of building 12. He was wearing a pair of black pants, a burgundy MSDHS JROTC shirt and a dark colored ball-cap. He continued west toward building 12 and during that time he was seen by Campus Monitor Andrew Medina.
2:21:16 PM	-0:00:22	Cruz entered the east hallway doors of building 12. Students Ashley Baez, Luke Hoyer and Martin Duque entered the building immediately prior to Cruz's entry.
2:21:38 PM	First Shot	Cruz fired the first rounds to the west of the first-floor hallway. Four victims were all shot in the hallway. Only 1 survived
2:22:13 PM	0:00:35	The first 911 call was made.
2:27:54 PM	0:06:16	Cruz exited the west end of building 12 and fled west between buildings 6 and 13. Upon reaching the northwest corner of building 6, he turned left (south), and continued running south to the southwest corner of building 9 and continued running southwest toward the group of fleeing students.
2:29:16 PM	0:07:38	Officer Burton transmitted that Cruz was "...last seen in the three-story building, north parking lot."

2:29:47 PM	0:08:09	Cruz joined in with a large group of students who were fleeing west towards Westglades Middle School.
2:32:42 PM	0:11:04	The first responding law enforcement officers entered building 12 through the west doors. These were four officers with CSPD and there were BSO deputies just outside the door.
2:42:22 PM	0:20:44	Sergeant Sklar asked over the radio "Who is out with an administrator that has access to the camera system and the school?" Sgt. Miller responded "Peterson would be the one that would have access to where the cameras are." Dispatch then asked "Does anyone know where Peterson is?" There was no response by Peterson. Peterson was still hiding at the northeast corner of building 7.
2:50:40 PM	0:29:02	Sergeant Rossman (BSO) and Officer Best (CSPD) transmitted over their respective radios that Cruz was last seen on the second floor.
2:52:39 PM	0:31:01	A group of law enforcement officers led by Sergeant T. Garcia (BSO-SWAT) reached the second-floor landing on the west side of building 12 still believing that Cruz was in the building.
2:54:32 PM	0:32:54	Sergeant Rossman (BSO) broadcasted that Cruz moved from the third floor to the second floor as if that was occurring in real time. Shortly thereafter, Captain Mock (CSPD) broadcasted the same information over the CSPD radio.

3:00:22 PM	0:38:44	Captain R. Gallagher (CSPD) broadcasted over the CSPD radio channel that the video was on a delay.
3:02:20 PM	0:40:42	Sergeant Rossman (BSO) broadcasted over the BSO radio channel that the school surveillance video is on a delay and that Cruz fled building 12 approximately 20 minutes earlier.
3:17:45 PM	0:56:07	All classrooms in building 12 had been accessed by law enforcement.
3:37:45 PM	1:16:07	Cruz was detained by Officer M. Leonard of the Coconut Creek Police Department approximately two miles southwest of the MSD campus.

The timeline described in the report revealed the challenges faced by law enforcement in trying to pinpoint the location of the perpetrator, even after the perpetrator vacated building 12 and left the campus. Video was not immediately accessible or utilized. At 2:42:22 PM, Sergeant Sklar first inquired about getting access to the camera system, approximately 12 minutes after the suspect left the campus. At 2:50:40 PM, Sergeant Rossman starting broadcasting location information obtained indirectly through Assistant Principal Porter approximately 8 minutes after the first call for video. The problem with video data was compounded even more because it was on delay. This didn't get communicated to responders until approximately 9 -11 minutes, after the first broadcast of the suspect location, when Captain Gallagher broadcasted over the CSPD radio at 3:00:21 PM and Sergeant Rossman broadcasted over the BSO radio at 3:02:20 PM.

The MDS-PSC report also concluded that had the Broward County Public School system given authorization to law enforcement for direct access to the camera system, locating the perpetrator and victim rescue efforts would not have been hampered. They stated, "The Broward County Public School's decision not to allow law enforcement live and real time direct access to the school camera systems in Broward County, including the system at MSDHS, adversely affected law enforcement efforts to locate Cruz and it hampered victim rescue efforts."

Appendix B 5G DEEP DIVE

B.1 3GPP 5G SYSTEM ARCHITECTURE:

The 3GPP Technical Specification (TS) 23.501 is the specification that defines the system architecture for the 5G System (5GS) (Reference [10]). At its core, the architecture is designed to support data connectivity and services. However, it is a paradigm shift from previous generations as it moves away from a "one size fits all" mobile communications solution to a model that supports and optimizes per use case, per traffic load, per service, etc. To achieve this vision and meet the requirements and 5G KPIs of the IMT 2020 and beyond, the architecture requires specific technology enablers and characteristics (Reference [7] and Reference [36]).

The 5GSA is defined by the following characteristics:

- User Plane and Control Plane separation, modular and more flexible design
- Supports procedures defined for network function services and re-use
- Supports network functions that can interact directly and indirectly through other network functions
- Supports minimized dependencies between the access network and the core network
- Supports a unified authentication framework
- Supports "stateless" NFs where the "compute" resource is decoupled from the "storage" resource
- Supports capability exposure outside the network
- Supports concurrent access to local and centralized services for low latency
- Supports access to local data networks also known as edge computing
- Supports roaming with both home routed traffic as well as local breakout traffic in the visited PLMN

The 5GSA has three main designs defined in TS23.501. In TS 23.501 clause 4.2.2. It is broken down into the non-roaming case and roaming case which has two variants. The non-roaming system architecture, illustrated in Figure 45 includes a home PLMN that operates directly with its own components and does not interact with other visitor PLMN user or control plane functions. In the roaming case, there are two variants 1) Local Break-Out (LBO) and 2) home routed. In the LBO case, shown in Figure 46, there is control plane connectivity only between a visiting network and a home network over the N32 interface. The control planes of the visiting and home network safely interact and pass messages through their own Security Edge Protection Proxy (SEPP). The SMF and all UPF(s) involved by the PDU Session are under control of the Visited Public Land Mobile Network (VPLMN). In the home routed case, shown in Figure 47, a visiting network and home network have interactions between network functions in the control plane and in the user plane. The control planes interact through SEPP similar to the LBO case, however, the user plane can also interact between the visitor and home network either directly over the N9 interfaces. The home routed case supports a PDU Session supported by an SMF controlled by the Home Public Land Mobile Network (HPLMN), an SMF controlled by the VPLMN, at least one UPF controlled by the HPLMN SMF, and at least one UPF controlled by the VPLMN SMF.

