GTI LTE, 5G NR Private Networks WHITE PAPER V1.0

GTI

http://www.gtigroup.org

LTE, 5G NR Private Networks

WHITE PAPER

Global TD-LTE Initiative

Version:	1.0
Deliverable Type	□ Procedural Document √ Working Document
Confidential Level	√ Open to GTI Operator Members √ Open to GTI Partners □ Open to Public
Working Group	Business & Services, Network WG
Task Force	Private Networks Task Force
Contributors	Reliance Jio, Sprint, AreteM, Qualcomm
Editors	Satish Jamadagni, Kathleen Leach, P S Tang
Last Edit Date	01-06-2019
Approval Date	DD-MM-YYYY

Document History

Date	Meeting #	Version #	Revision Contents
22-06-2018		0.1	First draft version
07-01-2019		0.2	Editorial
30-01-2019		0.3	Added CBRS Use Case
11-05-2019		1.0	Final Draft for circulation

Contents

Executive Summary

This white paper provides a technical overview on the LTE and 5G NR “Private Networks” opportunity. The paper discusses gaps in standards that may still hinder the development of private networks, possible deployment issues and ways to enable LTE and 5G NR “private wireless networks”.

Key factors that are enabling “Private Networks” are the following:

1. The increasing need for enterprise data sovereignty / data locality, security, local sensor networks and industry specific applications.
2. The flexibility that 4G and 5G technologies bring to existing enterprise/vertical use case scenarios such as high speeds, low latencies, enhanced reliability and lower power consumption.
3. Emerging new network management possibilities that could enable a single physical network to support a number of virtual networks with different performance characteristics, referred to as “network slicing”, it creates the possibility of tailoring services to the particular characteristics of specific devices/users.

This ability to support different services with or without having to build new / different physical networks gives raise to the possibility of new services targeted at new sectors (also referred to as industry verticals) like industrial sector, services sectors and at specific user groups. These networks addressing specific industry verticals and called as “Private networks” have the potential to create new business models benefiting all concerned, from network operators, end industry segments, intermediaries etc. The current marketplace has been mainly limited to varying pricing plans for services and differentiation.

These solutions address issues of security, data locality, in-house control over production reliability, multi-service capability and enterprise data sovereignty makes it possible for private organizations to realize on-premises private wireless networks, with or without requiring access to licensed spectrum.

Though “Private Networks” offers new opportunities and allows new business models to emerge, there are key interfaces between “Public” and “Private” networks that needs to be addressed. Work on such interfaces is ongoing in forums such as 3GPP, 5G-ACIA etc.

Terminology

Abbreviation	Explanation
3GPP	3rd Generation Partnership Project
CDN	Content Data Network
CSG	Closed Subscriber Group
CSGID	Closed Subscriber Group IDentifier
CBRS	Citizen Broadcast Radio Service
IMT	International Mobile Telecommunication
ITU	International Telecommunication Union
IMSI	International Mobile Subscriber Identifier
LIPA	Local IP Access
LTE	Long Term Evolution
LPGW	local PDN gateway
LAA	Licensed Assisted Access
LSA	Licensed Shared Access
MNO	Mobile Network Operator
NB-IOT	Narrow Band IOT
OAM	Operation, Administration and Maintenance
ODU	LTE outdoor CPE
PGW	Packet Gateway
PDN	Packet Data Network
QoS	Quality of Service
RAN	Radio Access Network
RRM	Radio Resource Management
SA-ID	Service Area ID
SIPTO	Selected IP traffic offload
SLA	Service Level Agreement
SAS	Spectrum Access System
SGW	Serving Gateway
TD-LTE	Time Division Long Term Evolution
TDD	Time Division Duplex
V2X	Vehicle to Everything

1. Industry Trends on Private Networks

1.1. Motivation:

As the number of connected devices and the data generated in enterprises increases, it is expected that organizations would want to control their own networking environment. This can help the enterprise to easily customize and/or optimize the network as well as monetise the enterprise data that is generated. The key motivators are the following:

- Coverage and capacity concerns in organizations: Enterprises can hope to better engineer the network to meet their specific performance needs, e.g., Specify uplink and downlink configuration as necessary, dictate access policies, determine specific user/device rights, traffic prioritization, etc.
- Deploy the network to meet specific challenging physical environments (e.g., warehouse or oil/gas facility with lots of metal). This can include robustness to recover from failure, implement for specific reliability and latency considerations which would be hard to ask for in a public network.
- Data security and control: Organizations can control the security of the data and ensure that sensitive information doesn't leave the premises; this is an essential requirement for many businesses nowadays. Companies can also hope to better use the generated data by controlling the type of analytics to run on the generated data.

With the emergence of “Host Neutral” small cells and shared/unlicensed spectrum access schemes, the use of private LTE and 5G networks in enterprise buildings, campuses and public venues is expected to grow significantly. In terms of spectrum, the new wave of private LTE deployments will be able to use the shared-access 3.5 GHz band in the US (i.e., Citizens Broadband Radio Service, or CBRS) and the 5 GHz unlicensed band globally (MulteFire as an example). Private LTE networks deployed in licensed spectrum using appropriate spectrum and network sharing mechanisms is an opportunity for existing operators.

Private networks offer predictable latency, necessary for many Internet of Things (IOT) applications. LTE or 5G Private networks can be designed for supporting large number of “enterprise or private” devices through small cells. Not only do LTE or 5G access points offer high data rates but, unlike Wi-Fi, these networks can also provide predictability and interference free access, critical for industrial scenarios, even when the small cell is shared by large number of users. LTE/5G private networks also provides over-the-air encryption, integrity protection and strong SIM based authentication. LTE/5G is power efficient, long device battery life can be factored into the configuration of the networks. Large enterprises

and campuses can be covered with a relatively low number of small cells, as an example the Citizen Band Radio Spectrum (CBRS) rules in the U.S. allow outdoor small cells to transmit at as high as 50W, sufficient to cover an area of a few kilometres. Small cells can also support Narrow Band IOT (NB-IOT) and or CAT M1 or any such 3GPP IOT variants as well.

LTE and/or 5G offers seamless mobility which means that enterprises that need mobility across the campus or a factory can leverage the LTE/5G networks for reliable connectivity throughout the building or campus. Public LTE / 5G network still makes sense for applications where enterprises want to access a wide-area mobile network. Private networks will have more benefits where the client device does not leave the enterprise campus.

1.2. Private Network - Use-Case Summary

With the deployment of enterprises private networks, restrictions from conventional connectivity technologies such as Ethernet is easily overcome. A Private network can support both human and machine communications on a single, reliable network offering mobility and supporting a host of Internet of Things (IoT) applications.

Private networks can serve well in a host of industry and service sectors ranging from farming, medical facilities, private enterprises, manufacturing sectors and traditional heavy industries like mining. Immediate and large scale impact is expected in the Industrial sector in what is also termed as Industry 4.0 covering automated manufacturing, supply chain management and warehousing. A summary is provide in the following.

Sl. No.	Use case type.	Description.
1	Automation and Industry 4.0	Wide scale adoption of robotics providing reconfigure production lines. Considerable advancements in Logistics and warehousing (adoption of pick-and-pack machines, IOT trackers etc). Bringing together Industrial IOT, Cloud, Big data and analytics into the industrial floor.
2	Mission-Critical Services.	- To monitor and control critical infrastructure - e.g., electricity distribution grids, power plants, etc., - Public safety agencies often need to creat closed user group ad hoc networks at the scene of emergency. - Government & military agencies want dedicated, highly available networks at their facilities.
3	Traditional Industries.	Enhancing traditional industries like mining to agriculture by providing remote conectivity and monitoring capabilities, making increasing use of automated machinery. Requires hardened equipment with good coverage and capacity
4	Local or Venue Services.	Adressing connectivity issues in Public venues such as airports, stadiums, hospitals, ports. These venues pose multi ownership issues such as venue ownsers, contractors, public institutions. The need for Private networks capable of catering to different user groups is essential.

Figure: Example use cases for Private Networks

1.2.1. Industrial IOT

The “Factories of the Future” will need technology that will enhance manufacturing productivity. Reliable connectivity is a critical requirement for Industry 4.0. The growth in data generation in enterprises and its significance to the overall process improvement concerns have forced enterprises to think more on analytics to achieve improved logistics, energy-management and so forth. Manufacturing companies are themselves becoming services companies, with various in-field business models related to their products. The changes will be brought about with on-site communications integrated with existing IT systems in enterprises.

Industrial IOT or just IOT application support has been shown to be a key concern in many private enterprises. Examples include trains and operational systems on railway networks, automated vehicles at an airport (eg baggage handling systems), construction machinery and sensors on a building site, various use-cases for smart cities and smart farms, such as automated transport systems or agricultural machinery. The critical systems running in these industry segments highlight the need and demand for LTE/5G private networks. It is unlikely that enterprises would want to use WiFi running in totally unlicensed and uncontrollable spectrum for these use cases. For IOT, the 3GPP specifications as of Release 15 also support the TDD version of NB-IOT enabling IOT along with possible enterprise broadband applications. 3GPP has also defined Ultra Reliable Low Latency communications for both LTE and 5G, which has the potential to address motion control and other demanding manufacturing applications.

An industry organization that is specifically focused on 5G applications in Industry 4.0 is the 5G Alliance for Connected Industries and Automation (5G-ACIA) [4], which includes representatives from manufacturing companies, mobile operators and wireless equipment suppliers. 5G-ACIA is focused on making sure that the specific needs and requirements of a particular vertical industry are adequately understood and considered by the telecom industry and, likewise, the capabilities of 5G are fully realized and exploited by the vertical industries.

1.2.2. Health Care

Healthcare segment is poised to have a significant amount of monitoring devices that are used in clinics, homes (elderly care) and hospitals. The need for private networks in hospitals comes from the fact that emergency response needs real-time response. Round the clock monitoring and analysis requires local data access and storage. High network availability and low response times (possibly with local breakouts) are expected to drive “Private Networks” in health care. Exchange of high resolution images/video files for immediate attention and tracking staff, patients and inventory on urgent basis on a public network would not be practical or recommended.

