5G IoT Private & Dedicated Networks for Industry 4.0

A guide to private and dedicated 5G networks for manufacturing, production and supply chains

October 2020

Table of Contents

Introduction

The Internet of Things (IoT) continues to expand into ever more areas of business, and where once the main focus of mobile networks was in direct to consumer services there is an increasing recognition that mobile networks can now be used more widely for specialised enterprise services, particularly when delivered alongside capabilities such as IoT monitoring, big data, artificial intelligence and edge computing. Indeed, it is estimated by GSMA Intelligence that enterprise applications will utilise 54% of cellular IoT connections by 2025.

In Industry 4.0[1] deployments, mobile networks are becoming established as the superior platform for 'wire-free' networking in applications from factory floor automation through to automated warehousing, logistics, autonomous vehicle deployments in campus environments, mining, materials processing and more. A deployment option of increasing interest to many industrial enterprises is that of mobile 'private networks'; that is, mobile networks that are for the exclusive use of that particular enterprise where all the devices operating on the network are part of a closed network community. Nokia, for example, in February 2020 announced 130 large industrial enterprise customers for such private mobile networks[2], and GSMA Intelligence forecast that between 25% and 40% of small/medium enterprises and corporates could be served via private mobile networks between 2023 and 2025[3].

The introduction of 5G networks and capabilities support the delivery of private and dedicated networks[4] even more effectively, building upon the successes of enterprises which have deployed such networks using 4G LTE. Mobile operators including DT, Telefonica and Vodafone are also responding to the breadth of requirements by offering '**hybrid**' 5G network solutions that offer flexibility by incorporating both public and private networks to suit the full range of needs of industrial enterprises.

Private and dedicated mobile networks can help meet industrial enterprise key business drivers, such as:

- **Minimising production line downtime** by use of a **highly reliable, highly scalable network with SLAs** from the mobile network operator covering uptime and availability;
- **Enabling manufacturing flexibility** by supporting reliable high-bandwidth wireless connectivity and capacity across the industrial campus;
- **Monitoring and management of goods and supplies** across the supply chain;
- Enabling **high reliability, critical monitoring and control applications** in primary production industries including mining, oil extraction, quarrying and refining industries**;**
- **Maximising productivity and manufacturing output quality** by the mobile network delivering **guaranteed bandwidth** to support key use cases including high resolution machine imaging;
- Supporting **real-time decision** making using locally deployed **edge processing capabilities** along with local **ultra-low latency** network infrastructure;

[1] The 'fourth' industrial revolution combines smart technology including sensors, high interconnectivity, automation, machine learning and real-time processing into traditional manufacturing and industrial platforms and the manufacturing supply chain. This industrial application of the Internet of Things allows manufacturers to analyse and improve productivity, manufacturing flexibility and product quality.

[2] https://www.nokia.com/about-us/news/releases/2020/02/27/nokia-deploys-5g-private-wireless-network-for-lufthansa-technik-virtual-inspection-trial/

[3] https://data.gsmaintelligence.com/research/research/research-2020/radar-june-2020

[4] Described later, 'dedicated networks' provide specific resource from the public mobile network for the enterprise through features such as 5G network slicing

- Achieving networking cost effectiveness for the manufacturer with **flexibility around capital expenditure (capex) versus operational expenditure (opex)** spend;
- Allowing the manufacturer **to focus on their core business** by **decoupling operation and management of the network** to the mobile network operator whilst still receiving **dedicated network resources** and **strict data isolation**;
- **Protecting IT and operational networks** against the cost and disruption of security and privacy threats through the advanced security features of 5G and the expertise of the mobile network operator;
- **Improving safety of workers and facilities** through the ability to implement specific safety use cases based on **high bandwidth** transmission of video imagery, **precision location positioning** and/or **high reliability communications**.

Figure 1 below shows that 5G introduces a range of possibilities between a public network and a fully standalone private network. For example, it is possible to **dedicate** resources on the public network to a particular enterprise using 5G '**network slicing**' to create a form of virtualised private network or for an operator to sublease their spectrum to enable a third party to build and manage a private network. Indeed, an industrial enterprise may adopt more than one of these deployment models in order to meet the varying needs of their use cases and applications, both on and off their premises. Similarly, Mobile Network Operators are increasingly offering a range of solutions from public networks through to standalone private networks, and in some cases as mentioned earlier a '**hybrid**' solution is offered which supports both public and private access. Therefore, this document addresses the range of options available to enterprises and also introduces the term '**dedicated network**' to describe models where public network resources are reserved for the sole use of the enterprise, for example by the use of network slicing.

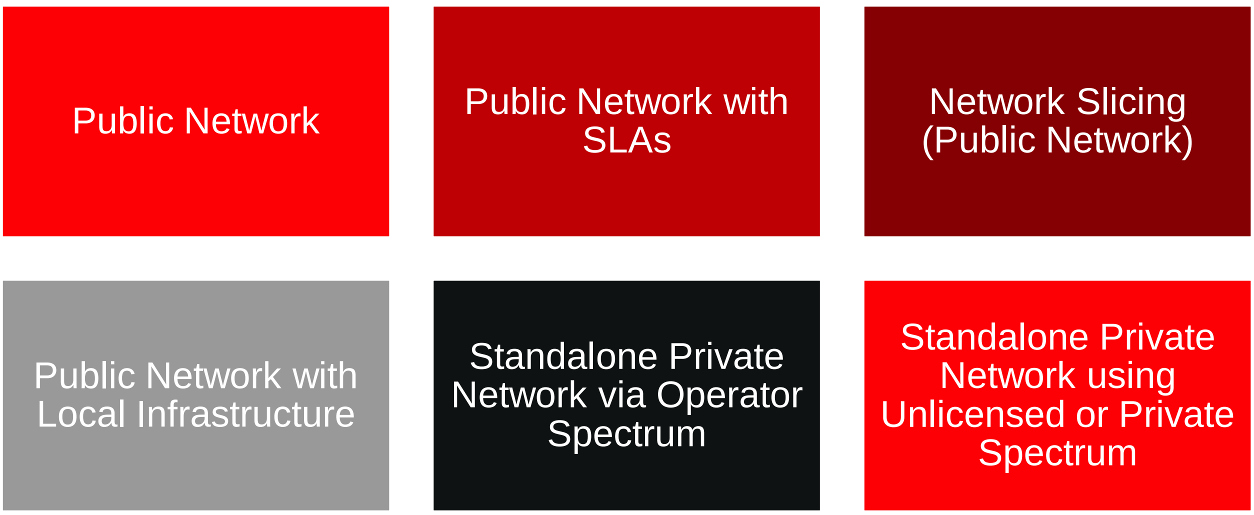


Figure 1. The range of options for manufacturing/ production/ supply chain enterprises from Public Networks through to Private/ Dedicated Networks

This document particularly concentrates on the application of private and dedicated 5G networks to the Internet of Things in manufacturing/production and the accompanying supply chain. It looks firstly at private and dedicated networks and their benefits, reviews a selection of use cases that benefit from these networks, outlines the range of public, dedicated and private network options available to enterprises, overviews key new features within 5G that make these networks work better for industrial applications and overviews important topics in security and spectrum.

What are private and dedicated networks?

Simply, a private (mobile) network is where network infrastructure is used exclusively by devices authorised by the end user organisation. Typically, this infrastructure is deployed in one or more specific locations which are owned or occupied by the end user organisation. Devices which are registered on public mobile networks will not work on the private network except where specifically authorised. Formally[5] these are known as 'non-public networks' however the term private network is more commonly used across vertical industries.

Such a private mobile network only serves the devices assigned by the end user organisation which means there is no concern about the impact of public users on the number of devices that can be connected, or, the throughput obtained, or other network performance indicators. Coverage can also be delivered precisely where needed whether to outdoor locations such as port areas or mines, or indoor areas such as manufacturing production lines or warehousing. The functionality of a private network extends, however, beyond capacity and coverage into areas like tailored security measures and integration with other operational or business systems belonging to the industrial enterprise.