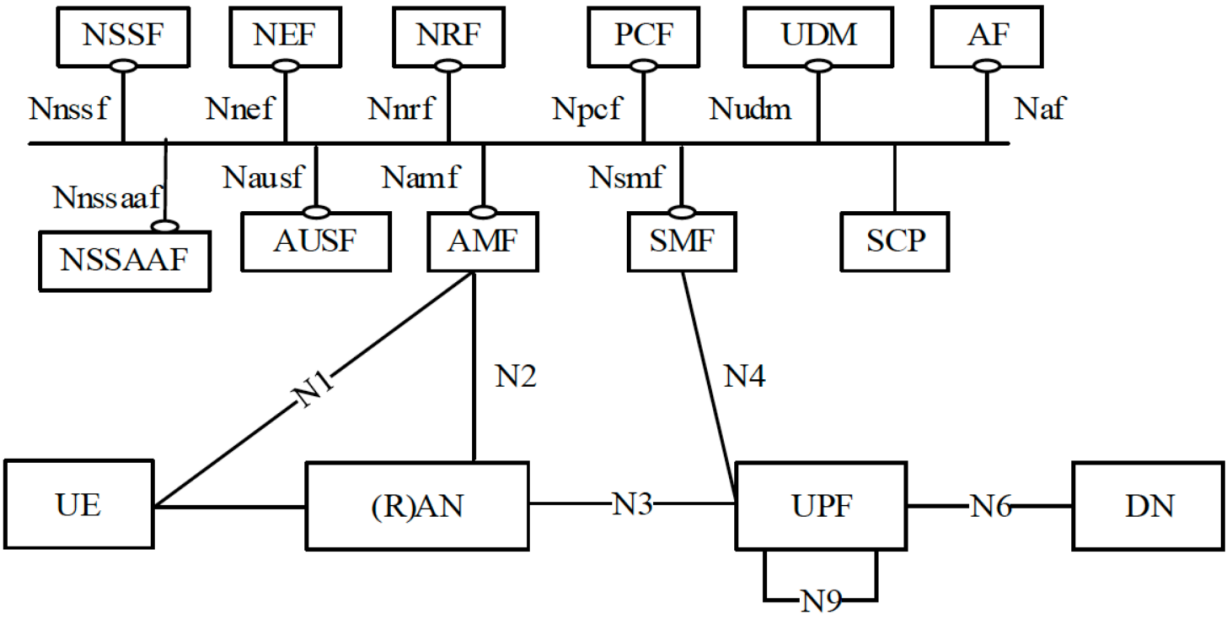


Figure 45 – 5G System Architecture Non-Roaming Case (Reference [10])

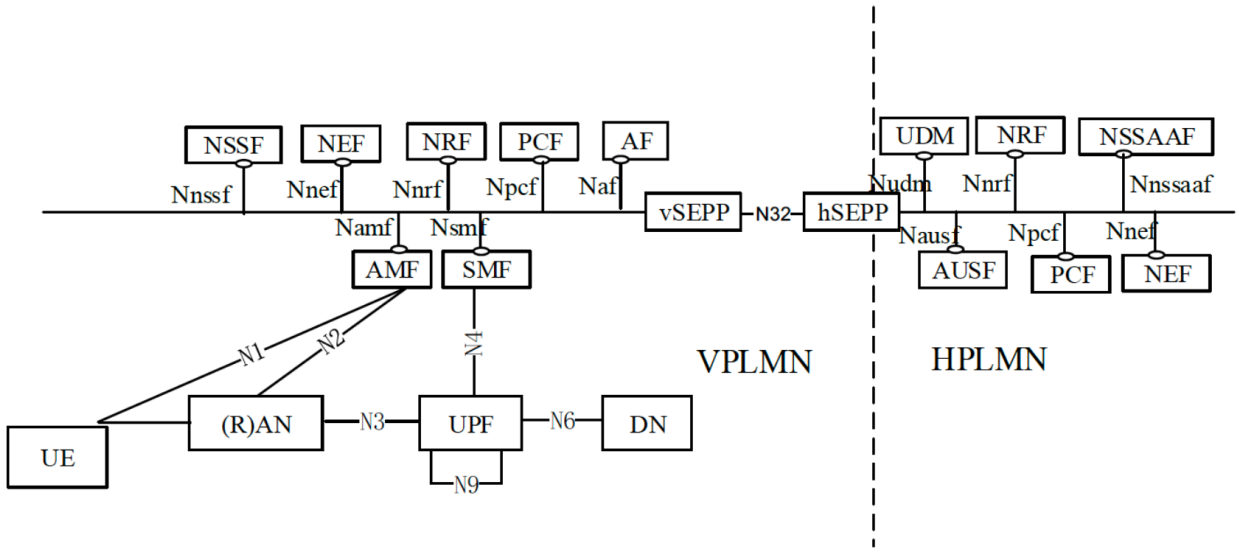


Figure 46 – 5G System Architecture Roaming Local Break-out (LBO) Case (Reference [10])