1.2.3. Industrial Plants

There are many industrial systems that are still connected to wires for want of better connectivity solutions. WiFi is not suited for the deterministic demands between process control computers and Programmable Logic Controllers (PLC) as timing is critical in a manufacturing ecosystem. Delayed actions or no action at all due to response time mismatch can disrupt system wide operations. As an example, welding robots used in an automobile assembly line operate in a synchronized manner, any communication delays between a robot and assembly line sensors can risk slowing down the assembly line or colliding with another robot that has had no delays. LTE/5G private networks can provide a reliable alternative to a wired scenario.

1.2.4. Transportation

With the emergence of V2X (Vehicle to Everything) there is an opportunity to enhance transportation hubs. Because of the security needs, transportation hubs are closed environments and the devices in use are both expensive and limited in function. LTE/5G private networks are critical in such scenarios which can cover large open indoor areas such as commercial jet hangers or outdoors such as areas that are away from the terminals/buildings. Private LTE/5G brings a closed system with a long signal reach that provides great coverage and unprecedented capacity.

Fright handling, baggage handling will need IoT. IOT helps in weather sensors (instrument the micro-climates across an airport), intrusion detection, Asset tracking, employee locators and other such aspects. These are best served more reliably by a private network. IoT is also expected to play a significant role in the turnaround time of aircrafts once they pull in at the gate. Such date from an aircraft's sensors and the personal responsible for "turnaround" time has to be on private networks.

1.2.5. Oil Exploration and production:

Many of the use cases explored in prior vertical markets are similar for exploration and production (E&P) and also refining. Some of these are PLC for sensors, instrumentation, control, and surveillance. The obvious benefits of Private LTE are greatly amplified in this market. The difference in E&P platforms and Refineries is the harsh physical environment and presence of explosive gases. The cost of running low voltage cabling in rated conduits and providing equipment either "intrinsically safe" or installed in a compliant enclosure is high.

1.3. Private Network – Requirements Summary

This section summarizes the key requirements for private networks.

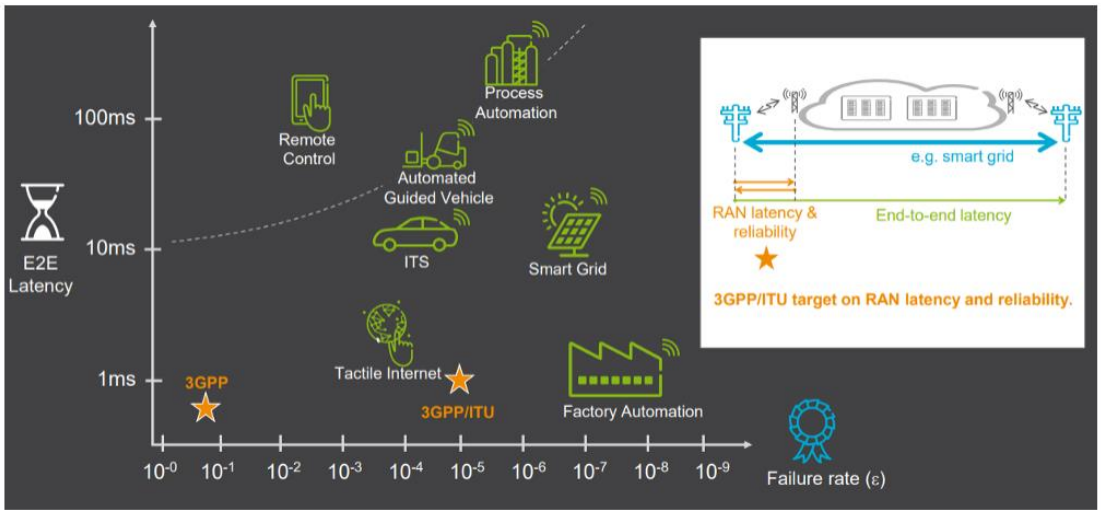
1.3.1. Network Service requirements

The below is a summary of the Network service requirements.

Latency and Reliability:

The target of very low latency combined with high reliability of LTE / 5G will enable many applications to be realized over these networks. For industrial applications the end-to-end latency requirements cover a range between 1000 ms to below 5ms, the latter for mission-critical applications where real-time transmissions are required for motion control. Reliability is defined as the ability to meet latency requirements i.e. data to/from peer entities is successfully transmitted to another peer within a predefined time frame, i.e., before a certain deadline expires. For some category of services, like "Factory Industrial Process automation & Motion Control", a reliability of at least 99.9999% is requested, this means that the probability of a packet not delivered within the specified deadline is to be below 10-6.

High availability within enterprises is essential to ensure minimal service downtime including under scenarios of disaster. This can be achieved by dedicated deployments in private networks ensuring network access to critical applications. For some emergency communication services, e.g. public safety, hospitals, 99.999% availability is required (i.e., less than ~300 seconds of accumulated outage per annum), aiming at equating availability of wireless and wired solutions.



Reliability and latency requirements for 5G networks (credit: Ericsson)

Figure: Latency, Reliability requirements for different verticals

Coverage:

While some industries need services only in a local area, others may require full coverage. For example, logistics and freight tracking need wide coverage and reliable location information for inventory and package tracking wherever they are. Other services have machines geographically located in many confined area, for example sensors/actuators in a hospital, refinery or garage. The 5G network will be able to efficiently manage several hot-spots areas which might be located in challenging coverage-positions (e.g., indoors or at the cell-edge). Furthermore, the service provider may not want to be dependent on the coverage and rollout strategy of a given operator and may therefor want to provide coverage on its own.

Private and Public Network Isolation:

While using a shared network infrastructure, the different vertical industries (and optionally the various services), need to be isolated one from another. That means that each virtual network belonging to different vertical customers are protected, preventing their resources from being accessed by network nodes of others. This is necessary to ensure a reliable and warranted service assurance, together with data and communication integrity and confidentiality. Appropriate data breakout architectures in a LTE / 5G public network have the potential to address enterprise data locality / confidentiality. Appropriate "Network Slice" separation is also necessary.

In a network sliced scenario, Verticals could deliver service to their own customers by ordering a network slice through a simple user interface. Several industries may rely on the Mobile Network Operator (MNO) for the deployment and management of their own network slice while other industries may want to do it independently. Self-Management of resources/policies, APIs, Service Assurance are core requirements for some vertical's businesses. Appropriate interfaces for flexible slice control between a Private and a Public network is essential. Another model is the one of a vertical who owns part of the network resources and designs and customizes their own service. In this case the vertical may need part of the network (for example the RAN) of the MNO according to a given SLA via appropriate interfaces.

Charging / Billing:

Verticals might have different requirements for charging, ranging from aggregated network usage information collection provided by a telco operator up to detailed per subscription accounting information. Appropriate interfaces between the Public and the Private networks are necessary to allow for flexible billing and charging. In some cases only the network infrastructure charges could apply and in some cases charges for the spectrum use could apply. The information collected should be suitable to allow verifying the SLAs the vertical has with the MNO in terms of services, quality of services, overall performance and the

resources assigned. As the specific charging or billing mechanism depends on the individual business cases, flexible interfaces are necessary for charging data delivery ranging from usage collection/recording to the supervision of the execution in real time.

1.3.2. Security and Identity Management requirements

Secure communications need to guarantee that personal or confidential data must not reach the public domain and not be modified or replayed by unauthorized parties. Verticals industries will require different levels of security. For example, security mechanisms used for ultra low-latency, mission-critical applications (e.g. autonomous driving, control of a smart grid or smart operation of industrial automation processes) require a high level of communication security and may not be suitable in massive Internet of Things (IoT) deployments where mobile devices are inexpensive sensors that have a very limited energy budget and transmit data occasionally. Private networks will connect a huge variety of devices and users which have subscriptions to vertical service providers. This requires that a new device-user identity management and related lifecycle management, which will complement the universal SIM (USIM) is put in place.

Different mechanisms for identifying, authenticating devices and their subscription needs to be supported. Appropriate trust relations needs to be defined between the Public and Private networks based on the level of network / spectrum sharing that is put in place.

• Authentication by the Private network only: service providers may rely on only the local network authentication.

• Authentication by the public service/network provider only: authentication is performed from the public service/network provider BUT the devices are recognized as “Private Network Use Only” i.e. with limited base station or geographically constrained network access rights.

• Authentication by both Private network and Public service/network providers, each for the related domain. This is applicable when services are shared across private and public networks.

• Protect control and user plane by means of encryption at network layer and/or application layer. In addition, applications may require not only encryption, but user plane integrity protection service that is able to guarantee the privacy of all users’ communications.

2. Private Networks, enabling technologies

The network infrastructure for a private LTE network can be a scaled-down version of the standard 3GPP infrastructure used to realize public mobile networks. This infrastructure typically consists of Radio Access Network (RAN) and an Evolved Packet Core (EPC). Using the 3GPP framework as the logical architecture allows enterprises to considering deployment of LTE/5G based private networks but with appropriate modifications by characterizing the desired deployment environment and the desired scale for their use case. In 3GPP, small cell solutions were conceived for deployment in venues, enterprises and other commercial premises. Small cells are low-power cellular base stations. These small cell based RAN solutions can be adapted to serve the Private Network use case. In addition to small cells, a private LTE network may require a private EPC. An EPC offers 3GPP specific routing and signalling functionality as well as maintenance of 3GPP specific database contents. With an EPC in place, the private LTE network becomes just another way to gain IP connectivity to the enterprise IP network and services, exactly in the same way as Ethernet or Wi-Fi are used. Several companies now offer 3GPP compliant EPC functionality as software running on single physical or virtual server (called a "virtual EPC"). The EPC should easily integrate with the enterprise's existing IT systems.

It is also essential that in the case of Shared Spectrum solution for private networks, the small cells should be able to communicate with the SAS (Spectrum Access System).