A virtualised private mobile network ('**dedicated network**') can also be provided to the industrial enterprise typically using 5G network slicing over the public mobile network. In this case the enterprise can obtain most of the advantages of a private network, but without the upfront cost or complexity involved to the enterprise in installing and operating on-site wireless infrastructure, and with the scope for one or more services to operate across the whole public mobile network operator footprint.

Mobile networks operate in specific dedicated frequency bands and these ensure higher reliability than available in widely shared unlicensed frequency bands such as those used for Wi-Fi networks[6]. In some countries, radio spectrum is being set aside for local/ industrial use including private networks but more generally it is expected that mobile network operators will offer private network solutions based on their own licensed spectrum. The spectrum licensed to mobile network operators is generally greater and this therefore supports higher bandwidth services for the industrial enterprise.

With suitable agreements and interworking it is also possible for devices belonging to a private network to be supported on the public mobile network. This allows the device to continue to function even where it moves outside of the geographical bounds of the private network, for example in wider area applications such as logistics. This can further extend to international roaming.

[5] 3GPP Standards define 'Non-public Networks' e.g. in the specification 3GPP TS 23.501 V16

[6] Limited, narrow frequency bands are commonly used for Wi-Fi in the 2.4 GHz and 5 GHz spectrum. Neighbouring networks or access points can interfere with Wi-Fi signals to make the network less reliable and reduce bandwidth. Other devices including microwave ovens and Bluetooth devices can also generate interference.

What are the benefits of 5G private and dedicated networks?

Private and dedicated networks delivered via 5G mobile technologies offer a wide range of benefits compared with other options including wired Ethernet or Wi-Fi or unlicensed wireless networks

- Private and dedicated 5G networks offer flexibility of device movement and deployment efficiency; it is costly and complicated to move cables and equipment around when reconfiguring wired Ethernet networks;
- Not all environments are suitable for wired connectivity whilst Wi-Fi and other unlicensed wireless technology networks do not always provide reliability at scale. Mobile private and dedicated networks can deliver required coverage and capacity with high quality and reliability through 5G 'Ultra Reliable, Low-Latency Communications';
- Strict security, privacy and data isolation requirements can be met particularly through the advanced range of features available with 5G network solutions;
- Autonomous guided vehicles need to have highly targeted, high bandwidth coverage, predictable error and delay characteristics, and device capacity to ensure efficiency and safety. These do not work well over Wi-Fi networks particularly when the network is congested or during 'handovers' between access points. 5G particularly delivers the required characteristics for AGV's operating in a campus over a private network or over wide areas over the public network;
- The enterprise has the means to determine how the mobile network is deployed for their specific situation – whether this is for capacity, coverage or associated aspects such as data privacy/ security or the required 'Service Level Agreement'. They can also engage the mobile operator to deliver key capabilities for example network design, deployment, operations and maintenance or sub-licensing of spectrum;
- Transmission latency can be reduced when local edge equipment is installed for the private or dedicated network as there is no longer a need to transmit 'user' data across sometimes large distances as is the case with earlier public mobile networks – particularly 2G & 3G. This enables 'real-time' or 'near real-time' services particularly with improvements delivered by 5G ultra-low latency services when used with edge computing;
- The transmission delay and error rate are highly predictable for 5G, allowing reliable software-based compensation to be applied. This is important for industrial and autonomous applications and contrasts highly with Wi-Fi networks where contention between devices is often an issue;
- Bandwidth can be delivered at scale to suit the needs of the enterprise without necessarily being dependent on the wider rollout plans of the public mobile network operator;
- Uplink/ downlink bandwidth ratios can be varied, utilising the new radio interface and Time Division Duplexing (TDD) technology in 5G, according to the enterprise use cases i.e. manufacturers do not have to be limited by network design choices relevant for public mobile network users[7]. This is relevant for use cases such as video image processing in factory automation or autonomous vehicles as the uplink bandwidth requirement can far exceed the downlink;
- 5G network slicing can be equally applicable to private networks to allow partitioning of devices and applications, this allows further enhancements to data security and containment especially with the deployment of on-site edge computing;

[7] The ability to fully tailor the ratios of uplink to downlink bandwidth may be governed by external factors including public mobile operators with network equipment operating in adjacent TDD bands. For more information on this see https://www.gsma.com/spectrum/resources/3-5-ghz-5g-tdd-synchronisation/

- Finally, time critical applications are enabled through the Time Synchronization Network (TSN) features available in 5G networks which support the integration of legacy Ethernet TSN networks.

Manufacturing 5G network use cases

The manufacturing vertical has a very wide range of use cases and requirements, ranging from those requiring the wide area service of the public mobile network to those which have more specific needs that are met by private and dedicated networks. The following are example use cases for manufacturing and the related supply chain where some manufacturers may elect to utilise private and dedicated networks to support a wider range of use cases than possible with wired or Wi-Fi enterprise networks:

- **Production line flexibility** is enabled using 5G private networks supporting the rapid reconfiguration of production lines to deliver new products. Fixed wire networking is difficult and costly to install and reconfigure and is impractical to install in certain environments. Wi-Fi networks have been used in some production facilities; however, these do not scale well for large facilities and for high bandwidth density use cases typical with Industry 4.0, and signal penetration can be an issue. 5G networks deliver massive increases in available bandwidth as well as facility wide coverage enabling the production line to have totally wire-free networking with sensors widely distributed across the manufacturing facility;
- **Machine to machine communications** are enabled so that an interconnected network of machines and sensors can collaboratively work to perform production tasks and optimally run complex processes. This enables, for example, applications such as robotics, "cobots"[8], autonomous production line quality optimisation, and smart warehousing and logistics. The 5G network enables high reliability and ultra-low latency, and network slicing implements secure virtual networking between devices;
- **Automated Guided Vehicles** (AGVs) benefit from the ultra-high bandwidth and reliable mobile handovers offered by 5G private networks across production line areas, warehousing and dispatch areas. As more of these use real-time sensors coupled with image and video processing for safety and improved efficiency the extremely high and reliable bandwidth available with 5G ensures AGVs can be used wherever needed throughout the manufacturing or warehousing facility as well as mines or shipyards;
- **'Connected Worker'** applications where machine operatives, supervisors and quality inspectors as well as maintenance and facilities staff can be provided with high bandwidth connectivity across the manufacturing facility or campus. Initial applications include the paperless shop floor, extending to connected tools such as screwdrivers and torque wrenches, and worker safety applications including personal safety monitoring and worker location tracking. Advanced use cases include Virtual Reality and Augmented Reality (VR/AR) for equipment set-up, manually assisted precision assembly, operative training and remote assistance to maintenance engineers. 5G ensures bandwidth is available everywhere needed across the facility/ campus;
- **End to end logistics** are supported across the production facility, the input supply chain, warehousing/ storage and the outgoing supply chain. 5G enables massive numbers of low-cost tracking devices to be deployed reporting both the location, status and environment relating to finished goods, parts, assemblies, and supplies. Seamless operation between

[8] "Collaborative robots" – where there is collaboration between humans and robots for performance of tasks such as remote inspection or maintenance

the private network environment and public 5G networks is also possible which especially benefits national and international logistics particularly for pallets, wagons and shipping containers;

- **Multi-client serving facilities** can offer clients 'private' sub-networks delivered from a common 5G infrastructure, enabled by 5G network slicing. This can be used in either production or warehousing facilities or campus environments. Network slicing can also extend to the public network offering seamless private network services between the production or warehousing facility and the national 5G network.

Those use cases, such as logistics or remote management, that require wide-area coverage tend to focus more on the isolation feature of provisioned network services and do not have particularly strict or extreme requirements on network performance in areas such as bandwidth or latency. In a wide-area coverage scenario, it is essential to serve devices over relatively general purpose, and shared network resources (especially radio access resources), with best-effort or Quality-of-Service prioritised network services.