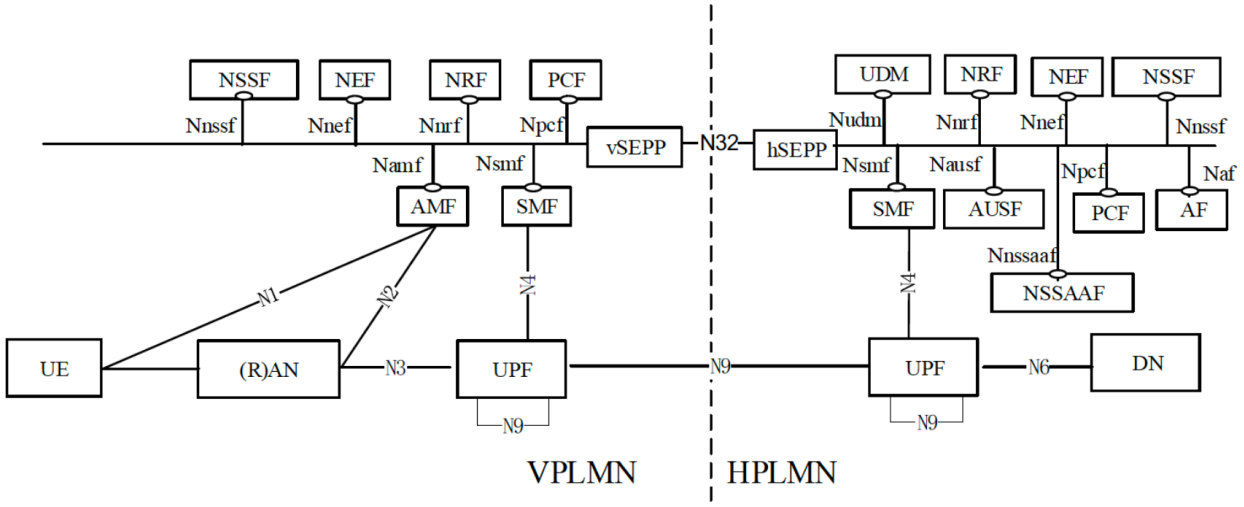


Figure 47 – 5G System Architecture Roaming Home Routed Case (Reference [10])

B.2 3GPP 5G NETWORK FUNCTIONS

In TS23.501 clause 4.2.2, the specification lists 26 network functions in total within the 5GSA. The list only grows when accounting for security functions and as new independent functions are developed.

B.2.1 USER PLANE NFS

Starting with the user plane of the 5GSA, there are 4 network functions, shown in Table 9, which include the UE, the RAN, the UPF and the DN. A brief summary of each network function in this diagram and their functionality will be provided to give context on their key roles within the system.

Table 9 – 3GPP Non-roaming 5G Architecture User Plane Network Function Acronyms

User Plane Network Function Acronym	User Plane Network Function
UE	User Equipment
RAN	Radio Access Network
UPF	User Plane Function
DN	Data Network

The UE is the mobile device that contains the Universal Subscriber Identity Module (USIM) which contains the Subscriber Permanent Identifier (SUPI). This ID identifies the subscriber and is used to authenticate and authorize a mobile device requesting access to the 5G network. The UE is where data and services are requested and consumed once it is authenticated and authorized. The future of 5G has the UE not only representing cellular devices, but also including vehicles, IoT devices and sensors, etc. The UE has control plane connectivity to the AMF, also known as the N1 interface, with control messages being forwarded over the wireless interface of the RAN and forwarded to the AMF. It also has standard 3GPP access to the network wirelessly to the RAN via the Uu-interface for user plane data.

The RAN is the cellular tower or base station, eNB or gNB, providing standard 3GPP access to the desired data and services for UEs after proper authentication and authorization. The RAN has wireless connectivity to the UEs it serves providing uplink and downlink user plane and control plane data. The

RAN also has connectivity to the AMF for forwarding control plane specific messages to the 5G CN or forwarding control messages to the UE. The RAN also forwards data in the user plane to the UPFs. This interface is known as the N3.

The UPF's primary purpose is to steer traffic, enforce QoS policies and filter traffic to and from the intended UE and DN. There can be multiple UPFs within the user plane and so the N9 interface is used for communication, steering and routing between UPFs. The UPF has connectivity to the RAN to forward user plane data over the N3 for uplink or downlink. It also has an N6 interface which is the interface where data officially leaves the 5GSA and moves externally to a DN. The N4 is the management interface where the SMF manages and deploys UPFs as well as monitors performance of the UPFs. The UPF serves as the anchor point for intra/inter RAN mobility.

The DN can be thought of as a general term for the application services, servers and data that a user requests. The 5GSA provides connectivity to DNs, but DNs are external entities from the 5GSA. 5GSA simply provides connectivity to a specific DN, a defined Quality of Service (QoS), and the mechanism for charging all based on a subscriber's subscription data.

B.2.2 CONTROL PLANE NFS

The control plane contains 11 network functions within the non-roaming 5GSA diagram, shown in Table 10. Following the SBA design, each NF has its own SBI for interactions between other control plane NFs. Only the AMF and the SMF in the control plane are shown having additional reference point connectivity to NFs in the user plane.

Table 10 – 3GPP Non-roaming 5G Architecture Control Network Function Acronyms

Control Plane Network Function Acronym	Control Plane Network Function
AMF	Access and Mobility Management Function
SMF	Session Management Function
PCF	Policy Control Function
AUSF	Authentication Server Function
NEF	Network Exposure Function
NRF	Network Repository Function
UDM	Unified Data Management
NSSF	Network Slice Selection Function
NSSAAF	Network Slice Specific Authentication and Authorization Function
SCP	Service Communication Proxy
AF	Application Function

The AMF's main role is to manage registration, connection, reachability, and mobility for UE's subscribed to the network. It supports access authentication and authorization and passing along session management messages to the SMF. It serves as the gateway between the control plane and the UE for control plane signaling as all control plane messages from the UE will travel over the RAN and to the AMF. It is the termination point for the RAN control plane interface and the Non-Access Stratum (NAS) and NAS ciphering and integrity protection. It also supports the security anchor functionality which supports the authentication procedure.

The SMF's main role is to perform session management such as session establishment, modification, and release. It is also responsible for maintaining the tunnels between the UPF and the AN node. It deploys the user plane configuration defined by the PCF such as UE IP address allocation and management and traffic steering and routing to the proper destination. It is also in charge of charging data collection and charging interfaces.

The PCF's main role supports a unified policy framework to govern network behavior and adhering to the software defined networking framework. It provides policy rules to control planes which are then enforced. It also accesses subscription information for policy related decisions from the Unified Data Repository (UDR).

The AUSF is a network function that is completely security related. It supports the UE authentication service requested by a NF which is typically the AMF. It supports authentication for 3GPP access, and non-3GPP access.

The NEF supports secure exposure of capabilities and events to 3rd parties, AFs, and edge computing. It also supports provisioning of information from external applications to the 3GPP network.

