5G Private Networking

Succeed with IoT

4G/5G Private Networking:

New Choices for IoT Deployment

beecham research

Shaping the IoT future

Proud to sponsor this important report on the rapidly-developing world of private cellular networking...

Contents

CLICK THE IMAGE TO GO STRAIGHT TO THAT SECTION

Introduction

Private cellular networks (PCNs) have come a long way in the last decade and are set to become increasingly crucial for business IoT operations over the next few years.
Why is that?

The rapid growth of cellular IoT in business

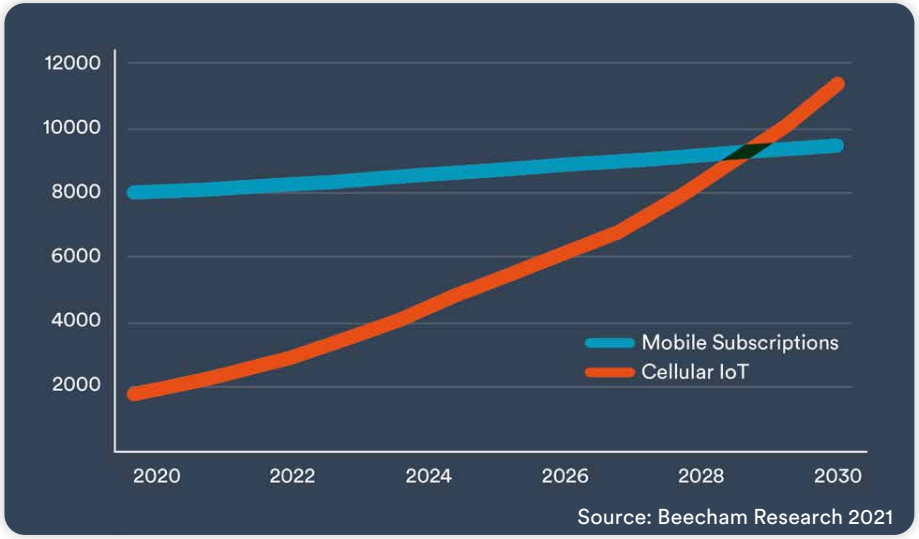
A decade ago 4G/LTE was a breakthrough development, much more than a step up from 3G. Now it has evolved into a comprehensive set of communications services offering Gbps data rates, low 50 ms latency and customised connectivity. 4G/LTE has become the networking technology that is delivering the demanding wide area connectivity requirements of IoT use in business. Those requirements include connecting staff, devices, vehicles and applications in industrial verticals such as transportation; military and defence; manufacturing; oil and gas; energy; mining and healthcare.

IoT in business operations has the proven ability to boost operational efficiency, improve product and service performance, and enhance operational agility. The overall result is a significant uplift to a company's competitive offer and its bottom line. IoT has truly moved from 'nice-to-have' as a low cost remote monitoring activity to 'strategic necessity' in many business operations as the emphasis moves more towards control and automation. This trend is set to continue at a fast pace over the next decade. At the same time, the IoT market is moving to 5G, which offers yet more new opportunities for use of IoT in business.

So what does that mean in terms of numbers? Taking an overall view, for one thing while the projected growth of mobile handset subscriptions in the decade 2020-30 is expected to average 1.8% CAGR, the equivalent for cellular IoT connections is expected to average 20.5%. In other words, by the time we get to 2030, there are likely to be more cellular IoT devices connected to mobile networks than mobile handsets.

This is an indicator, but it's not the whole story. One thing is for sure – business operations are increasingly relying on IoT and cellular IoT in particular.

Figure 1.1 *Projected Mobile Subscriptions vs Cellular IoT Connections (billions)*



Why private cellular networks?

Private cellular networks (PCNs) have been around for many years, operating in the Small Cell market and primarily supporting voice applications for on site use. The move from 2G and 3G to 4G/5G has brought the opportunity for PCNs to cater for IoT applications.

PCNs can take the growing need for cellular IoT in business operations to another level, in the process considerably enhancing the IoT offer. This includes innovative solutions that employ both licensed and unlicensed spectrum as well as combinations of public and private networks, potentially with seamless roaming between them.

When enterprises own their communications resource, IT management can take control of performance, security and resilience as required for local operations. They can determine user authorisation, how resources are employed and how traffic is prioritised. On a private network, data transfer is also secure, it remains on the company's premises. In addition, ownership allows these networks to be amortised; the financial model typically changes from OpEx to CapEx.