In contrast the use cases such as critical production line management or AGVs which are focused at local area coverage tend to have more specific and challenging requirements, which may be very different from the conventional network requirements of consumer mobile services:

1. **High reliability service with guaranteed Service Level Agreement (SLA)**: An SLA is a commitment from a service provider to a customer in terms of provisioned network services. Network performance attributes such as latency, reliability, deterministic communication could be part of the technical specification of an SLA which is delivered using network slicing or dedicated private network equipment. Other than performance requirements, functional and operational requirements could be also specified in an SLA, e.g. high-precision positioning, real-time monitoring, etc.
2. **New traffic model**: the uplink and downlink traffic ratio for such use cases is very different from the conventional consumer mobile network services, and this may require a new uplink-to-downlink bandwidth ratio.
3. **Strict data isolation**: Some industrial customers are keen to keep their own data within their premises or infrastructure. Hence, strict data isolation is required, e.g. isolation of data between customers (if they share the same infrastructure) and communication service data related user plane / control plane. Edge computing along with network slicing supports the use cases where strict data isolation or localisation is necessary.
4. **Security & privacy:** A strong privacy and security framework is needed to protect industry data (e.g. related to production line and corresponding management & operation). The industry data should be only available for industry customers themselves and data and networks protected from various potential attacks.
5. **Decoupling of operation and management**: Many small- and medium-sized enterprises (SMEs) do not have sufficient technical expertise or resources for network design, deployment and operation. Hence, obtaining these services from mobile network operators, will be the most cost-effective way for such enterprises to focus on their core business and offload the complexity of deploying and managing enterprise connectivity.

Deploying a private/ dedicated network

As outlined in the introduction there are a number of ways for enterprises to realise the benefits of 5G networks ranging from those enterprises which will utilise dedicated services of public networks, through to standalone private networks built in conjunction with, or totally isolated from a mobile network operator. The decision will ultimately depend on the preferred balance between capital expenditure (capex) and operational expenditure (opex), the willingness and capability of the enterprise to take on the various tasks involved in setting up and running a mobile network and associated solutions such as edge computing as well as the availability of spectrum to support required use cases.

As shown, in Figure 2 below, there are a wide range of examples of different 5G network options being deployed for industrial customers. This figure references network deployment examples that follow in Table 7 as well as additional reading items in Table 8 with categorisation based on available public information.

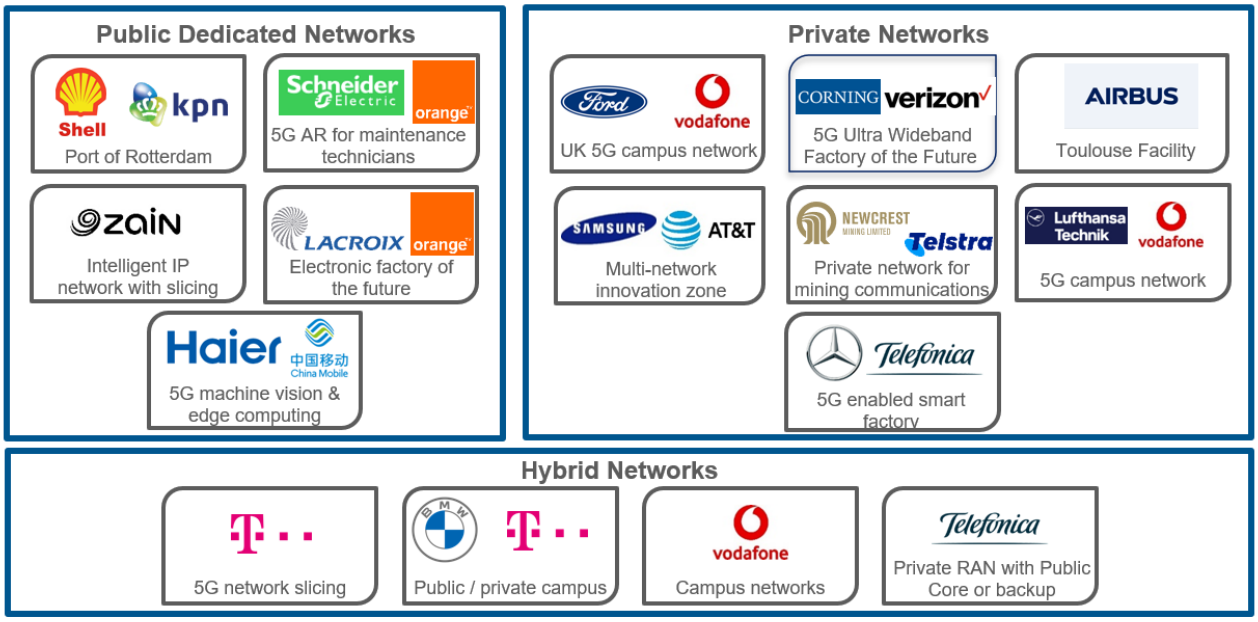


Figure 2. Examples of different 5G / manufacturing deployment models

Given the range of activities involved in implementing and operating a private network the preferred option for many industrial enterprises will be networks delivered as a managed service from one of the mobile network operators in country. Mobile network operators can further deliver a seamless service between the private or dedicated network and their own public network as well as offering proven expertise in managing all aspects of network rollout and operation. The interworking with the public network offers clear benefits for logistics and supply chain management where vehicles, supplies or finished goods can be managed as they move nationally or internationally.

Deployment scenario	Main characteristics
General Public Network	• Wide area mobility for common devices & services • Efficient use of network infrastructure, spectrum & operations • “Standard” Service Level Objectives (SLOs) • Edge computing on the MNO edge within public network and optionally with on-site gateways offer lower latency and localised data storage/ processing
Public Network (with SLAs)	• Leverages mobile network operator expertise, solutions & wide range of spectrum portfolio with a superior level of customer support • Full provision from & interoperability with public network • Quality of Service improvements for prioritising critical devices and applications • Also enables edge computing on the MNO edge within public network and optionally with on-site gateways offer lower latency and localised data storage/ processing
Mobile Operator Network Slicing	• Leverages operator expertise, solutions & wide range of spectrum portfolio with customisation of network services using network slicing • Enables higher data isolation, security, privacy and further SLA customisation including availability and reliability • Full provision from & interoperability with public network • Edge computing on the MNO edge and working with network slice offers lower latency and localised data storage/ processing
Dedicated radio equipment installed & managed by MNO	• Managed service where operator installs & manages dedicated radio network equipment for manufacturer under an SLA • On-site edge computing gateways enable very low-latency and fully localised processing and data storage • Choices regarding control plane/ data plane management/ localisation (network slicing) • Interoperability enabled with public network for wide area service
Standalone Private Network (via operator spectrum)	• Dedicated network enabling high security, privacy & “dark sites” • Access to broad range of spectrum options via operator • Full control over design, deployment timeline and operation • Full control over SLA • Edge computing on the MNO or customer edge within private network offers lower latency and localised data storage/ processing • Optional outsourcing of some or all of design or management of network to MNO
Standalone Private Network	• Totally isolated network with no interworking with public mobile network • Direct responsibility for spectrum access & usage

(unlicensed or private spectrum)	• Full independence over design, procurement, service level, operation & maintenance, spectrum allocation, radio plan[9] • Optional outsourcing of some or all of design or management of network to MNO

Table 1. Typical deployment options for 5G networks

Within these various deployment options, network slicing and edge computing offer major advantages for manufacturers and the supply chain. As described earlier network slicing offers a 'virtual network' capability supporting bespoke manufacturing / supply chain attributes including Quality of Service, privacy, security and specific SLAs. This allows the industrial enterprise to benefit from a highly customised service that can be delivered from the public network without the cost or complexity of the enterprise installing their own network. Added to this edge computing offers multiple options in data localisation for lower latency, and containment of data for privacy and security reasons.

The mobile network operator can also deploy network equipment at the site or sites of the industrial enterprise. In this way coverage can be directed wherever needed, including deep in-building, as well as to other areas that public networks would not usually reach such as underground or open cast mining or offshore oil rigs. Capacity can also be delivered at extremely high levels as required by complex Industry 4.0 use cases, especially for image and video processing. Edge computing in this case also underpins ultra-low latency applications complementing 5G's Ultra-Reliable Low-Latency Communications service, as well as being able to fully localise data/control within the boundary of the enterprise.

Whichever model is deployed, there are several roles that must be considered when implementing a private or dedicated network, and these can be split across one or more entities. These roles are detailed further in Table 2, below.