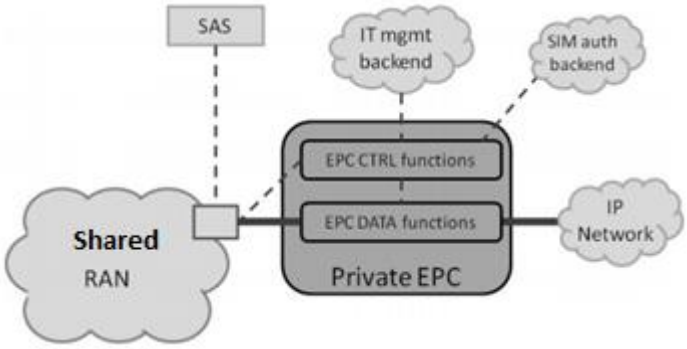


Figure: Example of Shared RAN with a Private EPC

2.1. Network Identification:

An LTE network is identified based on a Public Land Mobile Network Identifier (PLMN-ID). Each mobile operator has a unique PLMN-ID. Further, the 3GPP specification allows each mobile operator to create Closed Subscriber Groups (CSG) to offer separate access authorization and differentiated services to specific groups of its subscribers. An LTE RAN broadcasts the supported PLMN-IDs as well as the CSG-ID served by the specific local LTE deployment. Since it is not practical for every enterprise to obtain its own PLMN-ID, it is expected that private LTE networks will be identified using a common PLMN-ID and an enterprise-specific CSGID. The common PLMN-ID to support private CBRS network deployments could be acquired by a neutral industry organization. This industry organization would then be responsible for assigning CSG-IDs to enterprises.

2.2. Subscriber Identification & Authentication:

An LTE subscriber is identified using an International Mobile Subscriber Identifier (IMSI). A subscriber's IMSI is stored on SIM card, and is tied to the PLMN-ID of the mobile operator that issued the SIM card. This mobile operator is called the subscriber's Home PLMN. When a subscriber's device connects to a LTE network, the IMSI and associated credentials within the device's SIM card are authenticated against the Home Subscriber Server (HSS) located in the Home PLMN's backend. As discussed in the previous section, it is expected that all private LTE networks may use a common PLMN-ID that has been acquired by an industry organization. Any enterprise should be able to reserve a set of IMSIs associated with this PLMN-ID via the industry organization. A mid-sized hospital may reserve 2,000 IMSI values while a large distribution hub may choose to reserve 10,000 IMSIs. Once the enterprise has its set of IMSIs, it can procure the SIM cards and the associated authentication backend solution for its private LTE network. SIM cards can either be traditional plastic SIM card or be software based. The enterprise can then connect its EPC to a SIM authentication backend, which can either be a cloud-based managed service or a solution deployable by the enterprise itself. Examples of such a framework of IMSI assignment with PLMN-ID acquired by an industry organization is indicated below (From the CBRS Alliance [5]).

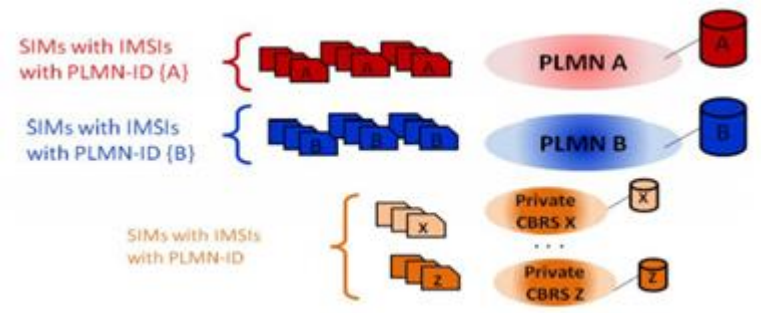


Figure: Subscriber Identification for PLMNs and Private Networks

2.3. Services & Applications:

The use of 3GPP-compliant network infrastructure, client devices, and authentication methods allows the private LTE network to use a scaled-down version of 3GPP-specified mobile service infrastructure. The private LTE network appears as just another way to gain IP connectivity to the enterprise IP network and services and the enterprise can load any operating system and application on its client devices.

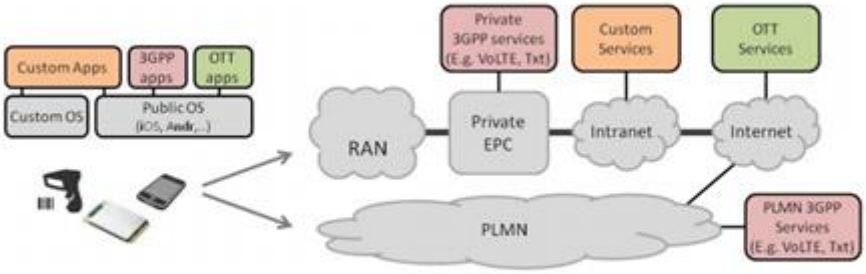


Figure: Various usable services and related client applications

2.4. Private LTE Network as Neutral Host for Public Networks:

Many enterprises have employees and guests who use their smartphones on public LTE networks. A private LTE network can be configured to also offer public LTE service for the smartphones. To support this use case, a private LTE RAN can be configured to simultaneously advertise PLMN-IDs of multiple mobile operators or private networks and to connect to multiple core networks. For example, the same private LTE RAN can be connected to a private EPC and up to five public mobile service provider EPCs. Recent changes to the 3GPP LTE specification make it easier for enterprises and mobile service providers to share a LTE RAN by allowing each service provider to assign its own cell identities and tracking area codes to the RAN, removing the need for coordinating these identifiers between the participating service providers.

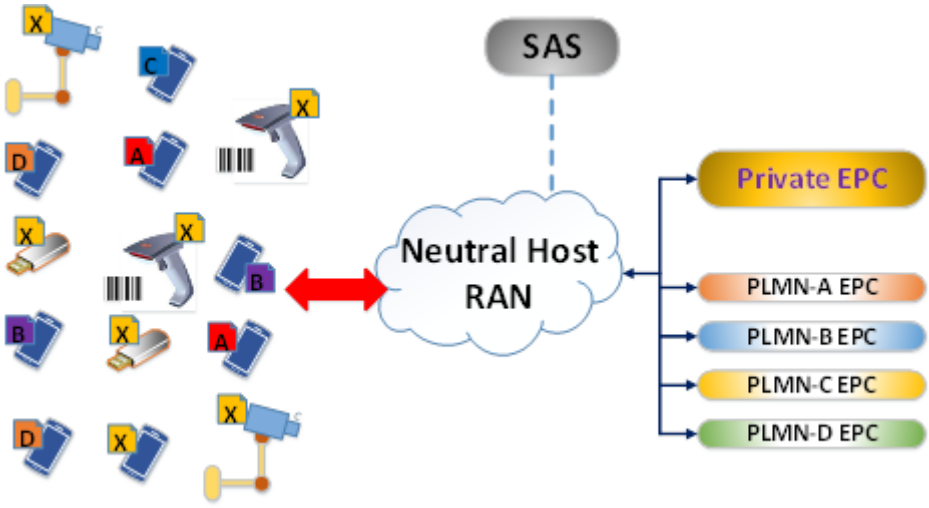


Figure: A Neutral host connected to multiple EPCs

Using the same network infrastructure for both private and public LTE / 5G networks can create new business models. Private networks can also be built and managed by a large mobile operator.

2.5. Network Sharing

Developing a private network practically relies on the network sharing specifications. 3GPP has defined two approaches for the eUTRAN sharing:

- The Multi-Operator Core Network (MOCN) approach
- The Gateway Core Network (GWCN) approach.

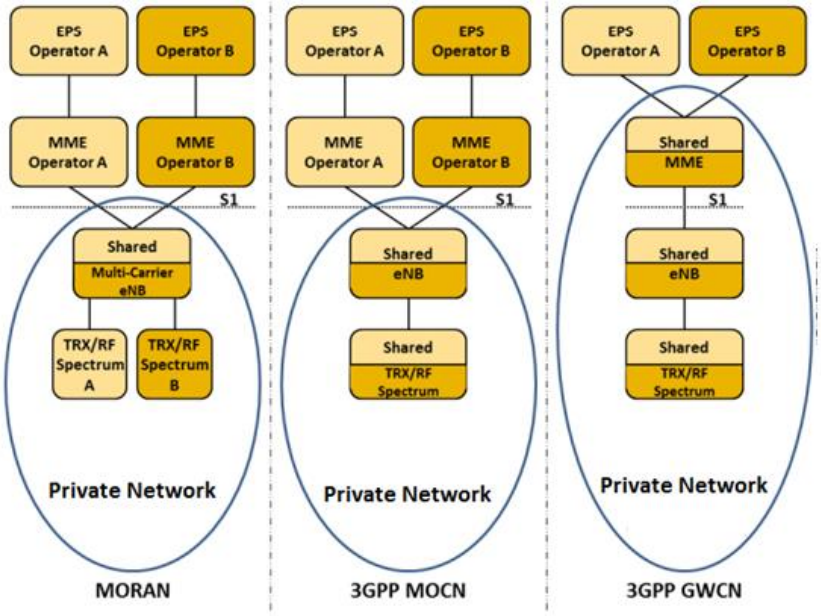


Figure: The Three Approaches to Network Sharing

MORAN (Mobile Operator Radio Access Network)

If each of the network operators sharing a base station uses his own spectrum (i.e. his own radio channel) the operators share the backhaul link from the base station to the core network and the digital module of the base station but have separate RF paths and radio units. A simple mobile device trace analysis can't reveal if the two signals come from the same base station or not. One would have to compare the network configuration parameters in the system information messages carefully but even here there might be differences.

MOCN (Multi-Operator Core Network)

In this sharing approach the base station is shared by broadcasting several Mobile Country Codes (MCC) and Mobile Network Codes (MNC) in the System Information of a radio channel. In the case of UMTS this is done in the Master Information Block (MIB), while in LTE this is done in the System Information Block (SIB) [1].

The Gateway Core Network (GWCN)

In the GWCN approach, contrary to the MOCN approach, the MME is also shared between the different mobile network operators.

2.6. Data breakout techniques (LIPA, SIPTO)

3GPP has extended the use of femtocells in order to limit the loads of both aggregation and core networks. Femtocells potentially allow a direct access to the public IP network via the fixed network. Hence, by adding a local PDN gateway (LPGW) which is either co-located with the femtocell or a standalone entity connected to the femtocell via a separate interface, mobile data traffic will bypass the mobile core network and thus reduce the load of the standard gateways (SGW and PGW) used in a 4G network.

