5G Private Networks for Maritime Use

Opportunities for Digital Port Automation

Sponsored by:

MFA™

beecham research

Shaping the IoT future

A study conducted by Beecham Research on behalf of the MulteFire Alliance (MFA) confirms that 5G Private Networks (5G PNs) operating in unlicensed spectrum now offer significant opportunities for port automation in the Maritime sector.

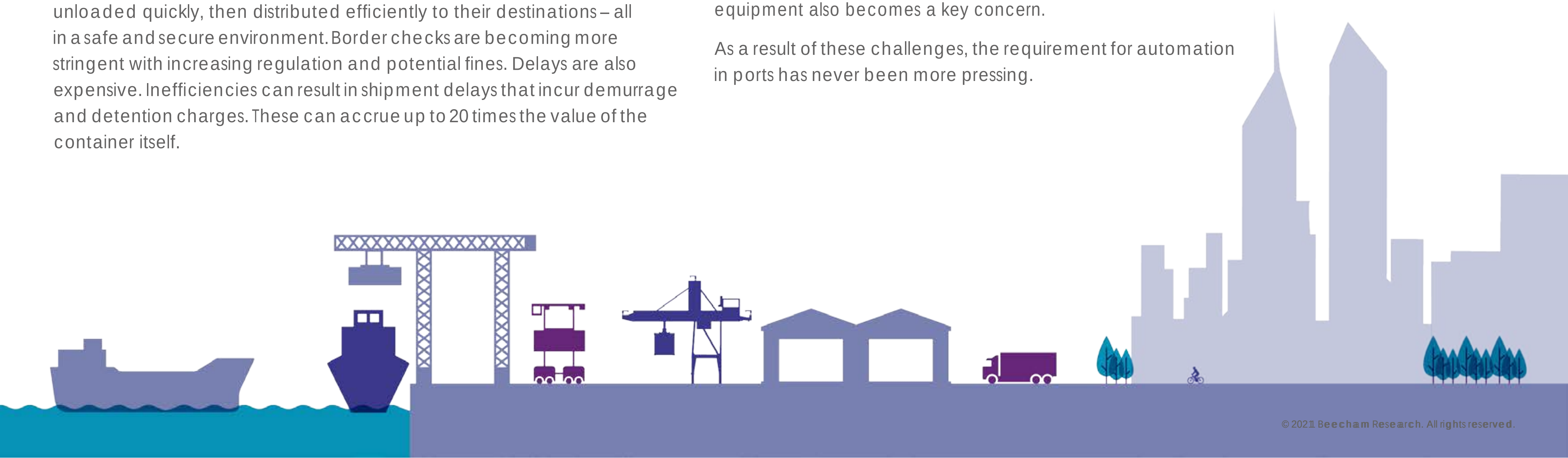
The enabling wireless technology is 5G NR (New Radio), which is the global standard for 5G networks. 5G NR-U, also part of the same 3GPP standard at Release 16 which was finalised in July 2020, enables the advanced features of 5G NR to operate in unlicensed spectrum. This combines the high performance and security benefits of 5G with the simplicity and low cost associated with Wi-Fi.

The need for port automation

Ports are challenging environments. Container shipping has to grow to keep up with demands in consumer and industrial trade and to accommodate the rapidly increasing size and capacity of huge vessels, but with limited port space. Time in port is of the essence. Cargoes must be loaded and unloaded quickly, then distributed efficiently to their destinations – all in a safe and secure environment. Border checks are becoming more stringent with increasing regulation and potential fines. Delays are also expensive. Inefficiencies can result in shipment delays that incur demurrage and detention charges. These can accrue up to 20 times the value of the container itself.

A related challenge is the need to minimise congestion within the port area, which not only creates inefficiencies, but also has an environmental impact. As more and larger vessels and trucks need access to a limited space the safety of staff whose work involves heavy cargoes and dangerous equipment also becomes a key concern.

As a result of these challenges, the requirement for automation in ports has never been more pressing.



The need for connected data in real time

At the root of automation is the need for huge volumes of timely data, used to control and monitor all of the moving assets. To provide that data reliably, cost-effectively and securely points to wireless connectivity as the only option.