Role	Responsibilities
Spectrum licensee	• Identifying availability of spectrum and whether it is able to meet the use case requirements • For licensed spectrum, securing rights to access spectrum including sign-up process and payment for initial license term and subsequent renewals • Complying with licence terms, conditions and obligations
Network owner	• Selecting, funding and purchasing the network equipment and related accessories including antennae, equipment racks and compute, storage and communications equipment • Purchases equipment/ accessory maintenance & upgrades • Purchases the applicable software stack and any related technology licenses

[9] The radio plan must consider interference to/ from adjacent users

Network architect	• Designs the logical and physical implementation of the network based on requirements for capacity & coverage • Identifies spectrum needed, recommended equipment types and location, and frequency reuse plan considering also external spectrum use in same and adjacent channels • Specifies edge computing equipment needed for industrial use cases
Operations and maintenance	• Routine operation of the network equipment, includes fault and performance monitoring, troubleshooting and simple fault resolution e.g. replacement of failing hardware modules, reconnection of severed communications links • Monitors delivered SLAs against requirements, reports to the end user organisation, and escalates if needed for resolution by others
Network controller	• Defines the service requirements for the private or dedicated network and the different types of devices/ machines that will be connected. This includes topics such as privacy, security, edge computing and interconnection to other networks, uplink & downlink bandwidth requirements • Ensure other parties know and fulfil their duties in delivering the private network
Network administrator	• Defines and manages access to the private or dedicated network in terms of devices/ machines which can connect, interconnection of servers/ PCs on other networks e.g. the IT network, and users of the private network • Also manages (or delegates) backup/ restore and security update processes for the private network equipment • Deploys and manages applicable software stacks including storage and computing resources • Directly provisions or deprovisions IoT devices where this is not automated or integrated into other authorization/ authentication systems
Network Integrator	• Deploy and integrate the private network within the enterprise network and facilities • End to end integration between devices, systems and applications as well as customer acceptance testing • Delivery of the solution to the customer, training, handover to the operation team and to network administration • Fulfilment of customer specific obligations e.g. security/ quality accreditations or other vertical specific certifications

Table 2. Principle roles involved in network deployment

5G features benefiting private and dedicated networks

Significant improvements are available for private and dedicated networks with the introduction of 5G networks, notably:

- Three new 5G 'standard' services are introduced which deliver specialised support for different industrial IoT applications
  - **mMTC –** Massive Machine-Type Communications
  - **URLLC** – Ultra-Reliable, Low-Latency Communications
  - **eMBB –** Enhanced Mobile Broadband
- The **5G radio interface has been redesigned** to allow multiple service types with different characteristics to **co-exist on the same radio channel**. For example, the above 5G standard services can simultaneously be delivered on the same radio channel but to different devices;
- In addition, a new capability called **'network slicing**' enables private and dedicated networks to have highly optimised characteristics tuned to the required industrial use cases or applications, this offers a form of 'virtual networking' with the added benefit of being able to customise specific characteristics e.g. uplink/ bandwidth ratio;
- **Edge computing[10]** provides the ability to interface industrial enterprise systems at the most local level possible to the mobile network (private or public) both to substantially reduce end to end transmission latency as well as to contain data within the bounds of the enterprise locality for information security and privacy reasons;[11]
- **Open networking** is increasingly viewed as a must-have for future network deployment and management, especially since this opens the ecosystem to advanced AI tools for building and operating the network. This new industry initiative, particularly relevant with 5G era network rollouts, is expected to provide manufacturing enterprises and mobile network operators with more choice and innovation for private and dedicated network deployments.

[10] Also known as multi-access edge computing or mobile edge computing
[11] See https://www.gsma.com/iot/wp-content/uploads/2018/11/IoT-Edge-Opportunities-c.pdf for further details.

Table 3, below, lists the specified International Telecommunication Union design goals for the three 'standard' 5G services[12].

Massive Machine-Type Communications (mMTC)	Ultra-Reliable Low Latency Communications (URLLC)	Enhanced Mobile Broadband (eMBB)
• Very high device density • Extended coverage range including deep in-building • Battery life extending to multiple years • Low data rate (1 to 100 k bits-per-second) • Variable (non-critical) latency • Limited mobility (particularly with NB-IoT) • Low device cost	• Under 1 milli-second air interface latency for small data packets • Ultra-reliable communications with 99.999% or better success rate • Low to medium data rates (50 k bits-per-second to 10 M bits-per-second) • Supports high speed mobility	• Supports at least 100 M bits-per-second user rates • Peak data rate of 10 to 20 G bits-per-second • High speed mobility of 500 km/h • Up to 15 Tbps/km^2 downlink and 2 Tbps/km^2 uplink area traffic capacity

Table 3. Comparison of ITU design goals for 5G services

Network Slicing

Network slicing is a new feature of 5G networks which allows particular customers or applications to have the network reserve resources for their sole use and deliver a range of performance attributes that is optimal for their needs. This is delivered by configuration of physical 5G infrastructure to provide a 'virtual' network delivering the same capabilities as if the customer or application had their own bespoke network.

With network slicing, the 'common' mobile network infrastructure is logically or physically configured to offer the required capabilities to the respective users/ applications. This is unlike what happens over 4G and earlier networks where users/ devices are essentially connected to a single network with common characteristics.[13] Multiple network slices, potentially delivering different network characteristics for different users or applications, can therefore share 5G networks.

[12] See https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf
[13] NB-IoT is arguably a little different as it is deployed in separate frequency bands ("guard bands") and having different characteristics therefore there is a degree of separation between IoT devices using NB-IoT and other mobile devices e.g. smartphones

For the industrial IOT this means that there is the ability to have a 'virtualised' network which optimises performance to the specifics of particular industrial use cases. For example

- Low latency network communications which might be required for near real-time control applications in manufacturing applications;
- Specific bandwidth availability such as high bandwidth suitable for conveying image data in AI/ Edge applications or low bandwidth for industrial measurement applications;
- Network or data reliability or other Quality of Service measures e.g. for industrial control applications knowing that a control command is guaranteed to be delivered across the network and with given communication characteristics, including privacy and security.

Massive Machine-Type Communications

mMTC or Massive Machine-Type Communications is the 5G solution to address mass market demands for IoT products and services. Subject to availability of spectrum this should mean that of the order of 1 million IoT devices can be connected per square kilometre of area. This suits a wide range of use cases across utilities, industrial and educational campuses, smart homes, smart cities, agriculture and transport and logistics.

mMTC connected devices in general will infrequently send or receive relatively small packets of data infrequently. This technology is therefore ideal for periodic sampling, or alerting of 'unusual' events such as

- Indicating manufacturing equipment failure;
- Sensing for pipelines or mining;
- Low frequency environmental sensing either within an industrial campus or across a wider geography;
- The opening, periodic location reporting or adverse condition detection of shipping containers;
- Warning that an emergency access door has been opened or closed;
- Use in smart energy management sensors or actuators including heating or lighting management.

Ultra-Reliable Low-Latency Communications

URLLC or Ultra Reliable Low Latency Communications is another key feature of 5G networks, expected to benefit a wide range of "mission critical" applications. On 4G networks the typical round-trip latency for radio transmission is around 15 milliseconds[14] with a typical end-to-end 'system' latency of some 30 to 100 milliseconds[15], but with 5G[16] the radio network latency reduces to 1 millisecond making it possible to deliver much more responsive 'real-time' control applications especially when edge computing is employed.

[14] See https://arxiv.org/pdf/1801.01270.pdf
[15] See https://arxiv.org/pdf/1704.05565v6.pdf and https://arxiv.org/pdf/1709.00560.pdf - overall latency is also dependent on the application performance
[16] Latency reductions are standardised in 3GPP Release 16 and Release 17, building on initial URLLC support in Release 15

Importantly 5G URLLC offers control applications a network reliability of 99.999% or better which enables high reliability 'real-time' control applications. This significantly improves on prior 4G networks with typical 99% reliability which is not sufficient for critical control applications.