LIPA and SIPTO, two solutions of traffic offloading, were also introduced in order to offload selected IP traffic from the mobile core network. LIPA and SIPTO both offer a direct connection between mobile users and the Home/Enterprise Local Access Network (LAN) devices. At the same time, a UE shall be able to have simultaneous access to the local IP network (using LIPA/SIPTO) and to the operator's core network through the normal path. These solutions were improved in 3GPP Rel-12 by solving some of the mobility issues raised in their first version. The figure below illustrates the 3GPP regular data path as well as offloading architectures for both LIPA and SIPTO solutions.

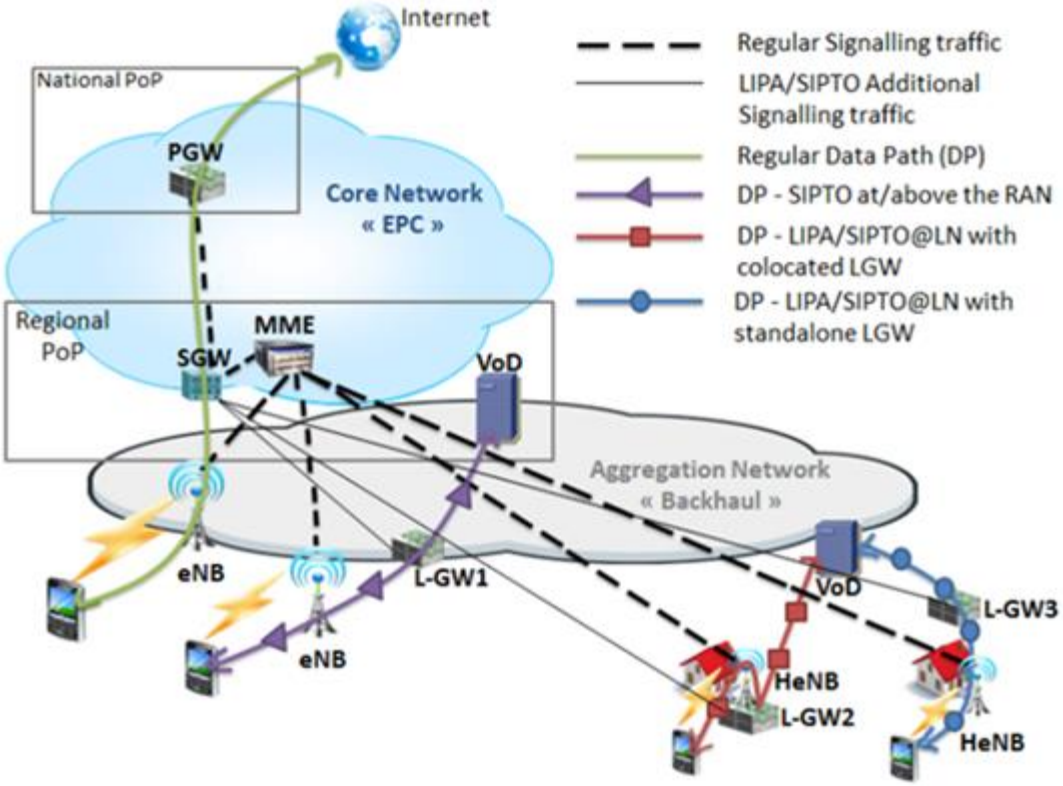


Figure: LIPA and SIPTO Solutions for Cellular Data Breakout into an Enterprise IP Network.

LIPA is an offloading technique allowing a direct connection between the UE and the local IP network using a femtocell (HeNB) with a co-located or a standalone Local Gateway (LGW). The LGW must support limited PGW as well as SGW functionalities such as interconnecting with the external IP networks, UE's IP address allocation functionality, DL packet buffering, etc. However, LIPA is only intended to allow the UEs to access their own Private Local Access Network via a femtocell. Thus, UEs may not apply LIPA when connected through a macrocell.

SIPTO is an offloading mechanism defined by 3GPP to allow mobile operators to selectively breakout some of the user's IP data traffic:

- "At the local network" using a femtocell with a co-located or a standalone LGW "Similar to LIPA";
- "At or above the RAN" using a macrocell by selecting an SGW and PGW that are topologically/geographically closer to the radio network.

Unlike LIPA, SIPTO can be used in both macrocells and femtocells.

2.7. Network In a Box (NIB) solutions

A compact LTE/5G box that implements most of the RAN and EPC functionalities is referred to as a Network in a Box solution. The solution is intended for private networks but some of the key interfaces towards HSS etc should still come from an operator as shown in the figure below.

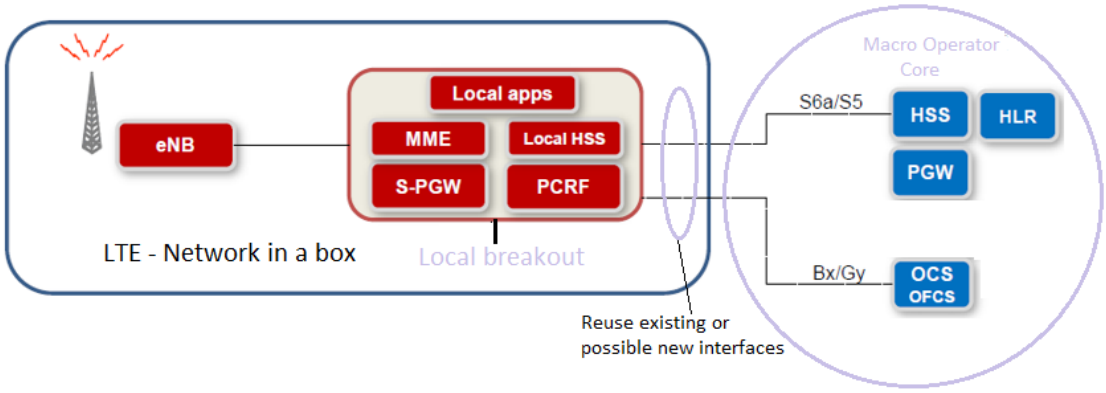


Figure: LTE Network In a Box (NIB)

2.8. **Spectrum sharing for Private Networks**

Spectrum sharing is critical for private network as most enterprises are expected not to own any spectrum.

Spectrum can be classified into the following:

Dedicated licensed: The conventional model used by mobile networks today, where specific operators (MNOs) gain rights, usually through auctions, to particular frequencies for exclusive use. This allows full management and therefore guarantees of QoS.

Unlicensed / license-exempt: Used for WiFi and other "ISM" (industrial, scientific, medical) applications. No specific user license is needed, which lowers costs but also risks interference and congestion.

Shared spectrum, or Dynamic spectrum access: Multiple users get access to a given band, but it is not a "free for all". There are some mechanisms to ensure separation, fairness, pre-emption, manageability and so forth - but not nationwide exclusivity.

There can be combined use of licensed and unlicensed spectrum (LAA) or a scenario where a primary user allows a “few” secondary users in an otherwise “licensed” spectrum (LSA, TVWS, CBRS).

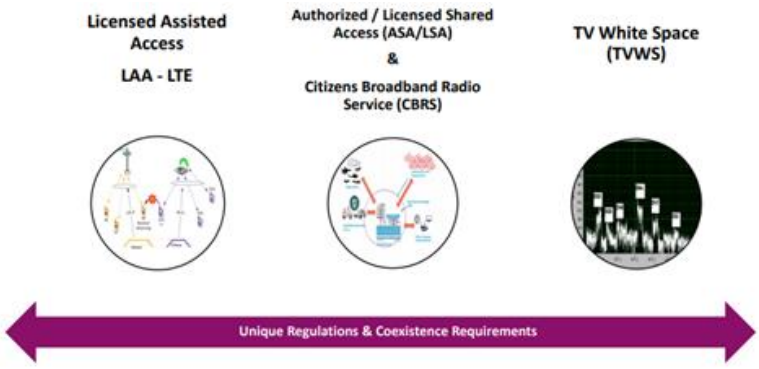


Figure: Combination of Licensed and Unlicensed and Secondary usage spectrum scenarios

It is worth noting that there are various approaches to using shared spectrum emerging. The "TV white spaces" is also a viable approach for “Private networks”.

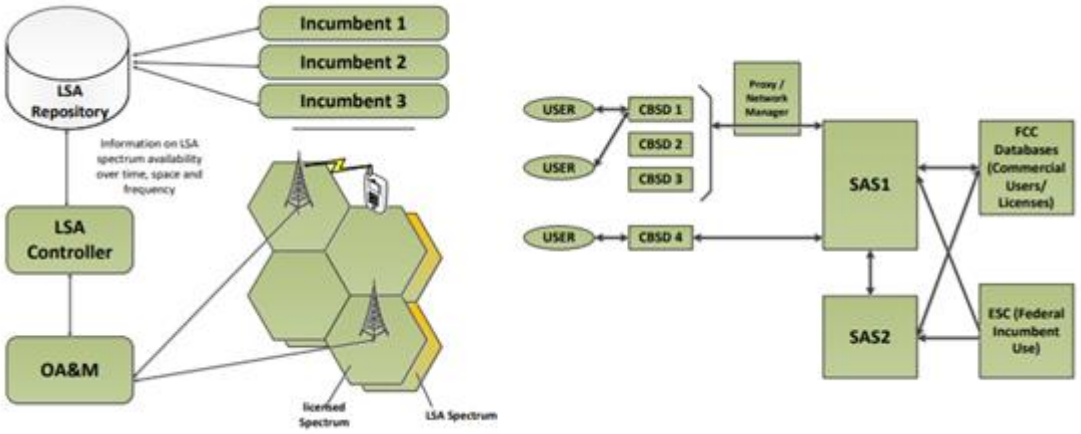


Figure: LSA and SAS spectrum usage scenarios

2.8.1. The CBRS example

In the CBRS case, the key issue for the success will be who will monitor the device/operator behaviour across tiers. 150 Mhz of spectrum in the US is open for new use without interrupting incumbents. The CBRS mode of operation is to provide protection of the incumbent reliable operation for Priority Access License (PAL) and opportunistic access to General Authorized Access (GAA) users.