Which wireless technology to use? Wi-Fi is simple to operate and low cost but ports are very large physical areas and the wireless coverage is required everywhere on site. Wi-Fi is a short-range technology so that means a very large number of Wi-Fi access points are required, all of which must in turn be connected and synchronised. In addition to that, Wi-Fi is not fundamentally designed for collecting data from moving objects and vehicles. Neither does it operate effectively in adverse weather conditions – the range deteriorates markedly in rain for example. It is primarily intended for office use.

A much stronger alternative is cellular networks – designed for mobile use, highly secure, and with industrial grade reliability in all weathers. Yet the cost of a cellular network can be high. A public cellular network may not provide the site coverage required and will most likely not be optimised to the port operations. It may also introduce too much delay (latency) to the data being collected from moving assets. It will also be managed by the telco, not the local port operations management, introducing admin delays for operational changes that may need a fast response.

Another solution is a private cellular network operated by a telco in licensed spectrum. The wireless coverage can be optimised for the site and the number of access points required will be anything up to a tenth of those required for Wi-Fi. This may be partially managed by the port management but may also be expensive. From an ROI perspective, a telco may charge anything from $8 to $100 per device in a period (ARPU).

A lower cost and simpler option, but retaining the other benefits of cellular, is a private cellular network in unlicensed spectrum. Like Wi-Fi, the ARPU for that type of network is $0. Such a network is also entirely managed by the port management so that changes can be implemented quickly.

5G Industrial use study

To assess the connectivity requirements for port operations, Beecham Research conducted a study on behalf of the MFA that included interviewing operations managers responsible for port activities in different locations worldwide.

The findings from these are summarised in the table in **Figure 1.**

Figure 1. *Assessment of connectivity requirements for port applications*

Application	Data Rate	Latency	Site Area Coverage	Density (of devices)	Power Effi y (battery life)	Mission Critical Reliability	Need For Low Cost	Mobility	Indoor/ Outdoor
Crane Operation	High	Slow	Large	Medium	Low	High	Low	Low	Outdoor
Autonomous/Semiautonomous Vehicles (Cargo Moving)	High	Fast	Large	Medium	Low	High	Low	High	Both
Environmental Sensing	Low	Slow	Large	Large	High	Low	High	Low	Both
Docking Ship Communications	High	Fast	Large	Medium	Low	High	Low	Medium	Outdoor
Video (Surveilance)	High	Slow	Large	Large	Low	Low	Medium	Low	Both
Drone (Inspection)	High	Fast	Large	Small	High	Low	Medium	High	Outdoor
Operational Equipment Monitoring	Low	Slow	Large	Large	Low	High	Low	Medium	Both
Remote Control: Static Machines e.g. Cranes	High	Fast	Large	Medium	Low	High	Low	Low	Outdoor
Remote Control: Loading Bays	High	Fast	Large	Medium	Low	High	Low	Low	Outdoor
Robotics (Material Handling w/in Warehouses)	High	Fast	Large	Large	Low	High	Low	High	Indoor

Figure I shows a selection of IoT applications used in automated port operations in the left-hand column. These include use of Rubber-Tired Gantries (RTGs), Autonomous Guided Vehicles (AGVs) and Autonomous Mobile Robots (AMRs), together with a control centre managing the autonomous operations.

The connectivity requirements for these applications are featured across the top of each column – Data Rate, Latency, Site Coverage Area, etc.

For each of these requirements, interviewees were asked what their requirements were for each application. The entries in the matrix shown are the aggregated responses.