Industry Vertical	Applications
Industrial/ manufacturing/ production	• Industrial equipment/ production line control • Control for both fixed and moving robots (including navigation/ collision avoidance) • Plant environment management • Safety monitoring & management
Automotive	• Driver safety assistance services – Vehicle to Vehicle & Vehicle to Infrastructure • Autonomous driving • Intelligent traffic management
Drones[17]	• Assisted navigation • Drone to drone communications for collision avoidance • 'Airspace' use optimisation including drone 'air gateways' and 'platooning'
Energy	• Fine control of power generation equipment • Grid demand management
Smart cities/ smart homes	• Fire alarms/ suppression • Access control / escape route monitoring & control

Table 4. Industrial use cases for 5G Ultra-Reliable, Low-Latency Communications

[17] See https://www.gsma.com/iot/connectedskies/

Enhanced Mobile Broadband

Bandwidth hungry applications benefit greatly from the much higher available downlink and uplink bandwidth available with 5G's Enhanced Mobile Broadband (eMBB).

eMBB delivers very high data rates across the 5G coverage footprint, with per-device usable downlink data rates of at least 100 mega bits-per-second over a typical dense urban environment. High performance is sustained across different coverage scenarios, as detailed below[18], with especially increased downlink (DL) and uplink (UL) bandwidth in indoor hotspot environments such as smart factories or industrial campuses:

Scenario	Experienced data rate (DL)	Experienced data rate (UL)	Area traffic capacity (DL)	Area traffic capacity (UL)
Urban	50 Mbps	25 Mbps	100 Gbps/km^2	50 Gbps/km^2
Rural	50 Mbps	25 Mbps	1 Gbps/km^2	500 Mbps/km^2
Indoor hotspot	1 Gbps	500 Mbps	15 Tbps/km^2	2 Tbps/km^2
Dense urban	300 Mbps	25 Mbps	750 Gbps/km^2	125 Gbps/km^2
High-speed vehicle	50 Mbps	25 Mbps	[100] Gbps/km^2	[50] Gbps/km^2

Table 5. Comparison of available data rates and capacities under different eMBB deployment scenarios

The following IoT applications benefit from the higher bandwidth available with 5G eMBB:

- Fixed or mobile CCTV monitoring systems;
- Production line imaging for quality inspection or robotics;
- Ultra-high rate 'real-time' electronic sensing, for example motor or actuator positioning, voltage or current monitoring;
- Precision farming;
- Drone based surveying;
- Autonomous vehicles including ultra-high-resolution mapping data downloads and guidance;
- Vehicle to vehicle applications such as ability to 'see-through' the vehicle in front;
- Remote maintenance worker assistance including virtual reality/ augmented reality;
- Remote healthcare;
- Logistics robots;
- Road or vehicle safety or security.

The latency over the air with 5G eMBB is also significantly lower than 4G LTE, this enables "nearer-real-time" data transmission and processing. On 4G LTE networks the typical latency is around 50 milli-seconds[19], and so the 4 milli-second latency of 5G eMBB offers an order of magnitude improvement.

This reduced latency enables quicker decision making for applications from industrial machine control to autonomous warehousing robots.

[18] See https://www.gsma.com/futurenetworks/wp-content/uploads/2019/03/5G-Implementation-Guidelines-NSA-Option-3-v2.1.pdf, Table 2

[19] Based on https://www.digitaltrends.com/mobile/5g-vs-4g/

Edge Computing

As the cloud moves closer to the edge of the network to transfer, store and process the large volumes of data generated by IoT devices with reduced latency, so enterprises will benefit from edge computing approaches being developed for public networks in the form of an "edge cloud"[20].

Multi-Access Edge Computing[21] (MEC) is a key enabler for Industry 4.0. In the context of IoT, the closeness of the data processing capability directly affects and increases the number of use cases that can be deployed. Having data processing capabilities on or close to the factory floor, combined with the low latency of 5G networks, means that very advanced services such as machine vision can be enabled and the ability to further automate complex processes becomes available. Edge computing more efficiently delivers localised data processing and storage, and the ability to isolate data for security, privacy or confidentiality reasons.

In a private or dedicated network context, it's important to consider whether the edge cloud should be built around a private or public cloud, and how this links with the network architecture deployed. The private or public architecture for edge cloud can be viewed in the same way as the private network itself. A private cloud requires dedicated infrastructure and management. A public or hybrid cloud will utilise best of breed elements from public cloud providers to enable edge functionality.

Private network / Private cloud: A completely isolated system with no external inputs or outputs, and all data processing completed and stored on site.

Hybrid network / hybrid cloud: Use of public cloud providers and public network providers to create a hybrid model where most data processing is completed on site on isolated edge infrastructure, but data can also be stored and accessed from a public network or cloud service for certain use cases e.g. logistics.

Public network / public cloud: Use of public edge agents and infrastructure to enable edge computing on either shared or dedicated infrastructure operated by the public mobile network operator. This makes use of resources of the public mobile network e.g. base station sites as well as regional, national or metropolitan data centres for edge infrastructure.

[20] Whereas cloud architectures typically centralise processing to servers operating on cloud infrastructure, with the edge cloud there is a migration of such processing nearer to or at the device edge, where the traffic is. This particularly benefits low latency applications.
[21] Also known as Mobile Edge Computing

	Private Edge Cloud	Hybrid Edge Cloud	Public Edge Cloud
Private Network	Fully isolated system with complete local control but expensive to build and operate	Local edge processing and storage may be isolated, but may also be stored or processed partially by cloud provider	All data processing and storage completed on cloud providers infrastructure
Hybrid Network	Allows a focus on data control and access, with dedicated communications only where needed	A very flexible model that allows dedicated network and cloud resources to be allocated precisely where needed, ensuring cost effectiveness	Allows flexibility in communications with dedicated network resources available to ensure quality of service, with the benefit of full cloud features
Public Network	For use when data security is of paramount importance, and a private network is not feasible for geographic or operational reasons	Will ensure that localised data storage and management can be isolated, even if wider integration is needed across multiple locations.	The most flexible and least costly model but with limited network QoS capabilities, and reliant on general features for data security, privacy controls and cloud capabilities.

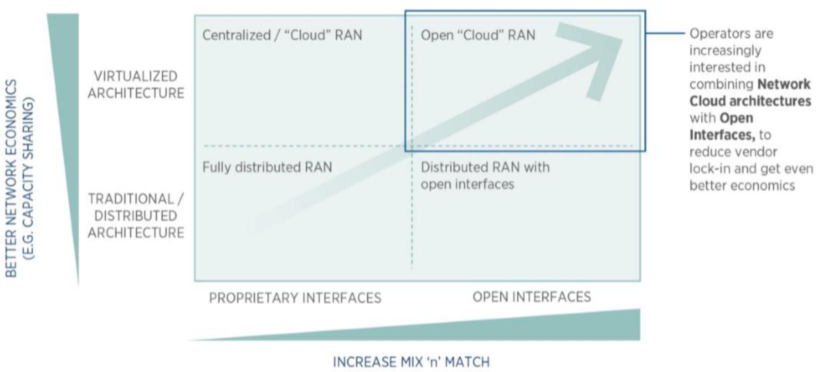
Table 6. Alternative applications of mobile edge computing

Open Networking

Open Networking creates the opportunity for Enterprises to seek Total Cost of Ownership (TCO) benefits from two architectural changes; Virtualization and Open Interfaces.

An enterprise can deploy one without the other, but technology is becoming available to combine RAN virtualization (centralisation) with open interfaces.

- ***Virtualization*** – For better economics through capacity aggregation or ‘cloudification’ in centralised architectures C-RAN or vRAN with an operator.
- ***Open interfaces –*** For more choice and innovation in the product of a network.



There are two modes in which an Enterprise can deploy an open network, taking advantage of localised private / hybrid / public coverage and capability (e.g. Edge Compute) and seamlessly be connected to a wide area network supported by a partner operator.

Plug and Play is where an Enterprise can deploy a dedicated network on its premise and at various open interfaces (e.g. Radio Access Network RAN or Core Network) can plug into an operators network for wide area coverage, with services (e.g. Edge Compute) and network management supported via a Network Slice and in the control of the Enterprise.