The NRF supports service discovery by receiving discovery requests from NF instances or from the SCP. It then provides the information of the discovered instances to the NF instance or SCP.

The UDM supports generating the 3GPP Authentication Key Agreement (AKA) credentials, user identification handling such as the storage and management of the SUPI, supports deconcealment of the Subscription Concealed Identifier (SUCI), and supports storing UE serving NF registration management. It lastly serves and access the information stored in a UDR located in the same PLMN.

The NSSF supports the functionality of selecting the set of network slices serving a UE. It also supports identifying the allowed and configured NSSAIs and if needed the mapping to the subscribed S-NSSAIs. It can also support determining the AMF set that will be used to serve the UE.

The NSSAAF supports specific authentication and authorization required by specific network slices.

The SCP provides indirect communication between NFs and message forwarding and routing to a next hop SCP.

The AF interacts with the 3GPP network in order to provide services (e.g. influencing traffic routing, accessing the NEF or IP Multimedia System (IMS), and interacting with the policy framework for policy control). Based on operator deployment, trusted AFs could interact directly with the NFs while non-trusted AFs would interact with the NEF which would serve as an intermediary between communication with the other NFs. The AF is the control plane portion of applications that can be found in a DN. In the user plane, the DN serves the ingress and egress user plane data whereas the AF is used to influence the way the traffic is arriving to the DN.

B.2.3 NF SERVICES

A service within a 5G SBA is an atomized capability that can be characterized as highly cohesive, loosely coupled, and supporting independent management from other services. This enables these services to be updated independently with minimal impact to other services and deployed on demand. A service will

produce expected outputs based on expected inputs based on operator and service provider requirements. A service is deployed based on the service framework including three main procedures:

1. service registration
2. service authorization
3. service discovery

A service is invoked through a specific interface, for example, an Application Programming Interface (API). Within the 3GPP 5GS control plane, NF services comprise the SBA architecture and each have their own SBI.

The service framework as mentioned starts with service registration. Each service is implemented based on a service registry which holds the information of services such as service status and availability and their reachability such as the name and address where they can be located. A service is activated when registered with the service registry and inactive when it deregisters. The Network Repository Function (NRF) serves as the service registry in a 5GS. Service consumers like other NFs in the network can query the service registry for the information it holds such as available services and where they can be found. The second concept in the service framework is service authorization which controls whether a service can be invoked or accessed by other services. With the concept of openness being enabled for a 5GS, service authorization and even authentication will be needed for external parties attempting to access 5GS information however, service authorization may not be needed for NFs requested access to service that are within the trusted domain. Lastly, service discovery is a process where a consumer queries for a service in the service registry and the service registry replies with the available services and their address. Load balancing can be performed with service discovery and can affect the shown available services.

B.3 3GPP 5GSA'S SUPPORT FOR EDGE COMPUTING

TS23.501 details how the 5GSA supports edge computing in general. The 5GSA defines edge computing as a feature of the network that supports operator and 3rd party services to be close to the UE's access of attachment. This access of attachment can be 3GPP access, like the RAN, or non-3GPP access, like a Wi-Fi access point. Edge computing's benefit achieves efficient service delivery through reduced end-to-end latency and load on the transport network, specifically the backhaul to the central cloud core network. Edge computing typically applies to the non-roaming and LBO roaming architecture cases only. The specification does not specify why it does not support home routed roaming. The specification details the following enablers or features of the 5G architecture that support edge computing:

- User Plane (re)selection
- Local Routing and Traffic Steering
- Session and Service Continuity
- Application Function (AF) Influence
- Network Capability Exposure
- QoS and Charging
- Support of Local Area Data Network

User Plane (re)selection is the feature of the 5G CN having the role of managing, deploying and selecting or reselecting the UPF which will route traffic to data networks, specifically to the local data network for edge computing. The 5G Core network refers specifically to the SMF which deploys, manages and selects a UPF for a particular PDU session. The SMF pulls the configuration settings from the PCF which will provide the policy data for subscribers and should detail for a particular application the local data network UPFs should route to for edge computing.

Local routing and traffic steering is tied with the user plane (re)selection enabler. The 5G core network can route specific traffic to applications hosted in the local data network. This is performed by the configurations, filtering and routing set within the UE, the RAN, the UPFs and the DNs. It starts with the configuration set in the core network and pushing these filters and rules to the entities required to route the data to the desired local data network.

Session and Service Continuity (SSC) refers to the required setting chosen by a network or requested by a user for PDU sessions or data sessions that are established between a UE and a DN. This setting can't be changed for the lifetime of the PDU session. The support of session and service continuity in the 5GSA provides the ability to accommodate various continuity requirements for services and applications for a UE. It supports when UEs are moving throughout a network or the application is moving throughout the network. The three possible SSC modes are Mode 1, Mode 2 and Mode 3. In Mode 1, the network preserves continuity service provided to the UE, for instance, the IPv4, IPv6 or IPv4v6 IP address is preserved for the PDU session. Mode 2 allows the network to release the connectivity service to the UE and release the PDU Session. For the IPv4, IPv6, and IPv4v6 case, the IP addresses allocated to a UE are also release as a result of the release of the PDU Session. Mode 3 provides the UE transparency of the changes occurring in the user plane and ensures no loss of connectivity for the UE. Mode 3 mainly provides a soft release as it will make a new connection or PDU Session with an associated IP address before it releases the current PDU session losing the current IP address.

AF influence refers to an AF having the ability to obtain information and communicate with the 5G core network control plane either directly communicating with the PCF as a trusted entity or through the NEF as an untrusted entity. The AF may request to the PCF to route specific traffic based on a subscriber's policy or geographic location. The PCF, if the request is accepted, may create policies which the SMF may be alerted and pull the new policy information, as well as configure and deploy. The AF may even have the ability to request the selection or reselection of an application or even relocate the application. In the case of MEC, the MEC can influence the 5G core network to route traffic to the local data network instead of reaching back to the central cloud. It could also request to select or reselect specific UPFs for traffic routing. It may even request the application which may originally reside in the central cloud to relocate and push an application instance into the MEC environment in the local data network.