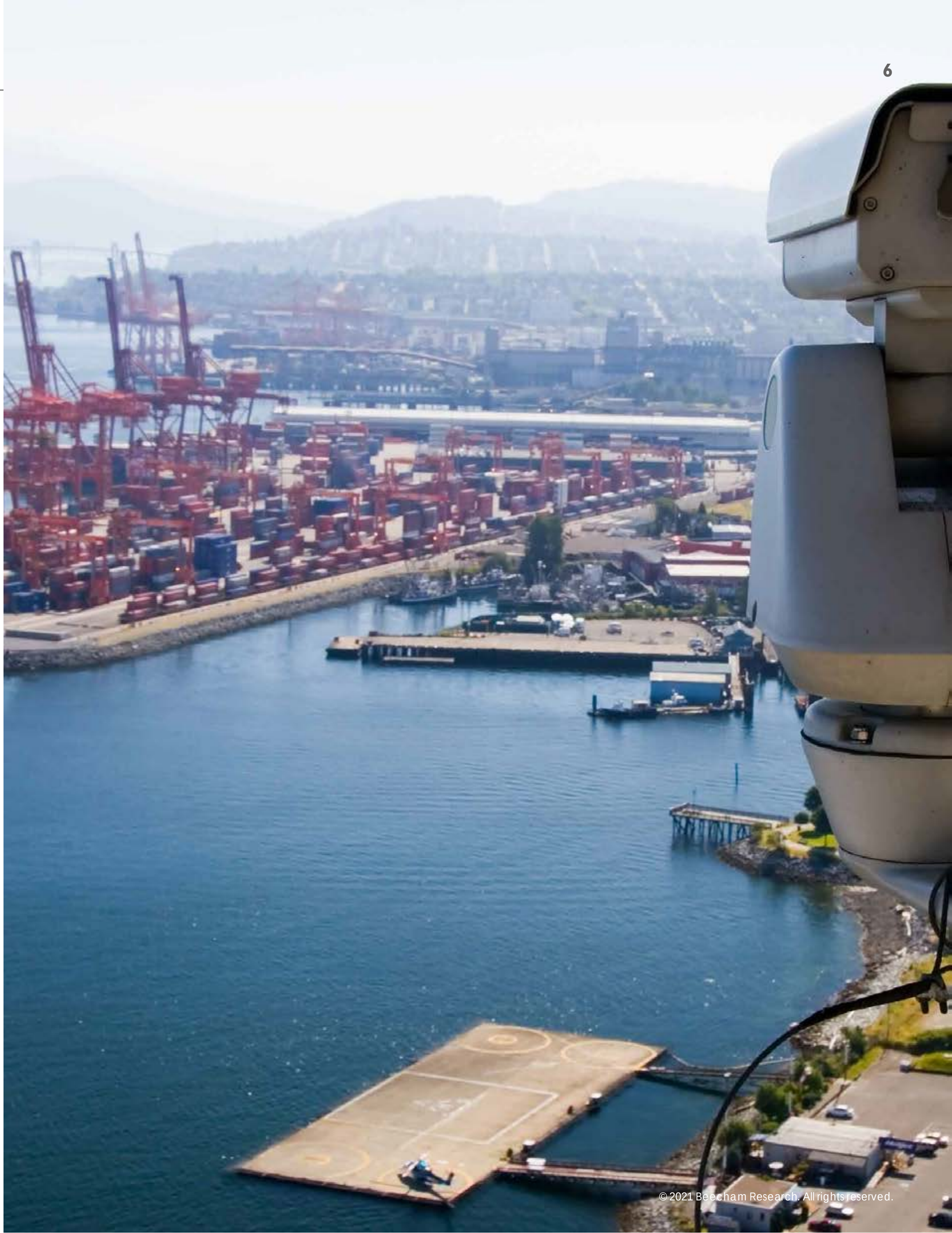
Figure 2 then provides a key to what these responses mean in technical terms. For example, a high data rate as required for Crane Operation is 250-500Mbps. This is needed in remote operation of a crane for high resolution video streams, with the crane operated remotely from the control centre.

Figure 2. Technical definitions of connectivity requirements

Sector Requirements	Low/Small/Slow/Sparse	Medium	High/Fast/Large/Dense
Data Rate	<10Mbps (avg mmTC dev UL 200b/DL 20b/day)	10-250Mbps	250-500Mbps
Site Area Coverage (F1) Distance Between Sites	<20m	20-250m	250-500m
Density of Devices	<100dev/Km2	100-1000dev/Km2	>1000dev/Km2
Power Efficiency (mm-Wave)	3 days	3 months	15 years
Mobility	0-3Km/h	3-50Km/h	>50Km/h

An increasing number of IoT applications involve near real-time data processing and today this functionality is also being deployed in container ports. Remote-controlled ship-to-shore cranes load and unload container ships, moving containers between the ship and the dock with precision. Automated guided vehicles navigate through ports using smart 3D sensors. They handle material flow efficiently and minimise the risk of accidents.