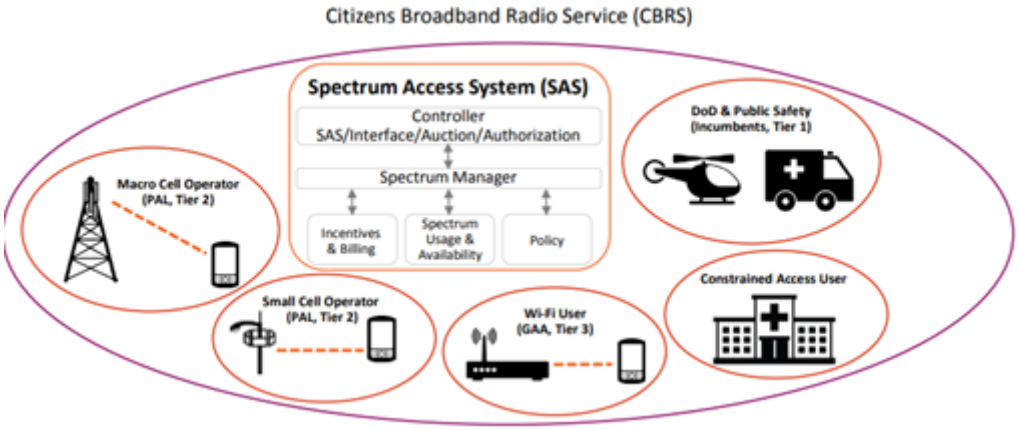


Figure: CBRS supported by the SAS

2.8.2. Other examples of Shared Spectrum

The Guardband, which is a band between two large chunks of allocated bands is also a viable spectrum for use in private networks. China is already using the guardband for vertical industries like Rail and metro operations, sea port, campus, and city wide public safety operations. As shown in the below diagram, AreteM (A Singapore based Operator) is

deploying the central 10Mhz guardband band in LTE Band 3 to deploy a dedicated TD-LTE network to serve the vertical industries.

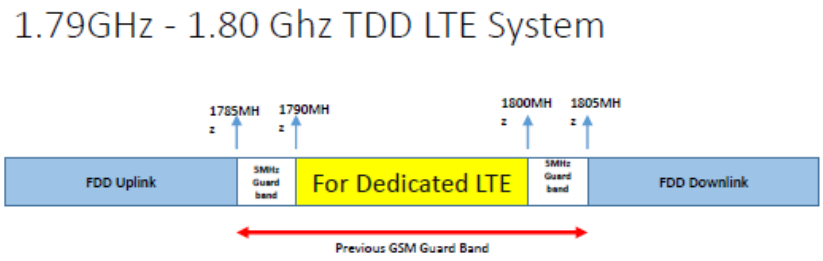
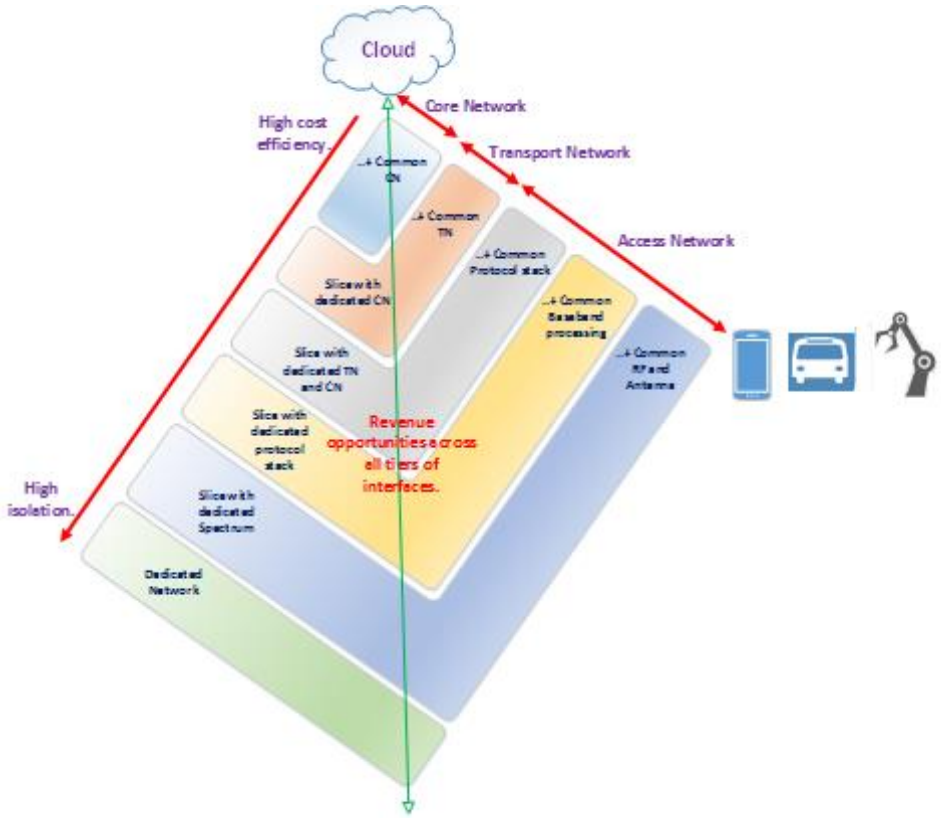


Figure: Guard band TDD deployment as an example

2.9. **Summary**

In summary different levels of network / service sharing is possible for the realization of Private networks. The below figure summarizes the different "Private Network" architectural/deployment possibilities to meet requirements summarized in the previous section.



Using a combination of Small cells, Network in a box solutions, data breakout mechanisms like LPIA/SIPTO and through the appropriate use of spectrum sharing mechanisms any quadrant of the above figure can be covered. In a 5G network it is also possible to take the network slicing approach for different verticals when the network is fully shared. When the network is not shared between a private and a public network, key orchestration points will be needed to achieve private network provisioning.

In this section, we list the gaps in the existing "enabling technologies" for the adoption of large scale "private networks". Gaps that need to be filled include, but are not limited to

- key architectures defining spectrum sharing, network sharing and data breakout mechanisms between a macro and a private network
- Dynamic Spectrum sharing with appropriate monitoring mechanisms across spectrums (Between TV WS, CBRS, Dedicated spectrum as an example)
- An Industry acceptable "Network In a Box (NIP)" definition with appropriate interfaces into a Macro core network.
- Well defined revenue sharing models for Dedicated/Shared spectrum deployments
- In the case of "Network Slicing", orchestration mechanisms that are flexible to allow for both Public and Private operators to control the network needs to be in place.

Detailed architectural model discussions are beyond the scope of this whitepaper.

3. Business Scenarios and Revenue models

This section covers possible business scenarios/models under different combinations of private and public networks. In order to arrive at the appropriate business models, the Private/Public network combinations can be seen as a network of networks.

Source: Adapted from Ericsson, "5G systems," www.ericsson.com/assets/local/publications/white-papers/wp-5g-systems.pdf.

Figure: 5G Network of Networks model

The evolution of mobile generations has seen a shift in the relationship between the user and the network operator. We can characterize this by an understanding of the relation between the Services, Devices, Network and the Customer.

Applications and services are becoming agnostic of the mobile network on which they're riding, termed over-the-top services, these applications or services can be expected to continue/evolve into 5G.

Devices are increasingly becoming agnostic of particular carrier networks, with regulation and competition aiding this model. With 5G there is a chance that the device ecosystem will move into an instalment plan based service. Most devices with the emergence of 5G will be Customer Premise equipment or IOT devices leading to the opportunity for telecom carriers to generate higher equipment revenues from instalment plans and leasing programs.

With the emergence of private networks, there is an opportunity to tap into the separation of networks allowing for operators to generate revenue from spectrum than by just selling SIMs to end customers. As the end customer revenues are falling, revenues from enterprise private networks, where the network costs are shared look lucrative.

The below model of network of networks is used as a model to study the business implications of "Private Networks"

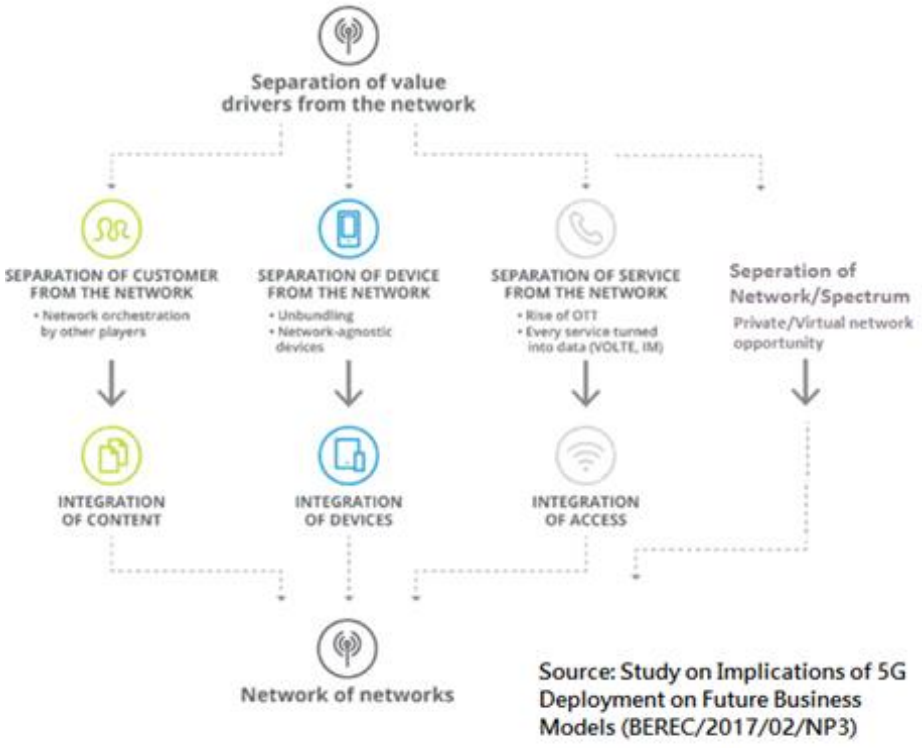


Figure: Separation of value drivers in a "Private Network" scenario.

3.1. "Private Networks" as a Network of Networks

Emerging networks are a "network of networks" where multiple network entities come together to realize end to end services. This includes OTT apps, Media devices and gateways, Service gateways etc.