Network capability exposure refers to the openness feature of the 5GSA. The 5GSA will allow trusted entities like NFs to communicate directly with and receive information from NFs within the 5GSA. If the entities is untrusted, then the untrusted AF or entity can still communicate and receive information from the 5GSA, however, through a proxy which is the NEF.

QoS and charging refers to the ability for the 5GSA to configure rules in the PCF that will provide directions for traffic routed to the local data network.

Support for Local Area Data Networks (LADN) is the term given to the feature of a 5GSA to support access to a specific DN via a PDU Session based on a specific service area location. It requires 3GPP access only and only the non-roaming and roaming LBO cases. This is a service provided by the serving PLMN.

In order to support selective traffic routing to a DN which is key to edge computing, the 5GSA must support single PDU Sessions with multiple PDU Session Anchors. This feature enables an SMF to control the data path of a PDU Session so that the PDU Session may simultaneously correspond to multiple N6 interfaces. The UPFs that terminate multiple N6 interfaces are called PDU Session Anchors (PSA). The PSAs provide different access to the same DN within a PDU Session. A PSA is assigned at PDU session Establishment and associates with an SSC mode. Additional PSAs can be added to a PDU Session. When a Policy Control and Charging (PCC) rule is provided to the SMF like the AF influence traffic steering enforcement control information, the SMF can decide whether to apply traffic steering based on the Data Network Assistance Information (DNAI), which are DN IDs, within the PCC rule request. The AF influence traffic steering enforcement control information would come from the PCF. The PCF would have received it directly from the AF or from the AF through the NEF. If traffic steering was applied it can implement two methods which is either Uplink Classifier functionality or IPv6 multihoming.

B.3.1 USAGE OF UPLINK CLASSIFIER

The usage of Uplink Classifier (UL CL) functionality for single PDU Sessions with multiple anchors relates to sessions that are of type IPv4, IPv6, IPv4v6 and Ethernet. The SMF may decide to insert or remove a UPF, known as an UL CL, within the data path of a PDU Session. This is illustrated in Figure 48. The UE is unaware of the traffic diversion by the UL CL and is not involved in the insertion or removal. The UE associates the PDU Session with a single IPv4 address, single IPv6 Prefix or both. When a UL CL is inserted in the data path of a PDU session, there will be multiple PSAs that provide access to the same DN. The mechanism for packet forwarding on the N6 reference point interface between the PSAs providing local access and the DN are outside the scope of TS23.501.

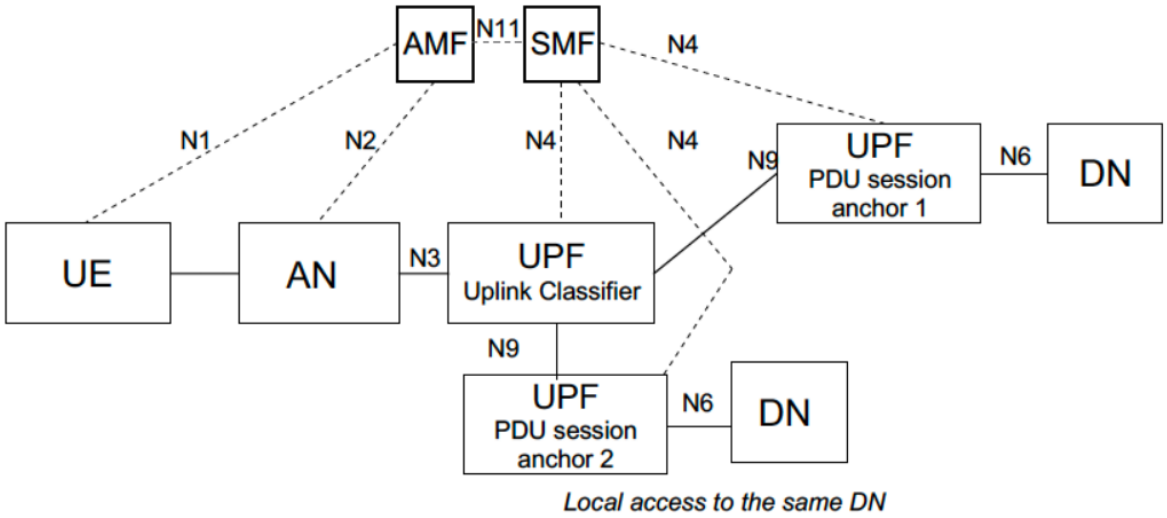


Figure 48 –User plane Architecture for the Uplink Classifier (Reference [10])

The UL CL provides forwarding of UL traffic towards different PSAs and merging of DL traffic to the UE. This traffic merging and forwarding are all based on traffic detection and forwarding rules provided by the SMF. The UL CL provides filtering rules such as examining the destination IP address and prefix of uplink IP packets sent by the UE and determines how packets should be routed. This functionality may also provide additional features such as traffic measurement for charging, traffic replication for lawful intercept, and bit-rate enforcement. Additional UL CLs can be added to the data path and it is up to the operator to organize and manage and the SMF logic that comes with the additional complexity. However, there will be only one UL CL UPF that connects to the RAN on the N3 interface unless UL CL relocation is occurring.

A PDU Session may be associated with multiple IPv6 Prefixes, referred to IPv6 multihoming, and illustrated in Figure 49 and Figure 50. The multi-homed PDU session provides access to a Data Network via more than one PSA. The different user plane paths leading to different PSAs branch out at a "common" UPF which is called a "Branching Point" UPF. Branching Point functionality provides forwarding of UL traffic towards different PSAs and merging of DL traffic towards the UE from different PSAs.

Similar to the UL CL functionality, the Branching Point functionality provides the same capabilities. It is managed by the SMF as the SMF decides when to insert or remove it from the user plane. It supports traffic measurement for charging, traffic replication for lawful intercept, and bit rate enforcement. It can be inserted during or after the PDU session establishment and can also be removed after this process. The difference for this method is it's only supported for PDU Sessions of type IPv6 and therefore only supports type IPv4v6 and IPv6. When a UE requests for a PDU Session of type IPv4v6 or IPv6, it also provides an indication on whether or not it can support IPv6 multihoming. A multihoming PDU session will use multiple IPv6 prefixes by configuring through the SMF the ability to spread traffic to specific PSAs based on the source prefix. The UE may have the ability to select the source prefix based on routing information and preferences received from the network. Other features multihoming may support is make-before-break continuity which is the soft release SSC mode 3. See the figures below showing a visual depiction of IPv6 multihoming and support of SSC mode 3.