Automated rubber-tired gantry cranes stack containers at terminals. Drones are employed for surveillance and deliveries. They deliver documents from ship to shore, thereby reducing costs and environmental impact of manned boats, while also conducting security surveillance of ports. In addition, condition monitoring using machine vision technology can detect faults before they occur, reducing unplanned downtime and maximising productivity.



The study found that the connectivity requirements for connected port assets fits well within the three generic services for 5G and that therefore 5G NR-U can provide for a significant proportion if not all port automation connectivity requirements.

Automated ports need 5G NR-U's advanced communications performance to handle the huge quantity of data that is generated by cranes, vehicles, and other equipment as well as the automated systems. For example, operating machinery via a remote-control system relies on the transmission of a live video feed to a remote operations center. Therefore, a robust, high-bandwidth connection is required. In addition, remote control removes the need to climb up to the driver's cabin, which increases worker safety.

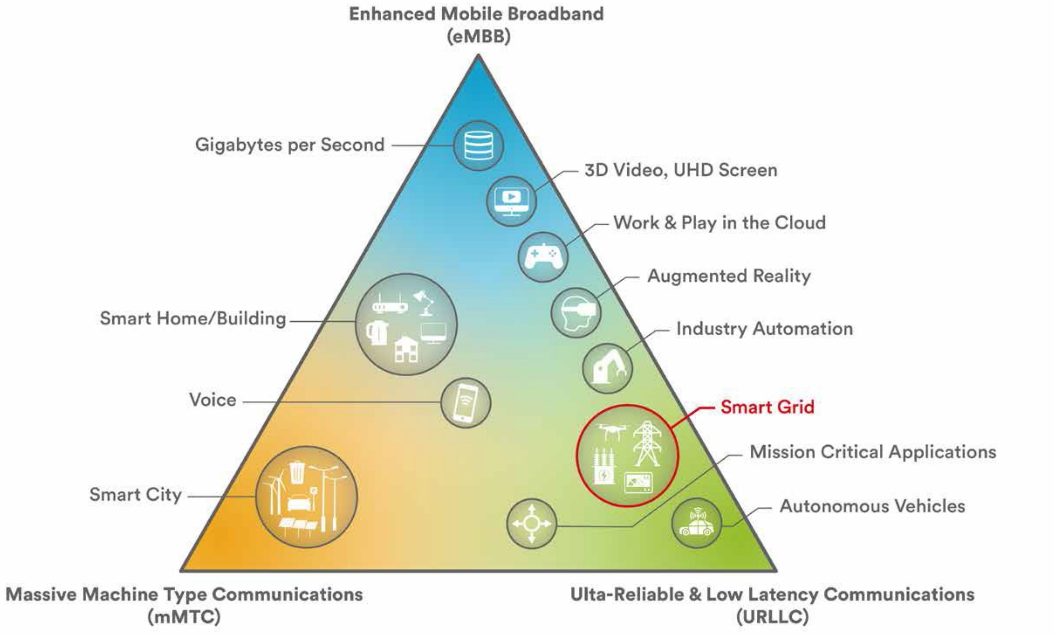
5G PNs provide state-of-the art connectivity. The technology, which is optimised for IoT applications, ensures low energy usage, enhanced data security, and the ability to support the high connection density of busy, automated ports.

About 5G generic services

5G has three generic network services. mMTC (massive Machine Type Communications), URLLC (Ultra-Reliable and Low Latency Communications) and enhanced Mobile Broadband (eMBB). mMTC defines the performance needed to support a very large number of devices in a small area. URLLC defines the latency and reliability for mission critical communications. eMBB targets data-driven use cases requiring high data rates across a wide coverage area. This indicates that the technology is intrinsically versatile, and it is robust because it represents a natural evolution of existing 4G services.