Mix and Match is where the network coverage (RAN) is deployed on the Enterprise premise or campus by the Enterprise and managed by the Operator, with bespoke local and wide area services (e.g. Compute) enabled via a Network Slice. The RAN vendor supporting Open RAN interfaces can be selected and owned by the Enterprise.

Enhancing security with 5G private and dedicated networks

Network security is a key consideration for industrial enterprises seeking to use 5G private or dedicated networks. Moving from wired connections, which have a level of physical protection, to wireless connections means that manufacturers have to consider new risks to their IT (Information Technology) and OT (Operational Technology) networks particularly from the larger number of connected devices that will form a potential attack surface. Mobile networks already have demonstrable security advantages over other wireless networks e.g. Wi-Fi, which are often poorly installed, configured or maintained. Further, new functionality to enable and isolate devices within a 5G private or dedicated network makes it possible to securely deploy a wider range of machines and sensors enabling Industry 4.0 use cases. For more information on the 5G security topics in this section see the GSMA publication "Securing the 5G Era" - https://www.gsma.com/security/securing-the-5g-era/.

SUBSCRIBER PROTECTION	RADIO PROTECTION	CORE PROTECTION
• Subscriber Permanent Identifier (SUPI); a unique identifier for the subscriber • Dual authentication and key agreement (AKA) • Anchor key is used to identify and authenticate UE. This key is used to create a secured access throughout the 5G infrastructure. • X509 certificates and PKI are used to protect various non UE devices	• Encryption keys are used to demonstrate the integrity of signalling data • Authentication when moving from 3GPP network to non 3GPP network • Security Anchor Function (SEAF) allows re-authentication of the UE when it moves between different access or serving networks	• The home network carries out the original authentication based on the home profile (home control) • Encryption keys will be based on IP network protocols and IPSec • Security Edge Protection Proxy (SEPP) protects the home network edge • 5G separates control and data plane traffic

Figure 3. Security controls outlined in 3GPP release 15

For industrial enterprises the 5G private or dedicated network will offer superior security to that typically achieved over private wired Ethernet or Wi-Fi networks because of the strong authorisation, authentication and access control features[22]. In particular:

- The 5G network uses **data encryption** and **integrity protection mechanisms** to protect the data transmitted by the enterprise, prevent information leakage, and enhance data security of the enterprise. Both **signalling plane and user plane traffic is encrypted and can be integrity protected,** leveraging the strong and well-proven security algorithms from 4G, namely encryption algorithms based on AES-CTR, SNOW 3G, and ZUC; and integrity algorithms based on AES-CMAC, SNOW 3G, and ZUC. The main key derivation function is based on the secure HMAC-SHA-256;
- 5G introduces a new network architecture element, the **Security Edge Protection Proxy** (SEPP). The SEPP **protects the home network edge, acting as the security gateway** on interconnections between the home network and visited networks so preventing data exchanged between networks from tampering or eavesdropping;
- A new **authentication framework** is introduced with 5G which allows the manufacturing enterprise to provide secure 'plug-in' device authentication procedures that work seamlessly for mobile and other networks. Importantly therefore this enables a manufacturing organisation to manage identity and access from its own protected IT systems;
- Proven **USIM/ eSIM technologies can also be used for authentication, authorisation and access control**, efficiently offering higher security than typical approaches using Wi-Fi keys or hardware ID (MAC address) controls;
- Improved **protection of device identity 'over-the-air'** including protection against false base stations. 5G networks use a combination of 'SUPI', a Subscription Permanent Identifier, and 'SUCI' a Subscription Concealed Identity to manage identity of devices or users. This combination provides **privacy preserving protection of device and user identity**, ensuring that the true identity cannot be stolen;
- A new **service-based architecture** is introduced, with network functions connected using **security protocols such as TLS 1.2** and above and OAuth 2.0 for application layer authorisation;
- **5G network slicing** can be used to create logically separated, virtual networks with the possibility of extension of the virtual network over the public network without reliance on additional encryption protocols such as PP2P, Ipsec or L2TP. Distinct slices can be defined for different types of devices, sub-networks or users to create distinct security perimeters;
- Adoption of **Software-Defined Network (SDN)/ Network Function Virtualisation (NFV)** in the architecture of 5G systems facilitates the **virtualisation of traditional security functions like firewalls, access authentication, SSL**, etc. These services can be deployed with increased flexibility, providing improved security as well as a user experience comparable to traditional networks. Furthermore, these virtualized security functions can be operated within the slice to meet the industrial enterprise requirements;
- Use of **Edge Computing** along with network slicing supports the ability to localise and isolate data traffic allowing information to be kept entirely within the premises. It is also possible to localise and isolate the 'control plane'[23] for enhanced protection of manufacturer networks from external attacks;

[22] It should be noted that there may be new solutions for 5G private networks which may have different authentication and security features so the security capabilities may vary between manufacturers.
[23] The control plane covers functions such as device access control and mobility management

- For **time critical applications** the 5G private network can be transparently integrated into one or more '**Time Sensitive Network**' bridges to safeguard time-sensitive communications from network attacks. This ensures correct ongoing operation of both the 5G network and time critical industrial devices and applications particularly benefiting use cases requiring 5G Ultra-Low Latency and Reliable Communications;
- Network management can be decoupled so that the manufacturing enterprise can outsource infrastructure management to a **mobile network operator** who can apply their **world class knowledge in monitoring and maintaining security** to the private network.

Aside from these 5G specific features the GSMA also supports best practice for IoT applications, devices and networks through initiatives such as IoT Security Guidelines and Assessments, and "IoT SAFE" which leverages the SIM card as a root of trust to protect IoT data. For more information see https://www.gsma.com/iot/iot-security/

Spectrum for 5G private and dedicated networks

The industrial applications for 5G described earlier are dependent on access to appropriate radio spectrum, a key consideration for any wireless technology. Many enterprises in manufacturing, production and supply chains have experience of using "unlicensed" Wi-Fi technologies to deliver limited scale wireless networks. Other enterprises have made use of 4G-based private networks. 4G can operate entirely in unlicensed spectrum or entirely in licensed spectrum, or a mixture of the two (e.g. through the 4G LTE technology of 'Licensed Assisted Access'). 5G, however, supports a much-expanded range of spectrum options especially across licensed frequency bands which support more diverse requirements.

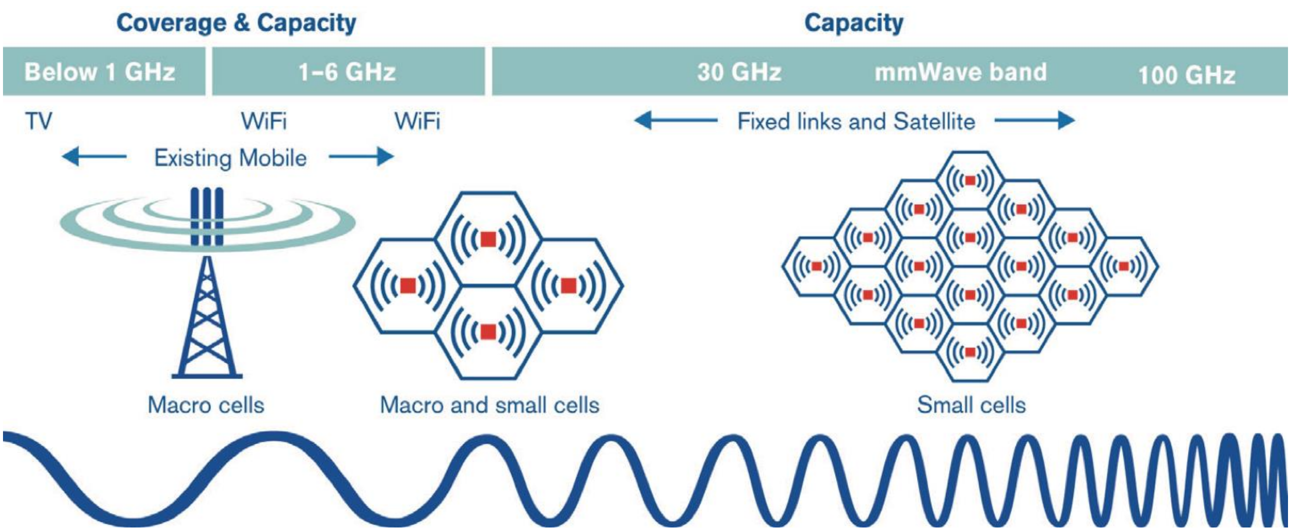


Figure 4. Spectrum ranges for 5G

Spectrum licensing and use will be an unfamiliar discipline to the majority of industrial enterprises. While regulators in some countries are setting aside distinct blocks of spectrum for local usage, which in practice can support Industry 4.0 applications for verticals, there is a need to think holistically about the needs of vertical networks as well as the public and businesses more widely. Setting aside licensed spectrum can have consequences for other consumer or enterprise users of mobile services and such set-aside spectrum may also be insufficient to meet the needs of many industrial verticals in terms of coverage, capacity, latency and uplink/downlink ratios[24]. The GSMA has considered in detail the subject of 5G spectrum approaches for delivering the optimum balance for industry and consumers in the public policy position paper "Mobile Networks for Industry Verticals: Spectrum Best Practice"[25]. This includes considerations for sub leasing mobile spectrum to verticals and considerations for limiting the impact local spectrum set-asides can have on 5G services more widely.