B.3.2 USAGE OF IPV6 MULTIHOMING

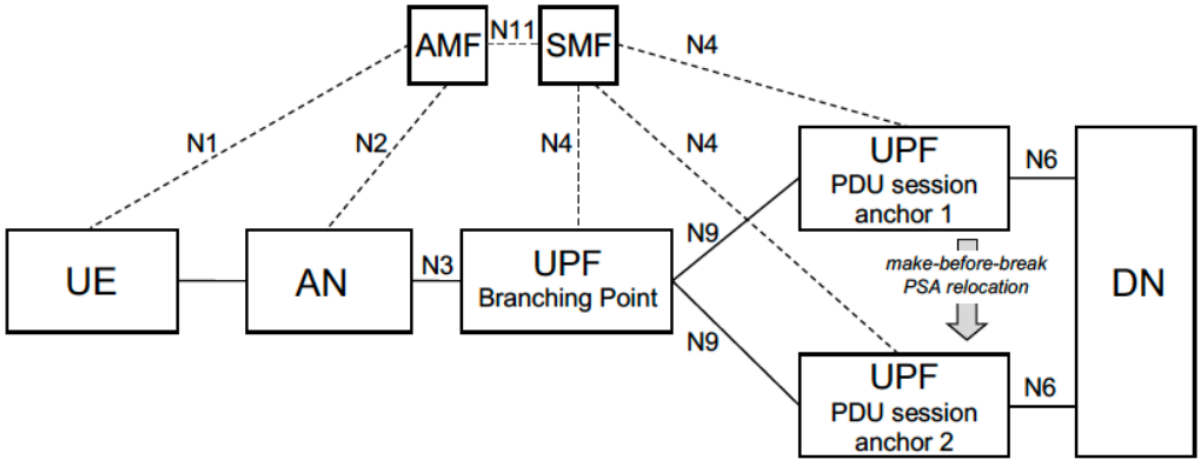


Figure 49 – Multi-homed PDU Session: service continuity case (Reference [10])

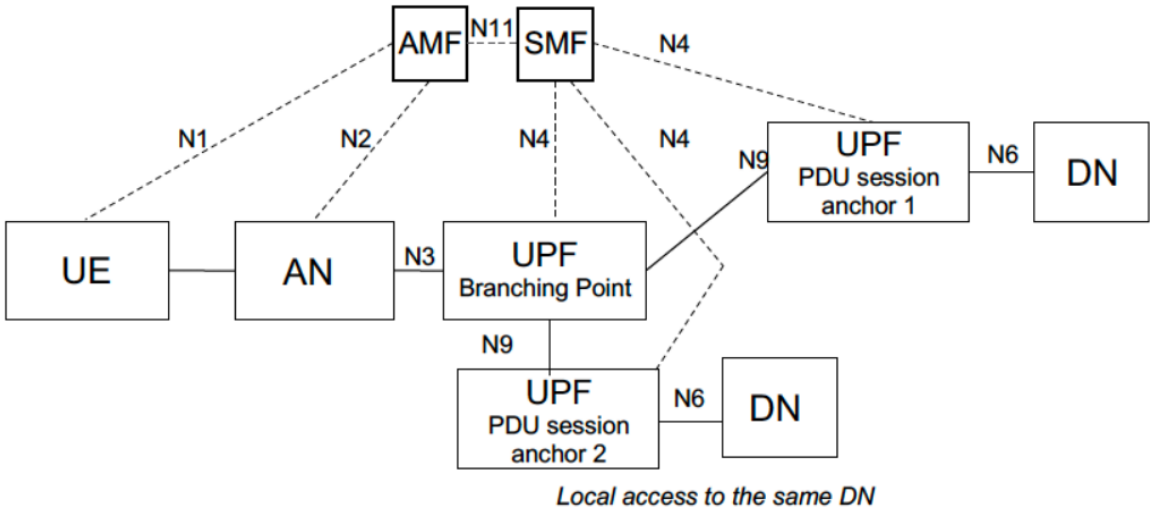


Figure 50 – Multi-homed PDU Session: local access to same DN (Reference [10])

Local routing and traffic steering is an important enabler for 5G MEC. Two specific methods to deploy local routing and traffic steering is through uplink classifier functionality and IPv6 multihoming functionality. These two techniques will support the success of edge computing allowing single PDU sessions to have PSAs anchored at the local access data network where traffic can be routed versus the central cloud.

B.3.3 Network Capability Exposure

The 5G SBA provides openness which is a major key characteristic difference from previous generations. Openness enables third parties applications and services the ability to communicate with the 5G core network control plane and obtain information related to the system. TS23.501 Clause 5.20 provides details on the 5G system's ability to expose network capabilities.

The Network Exposure Function (NEF) serves as the proxy for external exposure of capabilities of network functions. Such capability exposure includes the following:

- Monitoring capability
- Provisioning capability
- Policy/Charging capability
- Analytics reporting capability

The Monitoring capability is for monitoring of specific events of a UE in 5GS. The Provisioning capability is for allowing external parties to provision information which can be used for the UE in 5GS. The Policy/Charging capability is for handling QoS and charging policy for the UE based on the request from an external party. The Analytics reporting capability is for allowing an external party to fetch or subscribe and unsubscribe to analytics information generated by 5GS.

B.3.4 Application Function Influence on Traffic Routing

TS23.501 Clause 5.6.7 details application function influence on traffic routing functionality. It refers to the non-roaming or roaming LBO architecture. This functionality involves the PCF, AF, SMF, and the UPF as

the main entities. It requires they belong to the serving PLMN or the AF belongs to a third party with an agreement with the serving PLMN. It is explicitly not supported for the roaming home routed case. The core capability here is the ability for the AF to request to influence SMF routing decisions for traffic of a PDU Session. The AF request may influence UPF (re)selection and allow routing traffic to a local access data network identified by a DNAI. The AF may serve as a proxy to send requests to influence routing by applications that are third party and not owned by the serving PLMN. If an AF is untrusted and cannot communicate requests directly, than the AF communicates with the NEF to get a request through to the 5GSA. The PCF will transform accepted AF requests into policies that apply to PDU Sessions. A table of what a request will consist of can be seen below in Table 11.