5G network slicing is associated with public networks, but it is equally applicable to private networks. Instead of allocating an equal distribution of network to each device, network slicing allows network bandwidth to be distributed based on priority. It allows vendors and customers to employ the network, but only provides discrete information relevant to each use case. Private 5G networks can therefore be customised, built to align with specific performance requirements, and data can be managed and analysed internally. They offer more robust security than a public network and are therefore a more attractive proposition for organisations that have very high security requirements such as ports.

Figure 3. *The three 5G generic services of eMBB, uRLLC and mMTC services, together with typical IoT applications they enable*



5G NR-U and Wi-Fi

5G NR-U is the first global cellular standard to not require licensed spectrum at all for a standalone mode of operation. NR-U offers mobility and the QoS provided by 5G NR. It includes LBT (Listen Before Talk) to ensure fair spectrum interworking if there is other traffic such as Wi-Fi on the same channel. This can impact on latency and time-sensitive networking (TSN) where the other traffic is significant.

This situation can be avoided in a typical port where there is a controlled network environment. The port authority can simply set aside one channel for NR-U use so that it is then quite separate from other traffic. Latency issues can then be avoided altogether.

Standards and spectrum

The big benefits of deploying a private network are predicated on the standard, in this case 5G NR-U, and the availability of unlicensed spectrum.

There is a plethora of cellular standards. 3GPP defines standards for 5G and it unites seven different telecommunications standards development organizations. 5G NR-U is the first global cellular standard to not require licensed spectrum at all for a standalone mode of operation. MFA's Uni5G technology blueprint is closely connected with 3GPP's 5G releases, in particular changes and additions made specifically for IoT use cases. The 5G NR-U standalone variation, which defines a mode of operation relying solely on unlicensed spectrum was proposed by members of the MFA.

Release 16 of the 5G NR-U standard enables operation on the already-available, unlicensed 5 GHz bands as well as the upcoming 6 GHz bands. 5 GHz unlicensed is already available worldwide and currently used mainly for Wi-Fi. 6 GHz unlicensed spectrum provides not only new bandwidth for unlicensed use, but also flexibility usage in both indoor and outdoor environments. In the U.S., the FCC has made a massive 1200 MHz of bandwidth available in this band for Wi-Fi and other unlicensed technologies such as 5G NR-U.

Momentum around 6 GHz is growing. Countries include the U.K., Chile, South Korea, and the UAE have released 6 GHz spectrum for unlicensed use. Brazil, Canada, Mexico, Peru, Taiwan, Japan, Saudi Arabia, Myanmar, and Jordan are among the other countries initiating similar developments.

A further point is that if any Wi-Fi required on site is instead using the 6 GHz band, with NR-U using 5 GHz, then any latency issue is also no longer relevant.

Other spectrum availability

Availability of wireless spectrum is country centric and therefore varies around the world according to local requirements. Availability of spectrum for private network use is developing as follows.

In Europe the prevailing trend is the availability of licenses in 3-4 GHz range. In Germany private 5G network licenses were awarded in the 3.7-3.8 GHz band. The UK regulator, Ofcom, has made local spectrum licenses available on a first-come-first-served basis.

There is some use in France of 2.6 GHz spectrum for private 4G although license fees are high. Other countries, including Belgium, Croatia, Finland, The Netherlands, Norway, Russia, Sweden, and Slovenia have plans to make unlicensed spectrum available.

The Asia-Pacific region has seen some movement. Japan opened up the 3GPP band 39 in October 2017 with a 5 MHz bandwidth, due to be increased to 40 MHz. Applications opened in November 2020 for several bands between 24.7 GHz and 30 GHz in Australia, while New Zealand awarded 80 private licenses in 2009 for the 2575-2620 MHz band. Other countries, including Malaysia, have indicated an intention to make private network spectrum available soon. China has not yet made unlicensed spectrum available.

In Latin America, Brazil's auction is expected to take place in the first half of 2021 for 2390-2400 MHz, 3800-3800 MHz and 27.5-27.9 GHz. Chile has designated 3750-3800 MHz as a band for private 5G networks.