Provisioning, managing and securing devices over network assets from public and private networks is something that Service providers will likely need to shift focus to. This will require that "Private Network" interface definitions across all layers is in place. The same holds true for the management and operating relationships between connected devices for better management and integration. Currently users define these relationships on a static basis but this can become untenable when a large portion of IOT devices come into the ecosystem. Device management will likely have to move from this simple, static world to one where complex, flexible dynamic relationships can be established and changed.

The media industry is undergoing a rapid change with new synergies between the content generators and distributers. It happened with cinema and the studio system, and television is following the same pattern, with over-the-air broadcasters creating significant content assets. With the switch to the multichannel universe, we see integrated models emerging again with the creation of cable channels (many by cable TV distributors) and satellite companies being vertically integrated. As this trend becomes mainstream, content may also be integrated. Having distribution assets along with content assets can make a player better positioned in this emerging scenario.

Private Networks enabling Economies of scope. The advent of private networks (and 5G network slicing) is likely to catalyse a new wave of industry transformation driven by alliances, mergers, and acquisitions. Over the last two decades, as companies have sought greater economies of scale, the telecommunications industry has seen regular consolidation of like players. In this new era, the industry will likely be driven by a different kind of consolidation: one that increases companies' scope and capabilities as carriers look to acquire new capabilities and technologies from smaller private players.

3.1.1. Cost model for Operators:

The extent to which LTE/5G private networks are monetized way will depend on:

- Whether MNOs (or connectivity providers more generally) will be able to successfully identify all the relevant niches where LTE/5G might be useful (Vertical market use cases).

- Whether MNOs will be able to develop a range of standardised interfaces to possible “external” entities in terms of networks, services and verticals.
- Given the possibility of a number of specialized requirements, there may be a role for intermediaries in identifying new applications for LTE/5G private networks. MNOs will need to identify appropriate intermediaries and work out the business relations. This specifically applies for media content distribution.

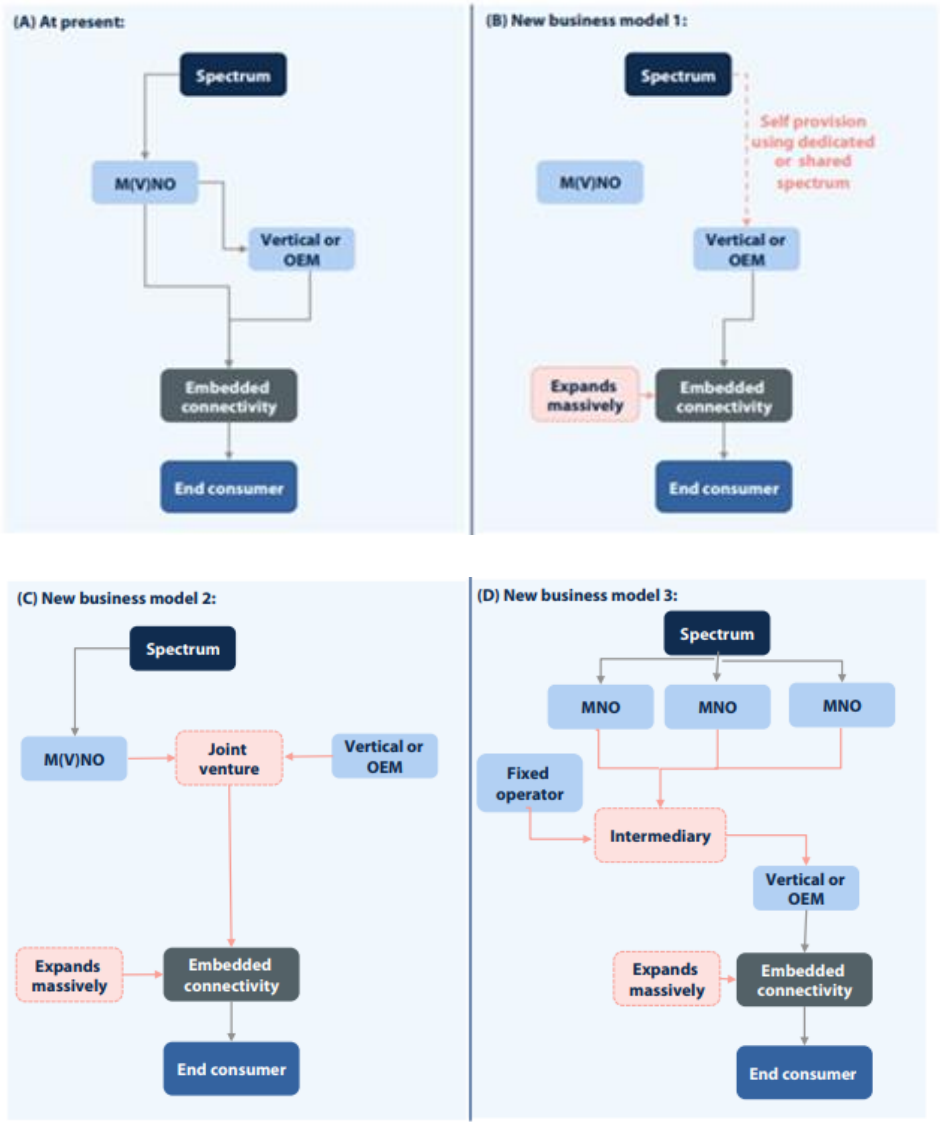


Figure: Possible business models for “Private Network” scenario.

4. “Private or Non-Public Networks” Roadmap in 3GPP

3GPP is currently studying use cases for using “3GPP 5G technologies” to provide “virtual LAN style services” as well as “Non-Public Network” services.

3GPP TS 22.261 provides the Service requirements for the 5G system; Stage 1 definition for non-public networks as “a network that is intended for non-public use”.

As per the 3GPP SA1 definition “Non-public networks are intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations, utilising both virtual and physical elements. Specifically, they may be deployed as completely standalone networks, they may be hosted by a PLMN, or they may be offered as a slice of a PLMN”.

The 3GPP SA1 requirements are listed below:

- The 5G system shall support non-public networks.
- The 5G system shall support non-public networks that provide coverage within a specific geographic area.
- The 5G system shall support both physical and virtual non-public networks.
- The 5G system shall support standalone operation of a non-public network, i.e. a non-public network may be able to operate without dependency on a PLMN.
- Subject to an agreement between the operators and service providers, operator policies and the regional or national regulatory requirements, the 5G system shall support for non-public network subscribers:
    - access to subscribed PLMN services via the non-public network;
    - seamless service continuity for subscribed PLMN services between a non-public network and a PLMN;
    - access to selected non-public network services via a PLMN;
    - seamless service continuity for non-public network services between a non-public network and a PLMN.
- A non-public network subscriber to access a PLMN service shall have a service subscription using 3GPP identifiers and credentials provided or accepted by a PLMN.
- The 5G system shall support a mechanism for a UE to identify and select a non-public network.
    - NOTE: Different network selection mechanisms may be used for physical vs virtual non-public networks.

- The 5G system shall support identifiers for a large number of non-public networks to minimize collision likelihood between assigned identifiers.
- The 5G system shall support a mechanism to prevent a UE with a subscription to a non-public network from automatically selecting and attaching to a PLMN or non-public network it is not authorised to select.
- The 5G system shall support a mechanism to prevent a UE with a subscription to a PLMN from automatically selecting and attaching to a non-public network it is not authorised to select.
- The 5G system shall support a change of host of a non-public network from one PLMN to another PLMN without changing the network selection information stored in the UEs of the non-public network.

There is also a study item on "Non-Public Networks" in the SA2 working group though not much progress can be seen.

There are multiple market segments such as enterprise, residential and private networks, where 3GPP operators could provide services for private communications. One example segment is industrial automation, where currently LAN-based technologies are used to interconnect sensors and actuators (e.g., both could be fixed or mobile) with closed-loop or supervisory control equipment. There is increasing interest in using new technologies which are characterised by stringent performance requirements such as those supported by the 3GPP-defined 5G system (e.g., low latency, high reliability.)

Another sector is residential broadband, which is expanding in scope. As more things are connected, 3GPP technology can provide improved experiences, both indoor and outdoor, over short or long distances, and in a unified manner across many different products. The performance requirements of these applications could also benefit from 3GPP 5G technology. The current 3GPP scope of study is provided below.

- The 3GPP network operator enabling a restricted set of UEs to communicate privately amongst each other over a 3GPP operator's network. The 3GPP network operator can be a 3GPP PLMN Operator or the owner of the 3GPP network used for communication between UEs.
- The 3GPP network operator enabled to control the UEs belonging to a group of UEs communicating privately amongst each other.
- 3GPP configuration and 3GPP communications between members of the private group under network operator's control.
- UEs communicating in a private group use the 3GPP network with a secure 3GPP authentication mechanism.

- The support of different application protocols between UEs (e.g., IP based, Non-IP based).

3GPP also is studying the possibility of enabling “Local Private Network for Industrial Automation”. Deployment with a local dedicated RAN and a local dedicated Core Network used exclusively for the Industrial Automation scenario provides a method to guarantee availability due to strict management of the subscriber base. In this scenario, local means that the infrastructure for both RAN and Core Network are located on the site of the network deployment and that dedicated means that only authorised devices can access the network.

Local situation enables on-site maintainability to ensure that preventative maintenance and recovery procedures are more directly managed by the end user of the system. Local situation also reduces end-to-end latency for those use cases which require core network interaction due to reduced number of interstitial nodes, no trunking (including delays on shared trunking infrastructure), shorter transport distances.

Dedicated usage enables increased predictability of latency and throughput due to controllable population, reduction of contention ratios, and customisability with deployments including RAN placement, core functionality, traffic routing, data storage, etc.

A scenario where this deployment may be suitable is factory floor automation, where a variety of sensors, devices, machines, robots, actuators, and terminals are required to communicate to perform efficiently. Some of these devices may be directly connected to the local private network and some may be connected via gateway(s).