Table 11 – Information Contained in AF Request

Information Name	Applicable for PCF or NEF (NOTE 1)	Applicable for NEF only	Category
Traffic Description	Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information.	The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI.	Mandatory
Potential Locations of Applications	Indicates potential locations of applications, represented by a list of DNAI(s).	The potential locations of applications can be represented by AF-Service-Identifier.	Conditional (NOTE 2)
Target UE Identifier(s)	Indicates the UE(s) that the request is targeting, i.e. an individual UE, a group of UE represented by Internal Group Identifier (NOTE3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s).	GPSI can be applied to identify the individual UE, or External Group Identifier can be applied to identify a group of UE.	Mandatory
Spatial Validity Condition	Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity.	The specified location can be represented by a list of geographic zone identifier(s).	Optional
AF transaction identifier	The AF transaction identifier refers to the AF request.	N/A	Mandatory
N6 Traffic Routing requirements	Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation.	N/A	Optional (NOTE 2)
Application Relocation Possibility	Indicates whether an application can be relocated once a location of the application is selected by the 5GC.	N/A	Optional
UE IP address preservation indication	Indicates UE IP address should be preserved.	N/A	Optional
Temporal Validity Condition	Time interval(s) or duration(s).	N/A	Optional
Information on AF subscription to corresponding SMF events	Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription.	N/A	Optional
NOTE 1: When the AF request targets existing of future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR. NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only. NOTE 3: Internal Group ID can only be used by an AF controlled by the operator.			

B.4 3GPP NON-3GPP NETWORKS

TS23.501 describes the following types of non-3GPP access:

- trusted non-3gpp access
- untrusted non-3gpp access
- wireline access

Trusted non-3GPP access refers to access types that can directly interact with the 5G System and can be seen in Figure 51. Untrusted access refers to access types that are not inherently trusted and so require to interact with the 5G System through an interworking function as seen in Figure 52. Wireline access refers to access to the 5G network that is not wireless but wired. Figure 53 and Figure 54 refer to two types of wireline access. The first is a 5G Residential Gateway (5G RG) that can wirelessly connect to a gNB for control plane messaging while simultaneously sending data over a wired line to the 5G network. The second type is a Fixed Network Residential Gateway (FN-RG) where there is no wireless capability to a gNB and so N1 control plane messaging as well as user data are all communicated over the wire.

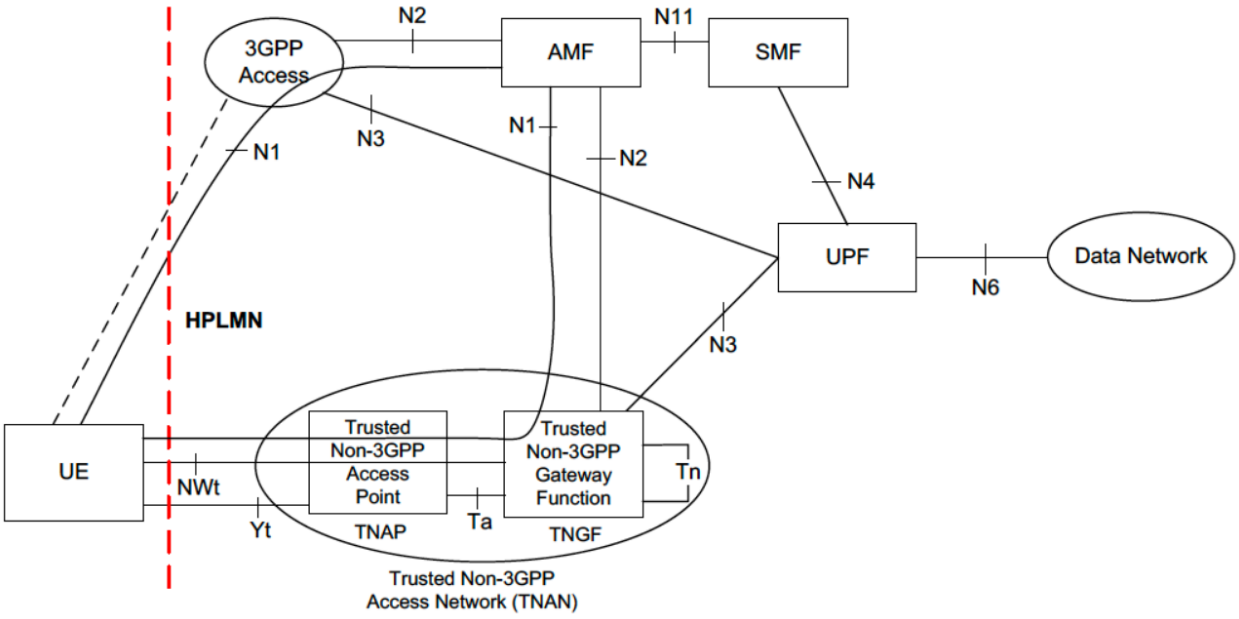


Figure 51 – Non-roaming architecture for 5G Core Network with trusted non-3GPP access (Reference [10])