Projected Use of 5G in Ports

Use of 5G NR and 5G NR-U is expected to grow quickly in the Maritime sector. A large port may typically have:

i. Millions of containers shipped in and out in a year
ii. Thousands of trucks delivering and removing loads daily
iii. Train operations daily
iv. Hundreds of staff on-site with communication requirements for voice and data
v. Potentially tens of thousands of sensors across the site
vi. Site covering tens of square kilometres
vii. Low hundreds of major port assets, including cranes, RTGs, AGVs, etc.

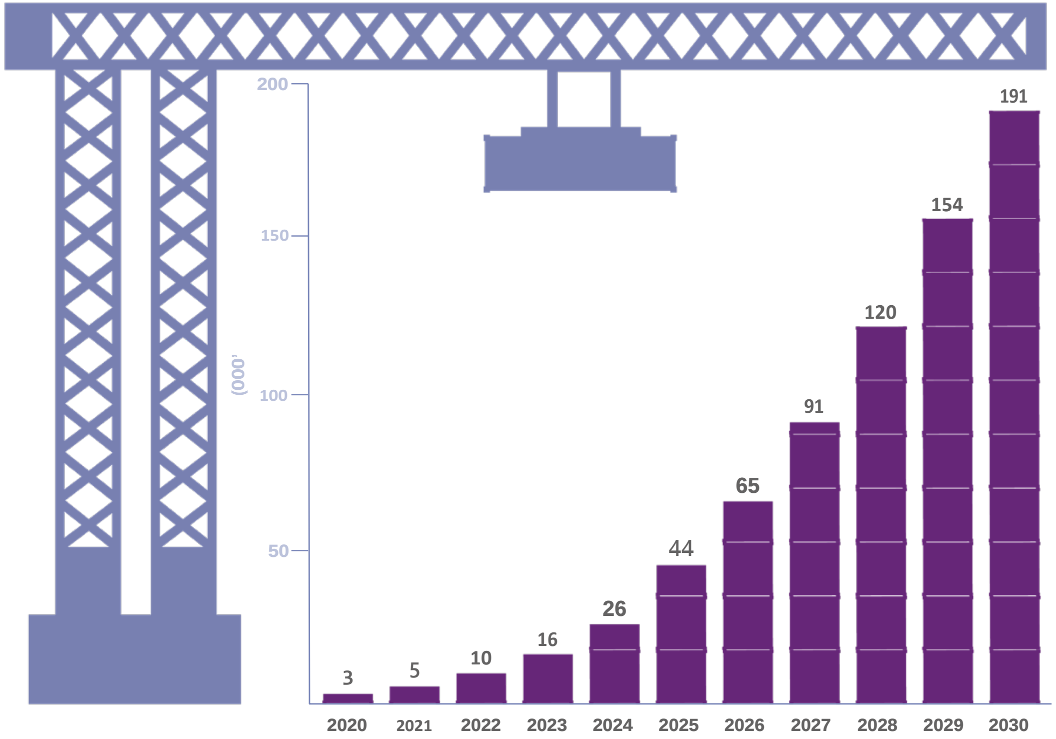
All of these can be supported with a 5G private network. Use of 5G across a large site provides a particularly cost-effective solution for achieving full site coverage, irrespective of weather conditions. Individual containers may need to be individually tracked and identified as they pass through the port. Similarly, trucks moving through the port are typically tracked while on site, with data also uploaded/downloaded for administration, authorisation, journey planning and truck maintenance purposes. In addition, large numbers of staff on site require voice and data communications at all times. Sensors measure and monitor environmental conditions, tracking of assets and security across the site.

In addition to all of these elements that need to be connected, the heart of the port automation system comprises the major port assets including cranes, mobile gantries and autonomous vehicles. All of these must also be connected to the port automation system, including the multiple video, remote control and positioning feeds attached to each of these assets so they can be controlled remotely. The projected growth of these connected large port assets globally is shown in **Figure 4.**

For a total number of 5G connections within ports, all other items (i) through (v) listed above must also be included.

This projection covers not only very large ports, but also medium-sized and smaller ports where automation is seen as beneficial. It shows a growth of 54% per annum to 2030, which is likely to be conservative. 5G PN use in ports is now moving beyond the trial stage. In addition, new releases of the 5G standard (3GPP Releases 17 and 18) will introduce further added value features relevant to port automation. For these and other reasons, use of 5G private networks in port automation is likely to accelerate faster than this projected rate.