An example of the deployment scenario is provided in the below figure:

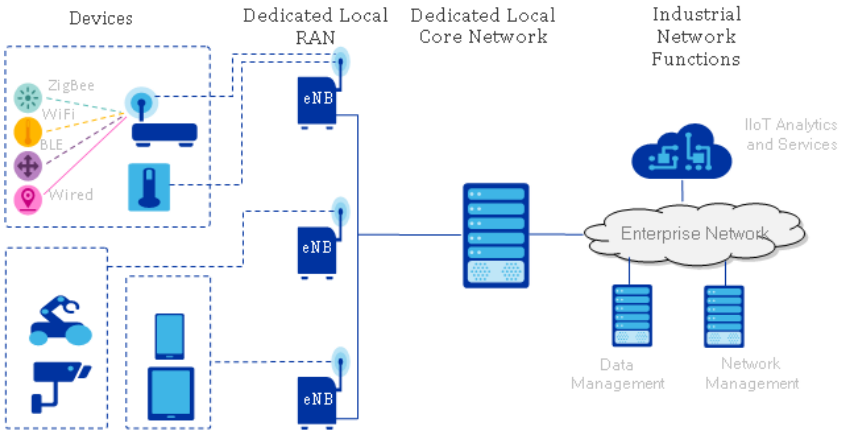


Figure: Possible Local Private Network for Industrial Automation deployment

5. Private Network Deployment - Case Studies

5.1. China Mobile

TBD

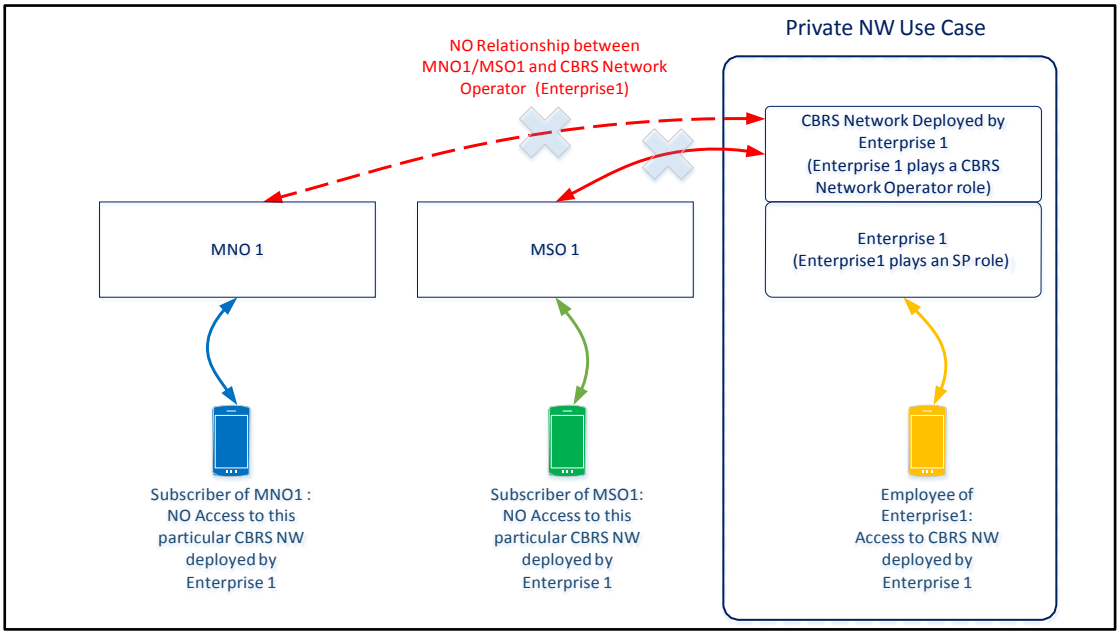
5.2. (US)

5.2.1. CBRS Example

LTE, and eventually 5G, is the mobile broadband technology of choice for MNOs to deploy services to its subscribers. Enterprises, however, have been unable to use LTE for their own private networks as LTE requires licensed spectrum. That will all change with the availability of CBRS spectrum in the U.S. Enterprises will be able to use the spectrum, from 3.55 GHz to 3.70 GHz (LTE Band 48), to deploy private wireless networks based on LTE in the U.S. without obtaining licenses from the regulator. Benefiting Enterprises that wish to deploy Private LTE networks in the CBRS GAA Spectrum is the tremendous ecosystem of infrastructure and devices that exist in the marketplace.

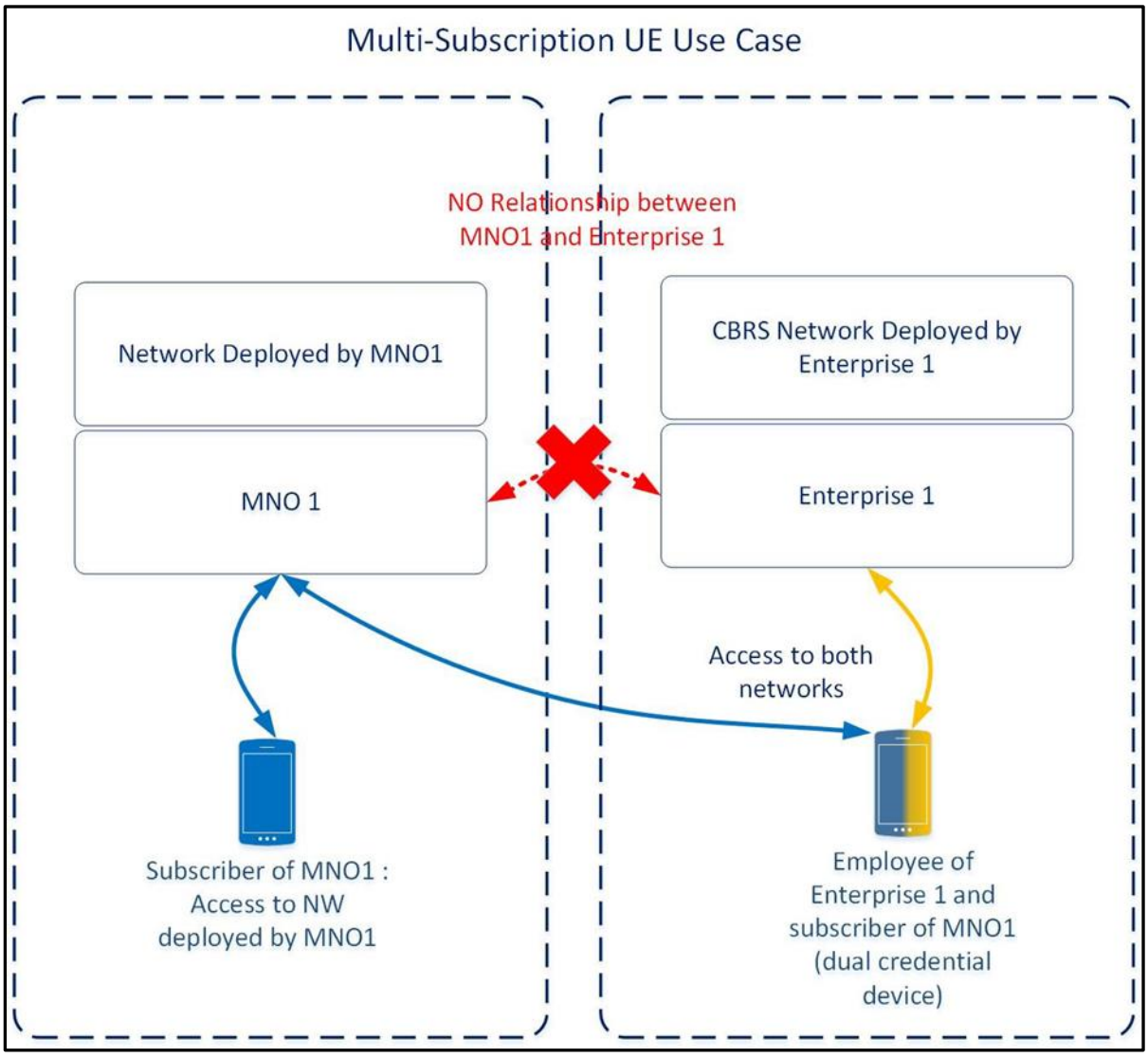
There are two specific use cases that have been outlined within the CBRS Alliance Technical specifications [8], although numerous use cases and information can be found in the literature/media.

The first use case is a single subscription UE use case. A Private CBRS network is deployed to provide service to employees, machines and other devices as authorized by the Private Network provider. In this case, the private network operator plays the roles of both Service Provider and CBRS Network Operator. A private network operator that deploys and manages an LTE Core network and an LTE RAN that operates in the CBRS band provides services exclusively for its own Subscribers. The figure below illustrates this concept.



In the figure, Enterprise 1 deploys a CBRS Network. Employees or customers of Enterprise 1 can access the CBRS Network deployed by Enterprise 1. Enterprise 1 does not have any business relationship with MNO1 or MSO1; hence the Subscribers of MNO1 or MSO1 do not have access to the CBRS Network deployed by Enterprise 1.

The second use case is a multi-subscription UE use case. In this instance, a UE used in a Private Network has both a subscription with the Private Network and a subscription with an MNO. The MNO subscription can be used to access the MNO's network when the Private Network coverage is unsatisfactory or when the Subscriber needs to access MNO services unavailable within the Private Network. The device uses separate, unique credentials for access to the different networks. The Subscriber may use an MNO subscription to access MNO services using a Private Network as an untrusted network. In this case, the subscriber can use untrusted non-3GPP access procedures to access MNO services. The figure below illustrates this concept.



In this example above, Enterprise 1 deploys a CBRS Network and provides private services to the authorized users. Enterprise 1 does not have any business relationship with MNO1. An authorized user of Enterprise 1 also has a subscription to MNO1 with a separate MNO1 credential. This employee can access the private network services through the CBRS network deployed by Enterprise 1. The employee can also access the MNO services with the CBRS network acting as an untrusted non-3GPP access (e.g., the UE can connect to the MNO's ePDG to access MNO network/services).

5.3. **AreteM (Singapore)**

AreteM is a Facility Based Licenced Operator in Singapore which provides dedicated TD-LTE Mission Critical Communications Services in Public Safety, Public Surveillance and Vertical Industries by deploying Private LTE Networks using 10 MHz spectrum at 1800 MHz band.

5.3.1. Shipyard/Seaport – Public Safety Trunking Solution

AreteM has deployed two-sectored outdoor site at one of the main Shipyard sites in Singapore. The customer is using the network for the public safety trunking (voice, video, text, group calling) solution currently. The customer has plan to use the network for different other applications such as ships movement monitoring, remote control of unmanned heavy vehicle, drone application for site inspection, CCTV surveillance, workers entry/exit logger application and so on.