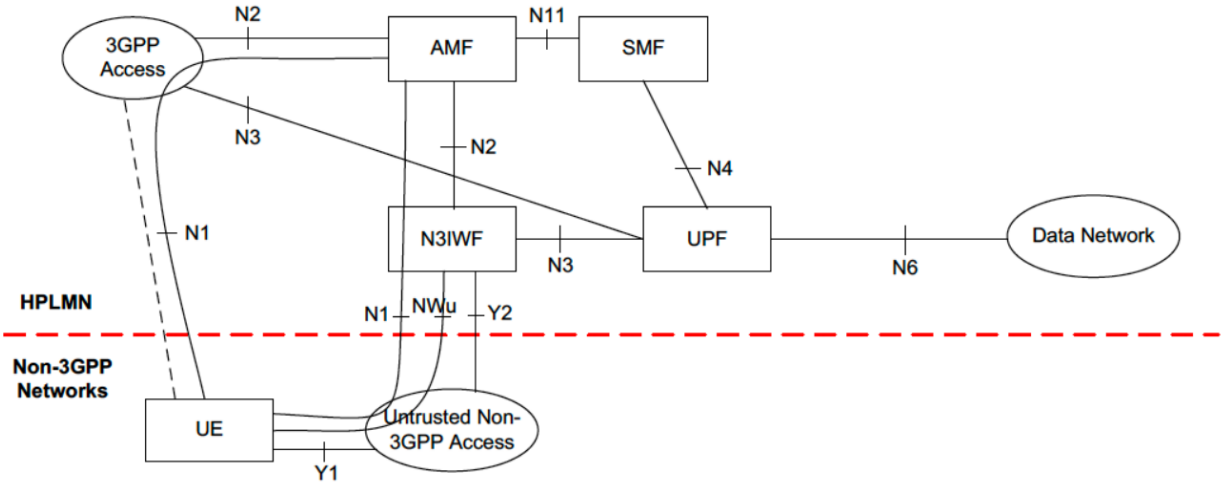


Figure 52 – Non-roaming architecture for 5G Core Network with untrusted non-3GPP access (Reference [10])

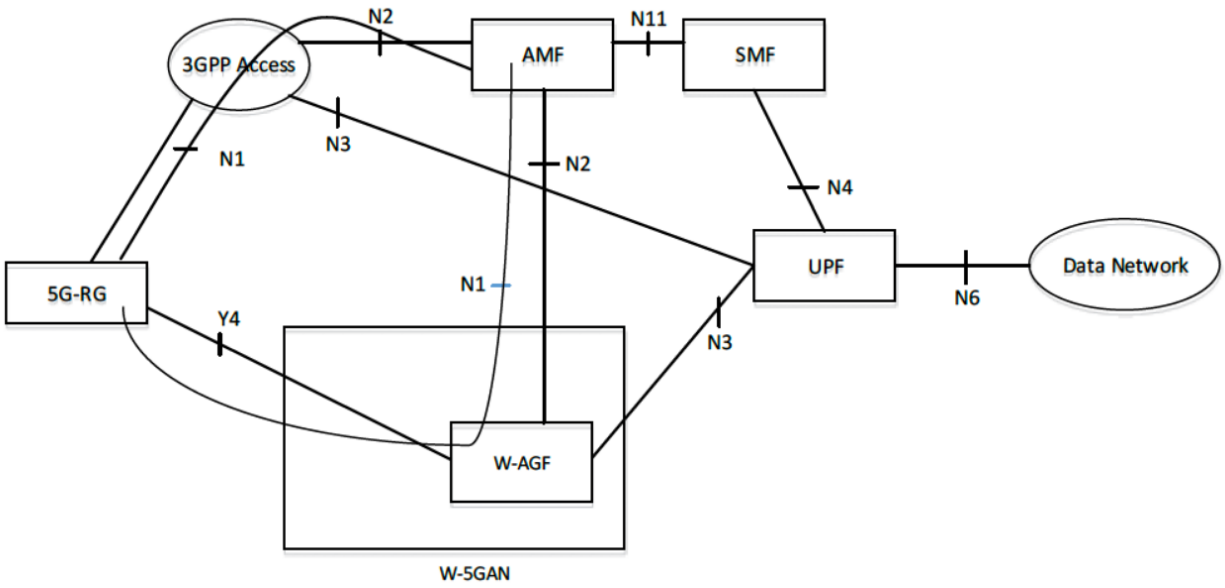


Figure 53 – Non- roaming architecture for 5G Core Network for 5G-RG with Wireline 5G Access network and NG RAN (Reference [10])

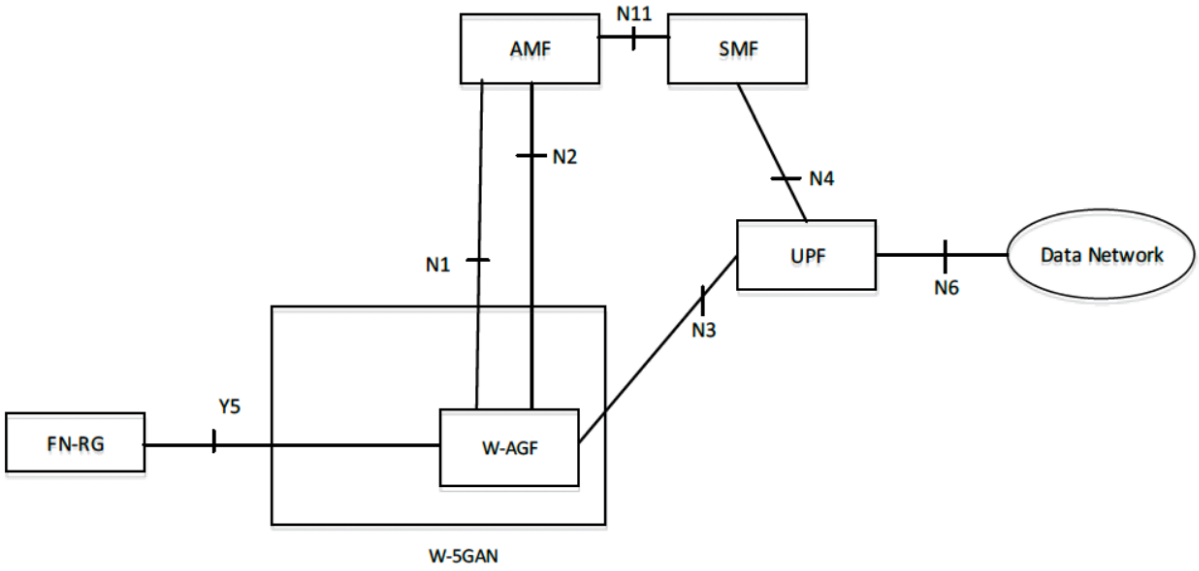


Figure 54 – Non- roaming architecture for 5G Core Network for FN-RG with Wireline 5G Access network (Reference [10])