Figure 4. *Projected growth of 5G Private Network Connected Major Port Assets*



Deployments

Even on large sites, a private cellular network equates to the deployment of a much smaller version of a public network. The hardware and software components are the same or very similar. They include small cells, which have small antennas that distribute the spectrum over the site. Routers and gateways will also be employed on large sites. A relatively new component is 5G Core, which is implemented in software and can run on a regular local server. The 5G Core aggregates data traffic from end devices, authenticates subscribers and devices and applies personalised policies. It replaces the 4G EPC (Evolved Packet Core).

In theory almost any organisation can set up and operate their own private 5G network. They just need spectrum, network infrastructure equipment, and edge devices that can connect to this equipment. However, in the case of ports this is clearly a task that will involve significant resources as well as experience.

This report does not advocate any specific deployment strategy, but various mainstream and specialist vendors have created generic networking and edge computing platforms and an ecosystem of compatible components. Nokia, for example, markets a Digital Automation Cloud (DAC) that combines plug-and-play connectivity with on-premises data management and processing to support real-time applications. The physical deployment would normally be done by a specialist system integrator that is an ecosystem channel partner. They should have the ability to drill down into the detailed requirements and determine the optimum locations of the small cells.

Use cases

One of the greatest challenges that ports face today is how they can evolve and adapt to become more efficient, competitive, and sustainable. With its low latency, high capacity, and enhanced flexibility, 5G can deliver enhanced process and operational efficiency that can significantly reduce costs, lower environmental impact, and boost economic value. For example:

The Port of Antwerp has signed an agreement with the city government and the Antwerp Fire Department to develop and test a private 5G network. The network is currently being developed and tested by technology company iSea in collaboration with Ericsson. The fire brigade, along with the police and the port, have developed a range of digital applications and having a faster, safer, and more reliable network will enhance the performance. In addition, the Ericsson Research team in Italy has leveraged enhanced connectivity at the Port of Livorno to carry out several leading-edge use cases that are documented in a Port of the Future report.

Nokia has announced an agreement with Tideworks Technology to deploy DAC at the Port of Seattle, Terminal 5. The operations include cranes, trucks, and lifts. Nokia DAC also incorporates ruggedised tablets and smartphones for terminal-wide, mobile voice communications and yard inventory applications. The company has also announced completion of the first phase of Port of Zeebrugge's 5G private wireless network deployment.

By deploying DAC the authority will be able to provide private wireless connectivity to more than 100 endpoints across the entire port. This will enable Zeebrugge to deliver a range of new and enhanced services that not only improve the port's operational performance, but which also differentiate Zeebrugge as a leader in port transformation and digitalization.

The MulteFire Alliance

The MFA (MulteFire Alliance) is an international organization that is championing the global industry adoption of private cellular networks using MFA-defined MulteFire specifications for LTE and Uni5G technology blueprints for 5G. With Uni5G or MulteFire, enterprises can efficiently deploy their own optimized, reliable, and secure private network in unlicensed, shared or locally licensed spectrum. For more information, visit www.mfa-tech.org.

MulteFire™

MulteFire is a 4G/LTE-based technology that operates standalone in unlicensed or shared spectrum, enabling industry verticals to deploy their own private wireless network with Wi-Fi-like deployment simplicity and LTE-like performance.

MFA deliverables:

- MFA global PLMN ID number for MulteFire (and 5G) private networks
- MulteFire End-to-End Specifications: Release 1.0, MulteFire Industrial Release, and Release 1.1
- MulteFire Certification Programs: MulteFire 1.0 and MulteFire 1.9 GHz (sXGP)
- MulteFire promotional, educational, and market research materials

Uni5G™

Uni5G is a technology blueprint that leverages 3GPP 5G standards to define profiling and classification requirements, enabling industry verticals to efficiently deploy their own optimized, reliable and secure private 5G network in unlicensed, shared, or locally licensed spectrum.

MFA deliverables:

- Uni5G Blueprints: Profiling and Classification
- Uni5G best practices and deployment guidelines
- Uni5G promotional, educational, and market research materials