Actual Network Deployment:

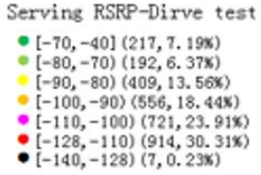
The front-end network consists of 1 remote unit with 4Tx4R which has been configured into two sectors of 2Tx2R feeding to two antennas as shown in the picture. For coverage inside two ships, two CPEs (Customer Premises Equipment) are installed inside the ships. A total of

Huawei Cabinet, C-Channel,150mmx 100mm and 50mmx50mm cable trunking as installed

65 mobile handsets are currently being used.

Private LTE Actual Deployment at Shipyard in Singapore

Signal Strength Trail Deployment:



from

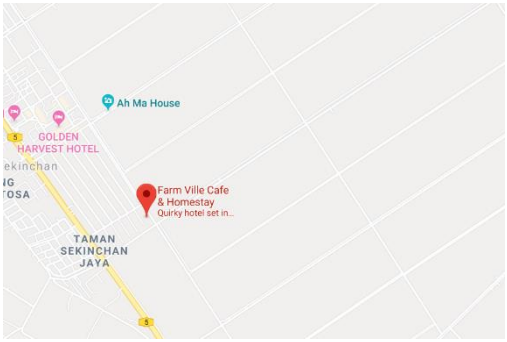
5.3.2. SkyLTE – Drone Control Platform

SkyLTE is AreteM's platform to control drone using AreteM's private LTE network. AreteM conducted a Proof of Concept (PoC) trial to test private LTE connectivity to control drone deployment Beyond Visual Line of Sight (BVLOS) environment under the coverage of private LTE network in the presence of the frequency regulatory body and the customer. The trial was successful with the following objectives:

- Setup and deploy LTE cellular network trial site in Malaysia.
- UAV (Unmanned Autonomous Vehicle) remote control via AreteM's platform using secured handshake protocol between UAV and the platform.
- Drone can fly Beyond Visual Line of Sight (BVLOS) with failsafe features.
- Remote Surveillance and Monitoring

Trial Setup and User Requirements:

The trial site was selected by the customer in Malaysia in the paddy field. An LTE cellular network was setup using AreteM's private LTE network. It consisted of 2 eNodeBs, Cell 1 and Cell 2. Both cells were setup to provide coverage to the padding field in front of the base camp where the customer had their servers, laptops and AreteM's UAV platform. Both Cell 1 and Cell 2 were configured to provide handover capabilities.

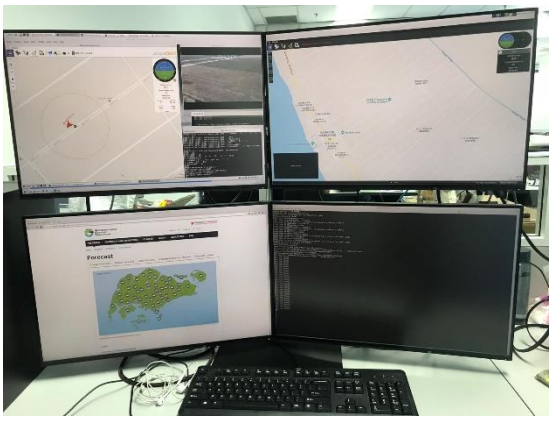


Private LTE Network Setup for Trial

UAV (Drones) and AreteM's Platform:

The UAV (Drones) were equipped with AreteM proprietary LTE and computing module that allowed the control of drone via AreteM's private LTE network and platform. The computing module provided the bridge between the UAV flight controller and the LTE module, relaying all the communications from the drone to the end user via AreteM's private LTE network. It

handled all the LTE communications and capabilities such as video streaming, secure heart-beat, etc.

UAV (Drone) and AreteM's Private LTE Platform

The platform provides the end user a visual method to control the drone which includes, but not limited, taking off from ground, returning to launch site, point and click flying using secure handshake protocol between UAV and the platform. It also provides real-time video streaming and telemetry coming back from the drone.

Can fly Beyond Visual Line of Sight (BVLOS) with Failsafe Features:

Due to handover capabilities of the AreteM's private LTE network, the range that the drone can fly is only limited by the coverage of the LTE network and thus enabling BVLOS flight. With the AreteM's computing module which monitor the LTE signal strength, it can provide various fail-safe features, e.g., hover at location, as requested by the customer.

AreteM's computing module allows the customisation of various fail safe to meet different clients' needs.

Remote Surveillance and Monitoring:

Using the combination of AreteM's private LTE network and Internet, the pilot view including video can be relayed back to a remote site, away from the theatre of operation, for remote monitoring and higher-level planning.

Test Cases and Results:

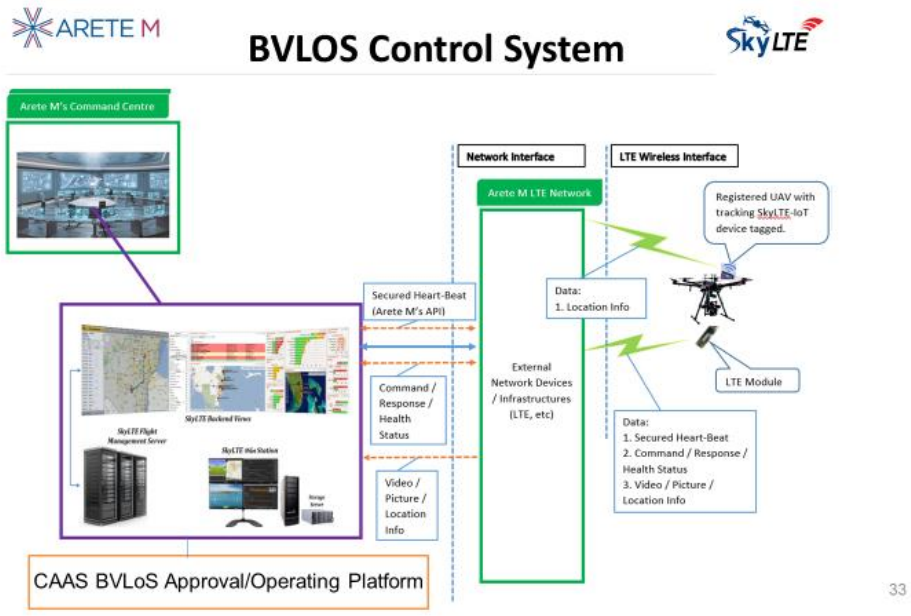
Objectives	Test Cases	Milestones Achieved
UAV remote control via AreteM's private LTE platform using secured handshake protocol between UAV and the platform	1. The drone able to take off, land and fly via point-click on the platform. 2. Display telemetry on the platform.	✓ UAV remote control via the platform. ✓ Fully controlled via secured handshake protocol between the UAV and the

	3. Display video on the platform.	platform.
Can fly Beyond Visual Line of Sight (BVLOS) with failsafe features	1. UE display different cell id to indicate handover. 2. EPC server should show the handover event. 3. Individual eNodeB should show the UE has moved across the different eNodeB. 4. Drone should hover in place when LTE signal is lost. 5. Drone is unable to fly outside the predetermined area.	✓ Can fly BVLOS with cell to cell handover. ✓ UAV failsafe feature. ✓ Geofencing.
Remote Surveillance and Monitoring	1. Able to view telemetry and video from remote site.	✓ Remote surveillance and monitoring.

Following the success of the trial, AreteM is now under the deployment of private LTE network for the application of drone control to monitor sky activities for the civil aviation and public safety.

The Civil Aviation Authority of Singapore had awarded a consortium to develop and show case BVLOS flight of UAVs in an urban environment that meets their high standard of safety requirements. One of the technology that this consortium has proposed is to use a combination of Private LTE together with Public LTE to provide superior communication resiliency to ensure that the UAV are always connected to the control and management platform. This combination of a Private LTE carrier is to guarantee that there will not have any congestion so that the UAV connectivity has guarantee low latency and the Public LTE can be used as a back up if and when the Private LTE network has a breakdown.

A picture of such a multi-carrier module combining Private LTE with Public LTE to control unmanned systems like UAV is shown below together with the BVLOS Platform :



Besides UAV, the same multi-carrier module could be used in controlling Unmanned Surface Vessel(USV) where USV can be used for remote territory water surveillance and high speed remote piloting during incident management instances.

….

….

5.4. **Reliance Jio (India)**

TBD

6. GTI Observations and Conclusions

It is evident that multiple markets exist such as enterprise, residential, industrial segments where 3GPP operators could provide services for private communications. 3GPP is focused on defining the non-public network specifications that provide coverage within a specific geographic area, support both physical, virtual and standalone non-public networks. When addressing the specifications, it is important to gather inputs from operators and vertical industry segments. Current 3GPP requirements are focused on “access restrictions” between Public and Private networks but the possible need for new network architecture is ignored. 3GPP is also trying to define service APIs for different verticals in the SA6 working group, multiple other standards bodies such as OneM2M are addressing these industry verticals with “Open API” and “service layer” approach. Such standards from different bodies need harmonization. This white paper enumerates possible business models for non-public networks as well as provide insights on the nature of “private” deployments envisaged by operators and vertical industry. The learnings from the white paper, which is a collection of inputs from different industry segments will be shared with 3GPP from time to time to influence the specification evolution within 3GPP. GTI through this white paper will also attempt hominization between different “Service Layer” standards and the emerging 3GPP Service APIs.

7. References

[1] 3GPP TS 36.300 Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2.

[2] Worldwide Business Use Smartphone 2014–2018 Forecast and Analysis, IDC #249178, June 2014;

[3] Worldwide Mobile Enterprise Management Software 2013-2017 Forecast and 2012 Vendor Shares, IDC #241650, June 2013

[4] https://www.5g-acia.org/

[5] https://sites.atis.org/insights/atis-and-cbrs-alliance-collaborate-to-advance-use-of-cbrs-spectrum/

[6] 5G Network Slicing for Vertical Industries, GSA, September 2017

[7] The Private LTE Opportunity for Industrial and Commercial IoT, Harbor Research, July 2017

[8] CBRS-Network-Service-Technical-Specification-1001 V1.0, CBRS Alliance, February 2018