For their Industry 4.0 deployments manufacturers will also need to be aware of the conditions typically set by regulators regarding how this scarce resource can be used. While, for unlicensed spectrum, the considerations will be mainly around power (or more precisely electro-magnetic field limits) and interference issues from or to other users; for licensed spectrum, obligations are more complex and various criteria can be set by national regulators and these could be different across the countries where the manufacturer is operating. Regulators will typically require that licensees comply with various regulatory terms and conditions, including usage and coverage obligations, technical parameters such as electro-magnetic field limits and interference avoidance approaches. Mobile network operators have long running experience in dealing with such regulatory obligations and are expected to be a valued partner to industrial enterprises in complying with these operational obligations.

Mobile network operators themselves are expected to deliver 5G services using spectrum from three principal ranges to support the full range of manufacturing related use cases across local and wide area deployments. This will allow them to provide services to a broad range of vertical customers, including utility companies, manufacturers, logistics companies, mining and other primary producers and operators of ports and warehouses:

- Low frequency bands, e.g. under 1 GHz, supporting wide area coverage e.g. wide area logistics and sensor networks;
- Mid frequency bands, e.g. in the core 3.3 GHz to 3.8 GHz range, delivering expanded device capacity and bandwidth. It is expected that public mobile network operators will each have between 80 MHz and 100 MHz in prime 5G mid-bands;
- High frequency bands known as "millimetre wave", e.g. 26 GHz, 28 GHz and 40 GHz which enable maximum 'traffic volume densities'[26] to be delivered. This is of particular importance to streaming video, image/ video processing, virtual reality/ augmented reality, and more general wireless networking for flexible production lines, AGVs, machine vision and supply chain management. Mobile network operators should have at least 1 GHz of spectrum available each in the high frequency bands enabling those industrial use cases which demand peak 'traffic volume density'.

Where mobile network operators are involved in delivering private and dedicated network solutions, they will leverage their high, medium and low frequency range spectrum to support the

[24] Some applications like video cameras are uplink intensive and thus may be incompatible with other applications such as broadband downloads and low latencies and thus cannot be supported in the same TDD band in the same area. See https://www.gsma.com/spectrum/resources/3-5-ghz-5g-tdd-synchronisation/

[25] See https://www.gsma.com/spectrum/wp-content/uploads/2020/05/Mobile-Networks-for-Industry-Verticals.pdf

[26] I.e. net bandwidth available across all users per unit of area. See https://www.itu.int/en/ITU-D/Statistics/Documents/events/wtis2016/EGTI_Garba.pdf

various needs of manufacturing, industrial and supply chain customers. Mobile network operators can deliver private and dedicated networks comprising very small cells using millimetre wave bands for highest traffic volume density as well seamless handover on to 'macro' cells for wider coverage, this flexibility also provides advantages in addressing interference or jamming. The long-term experience of mobile network operators in site surveying, equipment selection and deployment and radio frequency optimisation will ensure industrial enterprises benefit from capacity, coverage and bandwidth optimised to suit their needs whilst eliminating the need for them to build new teams, processes and systems to roll out their own private networks.

Examples of private and dedicated network deployments

Table 7, below, contains summarised details and links to public examples of private and dedicated network solutions and deployments involving industrial end users and GSMA member companies

AT&T and Samsung have deployed a 5G testbed at Samsung's Austin manufacturing facility as part of a "5G Innovation Zone". This provides a private 5G network that uses millimeter-wave (mmWave) spectrum, and also leverages LTE and Wi-Fi. Additionally, the network uses multi-access edge computing, meaning that on-premises servers are connected to the 5G network. This solution enables training of new employees and direct workflow by using extended reality; the best trainer in the country can lead new employees on interactive training experiences. Other use cases include using a 5G connection to Austin's first responder network in case of emergencies, and sensors on factory equipment to monitor variables like temperature and humidity. https://www.lightreading.com/private-networks/inside-samsungs-5g-factory-for-atandt/d/d-id/757178
China Mobile, Huawei and Haier have completed a deployment of edge computing, 5G and machine vision into Haier’s manufacturing environment. With this solution top of the range stainless steel refrigerators are visually inspected, in near real-time, to screen out production defects. Edge computing is deployed to host machine vision applications, with all data processing on-site at the production facility. https://www.gsma.com/iot/wp-content/uploads/2020/02/Haier-Edge-Computing-Case-Study-final.pdf
China Mobile, and Yangquan Coal Group successfully built the first 5G underground coal mine network in China, which at 534 meters below the surface is also the deepest underground 5G network in China. With the help of this "super Gigabit uplink" underground network, supporting a peak uplink rate of 1100mbps, the network enables high-definition audio and video communication, rapid data transmission and remote intelligent control of equipment. This network enables three 5G applications together supporting unmanned, automated and remote

visual operation of the coal mine including inspection of mechanical and electrical chambers, autonomous driving and fully mechanized mining. http://en.sasac.gov.cn/2020/06/24/c_5145.htm
Deutsche Telekom installed a dual-slice private LTE 'campus network', hived off its public LTE network, at a BMW plant in Leipzig. Deutsche Telekom is working with Ericsson, for industrial LTE and 5G equipment, on a 5G dual-slice solution. This dual-slice architecture enables in-house industrial connectivity and regular mobile working supported on private and public slices, respectively, without interference in either case. https://enterpriseiotinsights.com/20200303/channels/news/dt-deploys-dual-slice-lte-for-bmw-promises-integration-with-private-5g-spectrum
Ford Motor Company and Vodafone Business are installing a 5G private mobile network at a new electric vehicle production site in the UK, in order to speed up the production of electric batteries. The aim is to reduce delays in manufacturing, increase bandwidth across the campus, improve security and reliability, and increase productivity. https://www.lightreading.com/5g/vodafone-partners-with-ford-to-deploy-private-5g-network-in-uk/d/d-id/761965
KPN, Shell, ABB, Huawei and ExRobotics have tested the first industrial 5G-applications in Rotterdam harbour in the Netherlands. Thanks to 5G mobile networks manufacturing can be optimised, industrial maintenance can be better predicted and safety further improved. By using Ultra High Definition (UHD)-cameras connected to 5G combined with machine learning algorithms, future maintenance can be better predicted. 5G technology is also used to give inspectors and engineers access to additional information from the process installation via tablets and the use of augmented reality. https://www.overons.kpn/en/news/2018/kpn-shell-and-partners-test-industrial-5g-applications-in-the-port-of-rotterdam
LACROIX Group, and Orange are entering into a joint innovation partnership to explore how 5G can be used within "Symbiose", the ground-breaking prototype factory project from the LACROIX Group. These trials will involve setting up an indoor network to test ambient connectivity on the industrial site or optimising production using automated vehicles and other vehicles connected through 5G. https://www.orange.com/en/Press-Room/press-releases/press-releases-2019/Orange-is-bringing-together-French-companies-to-test-and-develop-5G-uses
Lufthansa Technik and Vodafone Business have built a standalone private 5G campus network at the 8,500 square meters Lufthansa base at Hamburg Airport. This means Lufthansa Technik can now freely configure the network according to its needs, for example in relation to the upload and download speed of information required for its operations. Technicians can also use high-resolution virtual and augmented reality technologies to work even more precisely on the aircraft

fuselages. As part of the private network, sensitive data is completely secured, as it does not leave the aircraft hangar. https://www.vodafone.com/business/news-and-insights/company-news/lufthansa-technik-and-vodafone-business-launch-5g-private-network
Mercedes-Benz Cars is putting in place the world's first 5G mobile network for automobile production in its "Factory 56" in Sindelfingen, Germany. The 5G network has been installed by telecommunications company Telefónica Deutschland in collaboration with network supplier Ericsson. The use of 5G network technology allows Mercedes-Benz Cars, among other things, to optimise existing production processes such as data linking or product tracking on the assembly line. The 5G mobile communications standard allows fast data transmission rates in the gigabit range, with extremely low latency and a high level of reliability. And with a separate dedicated network, all processes can be optimised and made more robust, and if necessary adapted at short notice to prevailing market requirements. https://5globalnews.com/telefonica-and-mercedes-benz-to-build-a-5g-factory/
Nokia, NTT DOCOMO, INC. and OMRON Corporation have agreed to conduct joint field trials using 5G at their plants and other production sites. This aims to establish the feasibility of a layout-free production line using Autonomous Mobile Robots (AMRs). As product cycles become shorter due to fast-changing consumer demands, manufacturing sites are under increasing pressure to rearrange production lines at short notice. By taking advantage of 5G's high speed, large capacity, low latency and ability to connect multiple devices, the solution will see AMRs automatically conveying components to the exact spot where they are required based on communication with production line equipment. https://www.nokia.com/about-us/news/releases/2019/09/10/nokia-ntt-docomo-and-omron-bring-5g-to-the-factory-floor-in-industry-40-trial/
OSRAM and Deutsche Telekom are prototyping and testing a mobile robotics solution based on LTE as part of a 'dual-slice' solution which provides dedicated indoor factory coverage along with a local core network. Automated Guided Vehicles (AGV) will be used to transport goods across the OSRAM shop floor to support a more flexible production environment. https://www.ericsson.com/en/news/2018/11/deutsche-telekom-and-ericsson-partner-to-provide-industry-solution-for-osram s
Schneider Electric, a leader in the digital transformation of energy management and automated processes, and Orange are working together to evaluate the feasibility of opportunities brought by 5G in industrial production processes. From the end of 2019, an initial test will assess the value of 5G for real-time augmented reality solutions used by maintenance technicians at the Schneider Electric factory in Vaudreuil. https://www.orange.com/en/Press-Room/press-releases/press-releases-2019/Orange-is-bringing-together-French-companies-to-test-and-develop-5G-uses

Telstra Mining Services, and Newcrest implemented Papua New Guinea’s first private 4G LTE mobile network at Newcrest’s Lihir gold mine. Telstra worked with Newcrest to provide design, staging, site deployment and testing of the network supporting greater levels of safety, remote operation and automation. Every kind of production vehicle asset, including trucks, drills, excavators, dozers, shovels and barges has been connected and operationally proven over LTE. This provided significant performance improvements in terms of reliability, speed and latency. The network has been able to resolve challenges with existing Wi-Fi connectivity and is making Newcrest’s safety and productivity systems more effective. https://www.telstra.com.au/aboutus/media/media-releases/Newcrest_turns_digital_mining_future_Lihir
Verizon 5G Ultra-Wideband is being used at the Corning factory in Hickory North Carolina where the companies are working together to build the 5G factory of the future. The network is being used prove how 5G can enhance functions such as factory automation and quality assurance in one of the largest fibre optic cable manufacturing facilities in the world. Engineers from Verizon and Corning can use 5G to dramatically speed data collection, allow machines to communicate with each other in near real time, and wirelessly track and inspect inventory using 5G-connected cameras. They’ll also test how 5G can improve the function of autonomous guided vehicles (AGVs) by helping them move more efficiently around the factory floor. https://www.verizon.com/about/news/verizon-corning-co-innovating-5g

Table 7. Private and dedicated network deployment examples

Conclusions & next steps

As covered through this document 5G private and dedicated networks are a key approach to enable industrial verticals, and, provide infrastructure support for intelligent upgrading of complex environments such as deep wells and smart ports.

Private networks have already become established based on 4G LTE networks and it is expected this trend will grow dramatically with the improved feature set, and expanded bandwidth available on 5G networks. As seen in the deployment examples referenced MNOs are able to offer a wide range of solutions to industrial customers including 5G virtual networking for point-to-point connections, 5G private networks that cover a certain area, 5G+cloud, where vertical industry applications are deployed on the public cloud and connected through the 5G network and 5G edge computing for ultra-low latency processing and data/ processing localisation.

It is expected that for the majority of private and dedicated network deployments these will in some way involve mobile network operators. The reasons for this are various including

- Access to wider spectrum to support higher bandwidth use cases or device densities;
- The support for certain use cases which require network access outside of the confines of the industrial campus with service continuing onto the public network;
- Availability of relevant experts necessary to design, implement or operate the private/ dedicated network;

- The level of investment necessary to establish an enterprise owned private network.

Finally, manufacturers and the wider industrial sectors are encouraged to join the GSMA's 5G IoT for Manufacturing Forum. This forum is designed to bring together manufacturing industry, mobile network operators, equipment and device vendors and other ecosystem partners to encourage adoption of 5G private and dedicated networks across the manufacturing vertical. For more information see https://www.gsma.com/iot/manufacturing/

Additional reading

The following are additional sources of useful information about 5G and industrial applications

GSMA "The 5G Guide" https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf
GSMA "An Introduction to Network Slicing" https://www.gsma.com/futurenetworks/resources/an-introduction-to-network-slicing-2/
GSMA Security guide "Securing the 5G Era" https://www.gsma.com/security/securing-the-5g-era/
GSMA Spectrum white paper "TDD synchronisation in the 3.5 GHz range" https://www.gsma.com/spectrum/resources/3-5-ghz-5g-tdd-synchronisation/
5G-ACIA "5G Non-Public Networks for Industrial Scenarios (White Paper)" https://www.5g-acia.org/publications/5g-non-public-networks-for-industrial-scenarios-white-paper/
5G-ACIA "Security Aspects of 5G for Industrial Networks" https://www.5g-acia.org/publications/security-aspects-of-5g-for-industrial-networks/
Deutsche Telekom 5G network slicing

https://www.telekom.com/en/company/details/network-slicing-485776
ENISA European Union Agency for Cybersecurity "Good Practices for Security of IoT – Secure Software Development Lifecycle" https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
Ericsson and Finnish mobile network operator Elisa private network solution https://www.ericsson.com/en/news/2019/8/ericsson-and-elisa-pilot-private-networks-in-finland
Orange 5G Network Slicing https://www.orange-business.com/en/magazine/5g-network-slicing-can-drive-industry-40
T-Systems smart factory/ 5G campus network https://www.t-systems.com/gb/en/connectivity/5g-campus-networks
Telefonica 5G campus networks https://www.telefonica.de/news/press-releases-telefonica-germany/2020/03/5g-campus-in-berlin-basecamp-telefonica-deutschland-invites-the-public-to-try-out-5g.html
Vodafone (Germany) campus network solutions ("RedBox") https://www.vodafone.de/business/loesungen/campus-netz.html
Zain 5G network / improved service level agreements https://www.cio.com/article/3534020/zain-upgrades-5g-network-for-enterprise-service-level-agreements.html

Table 8. Additional reading

About the GSMA Internet of Things

The GSMA's Internet of Things is an industry initiative to help operators add value and accelerate the delivery of new connected devices and services in the IoT. This is to be achieved by industry collaboration, appropriate regulation, optimising networks as well as developing key enablers to support the growth of the IoT in the longer term. Our vision is to enable the IoT, a world in which consumers and businesses enjoy rich new services, connected by an intelligent and secure mobile network.

For more information, visit gsma.com/iot or follow gsma.at/iot.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com