While PCNs for IoT are a relatively recent development, private Wi-Fi networks have been around for a couple of decades and this communication medium has become the mainstay in business premises and campuses. They were designed to accommodate both voice and data traffic and also to ensure that mobile phones could use Wi-Fi when making calls inside the company's premises. They have never worked too well for IoT on very large sites though, such as airports, large manufacturing sites, mines, ports and more.

While Wi-Fi 6, the new standard, improves overall network performance, it is struggling to accommodate today's data-centric, business-critical IoT applications. Has the time come when such Wi-Fi networks used for business IoT operations should be augmented or replaced by PCNs? This has come into sharper focus with the huge success of the CBRS (Citizens Broadband Radio Service) band (band 48) in the US for private cellular use in unlicensed spectrum.

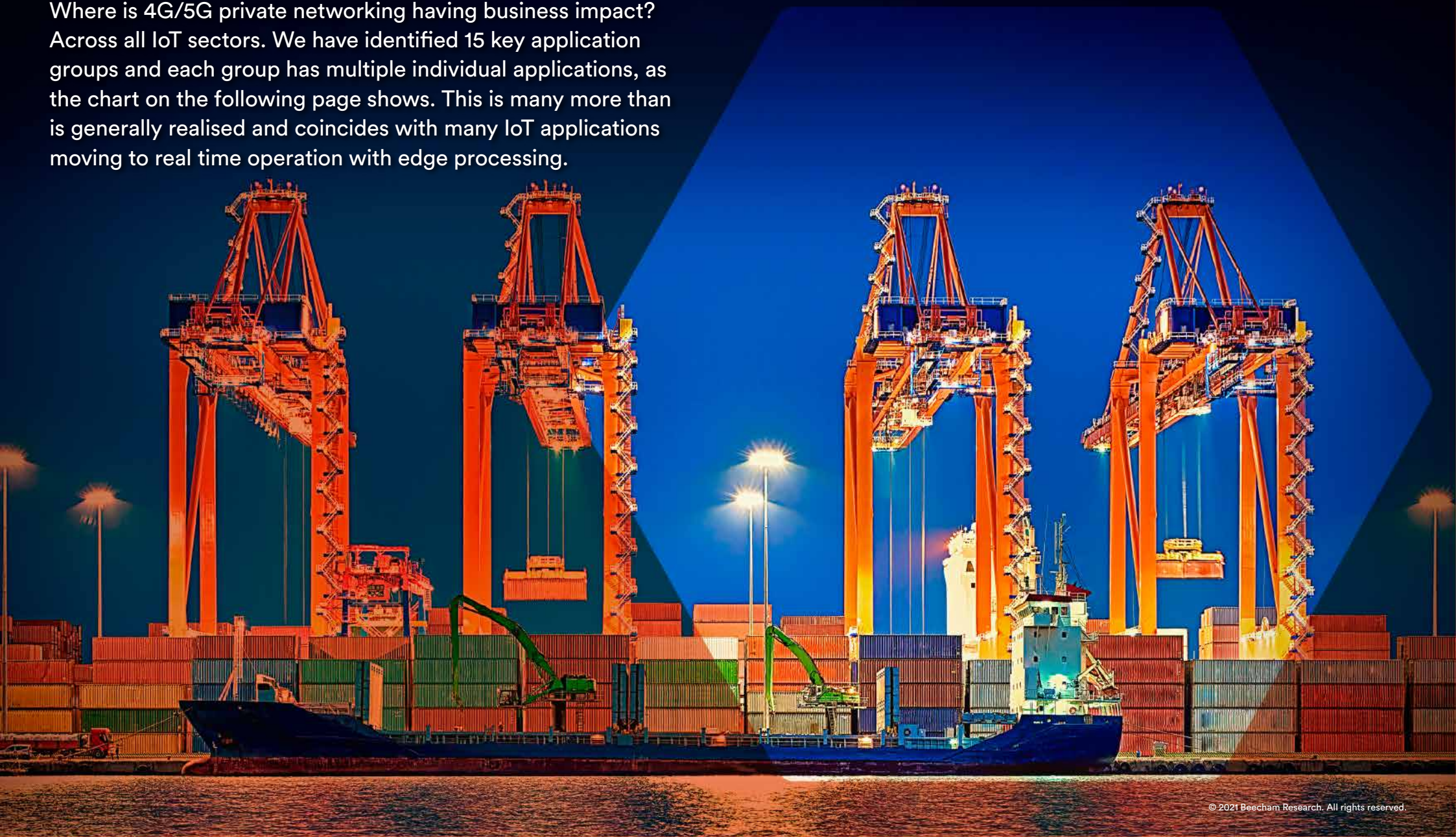
The choices for PCN deployment are now increasing around the world and this will continue. PCNs are now expected to become an increasingly popular choice for businesses, offering the following main benefits for their operations activities:

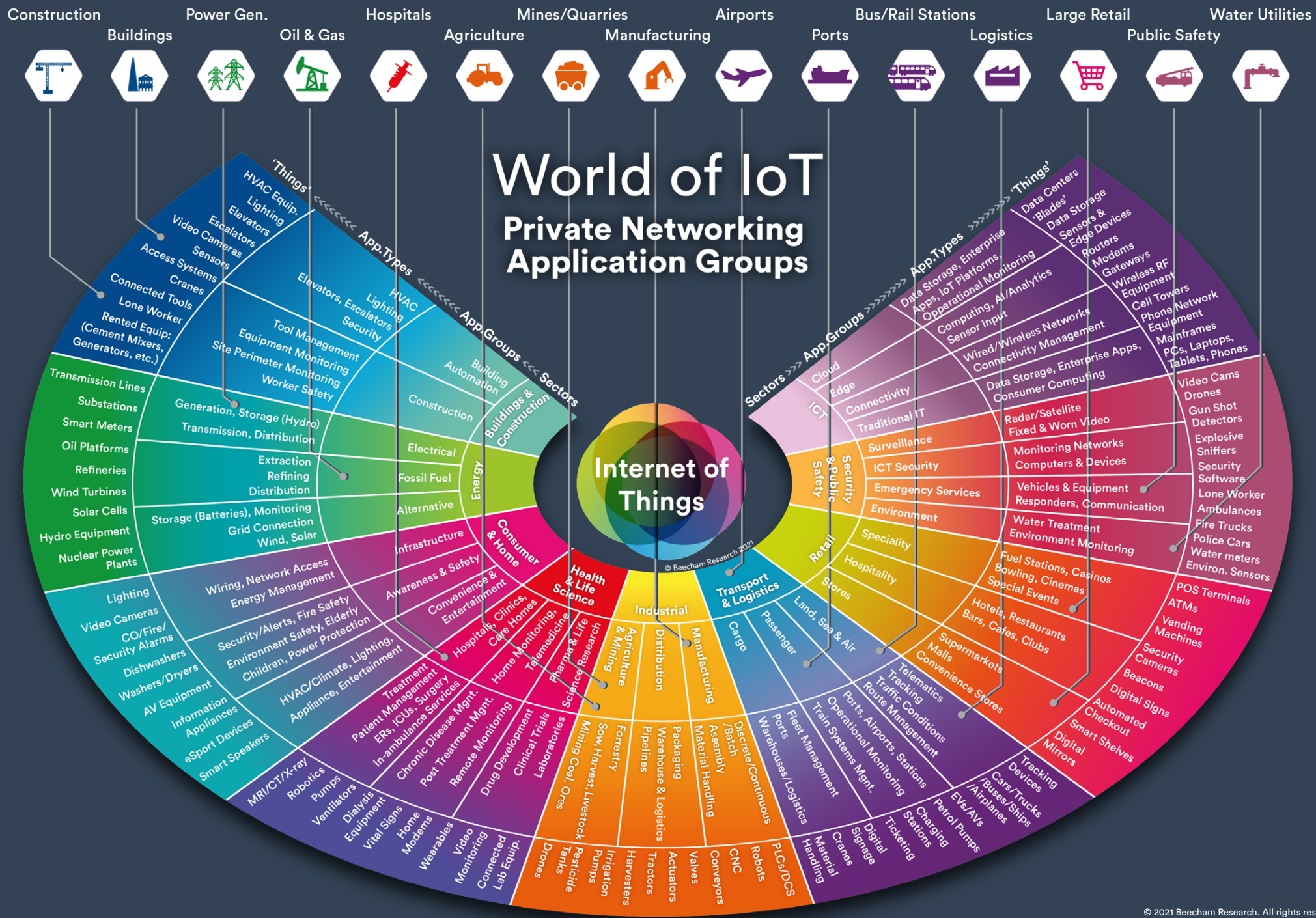
- Local coverage, both indoors and outdoors, designed to meet on-site needs
- High level of network security, with data remaining on-site
- Sufficient network capacity for requirements at all times
- Local management control over network traffic and use, including seamless integration with enterprise IT/OT
- Very high network reliability
- Predictable and ensured low latency – data control
- High data rates and high density devices

With more PCN choices becoming available, it's time for businesses to review their options. Hence this report.

IoT Sector Activities

Where is 4G/5G private networking having business impact? Across all IoT sectors. We have identified 15 key application groups and each group has multiple individual applications, as the chart on the following page shows. This is many more than is generally realised and coincides with many IoT applications moving to real time operation with edge processing.



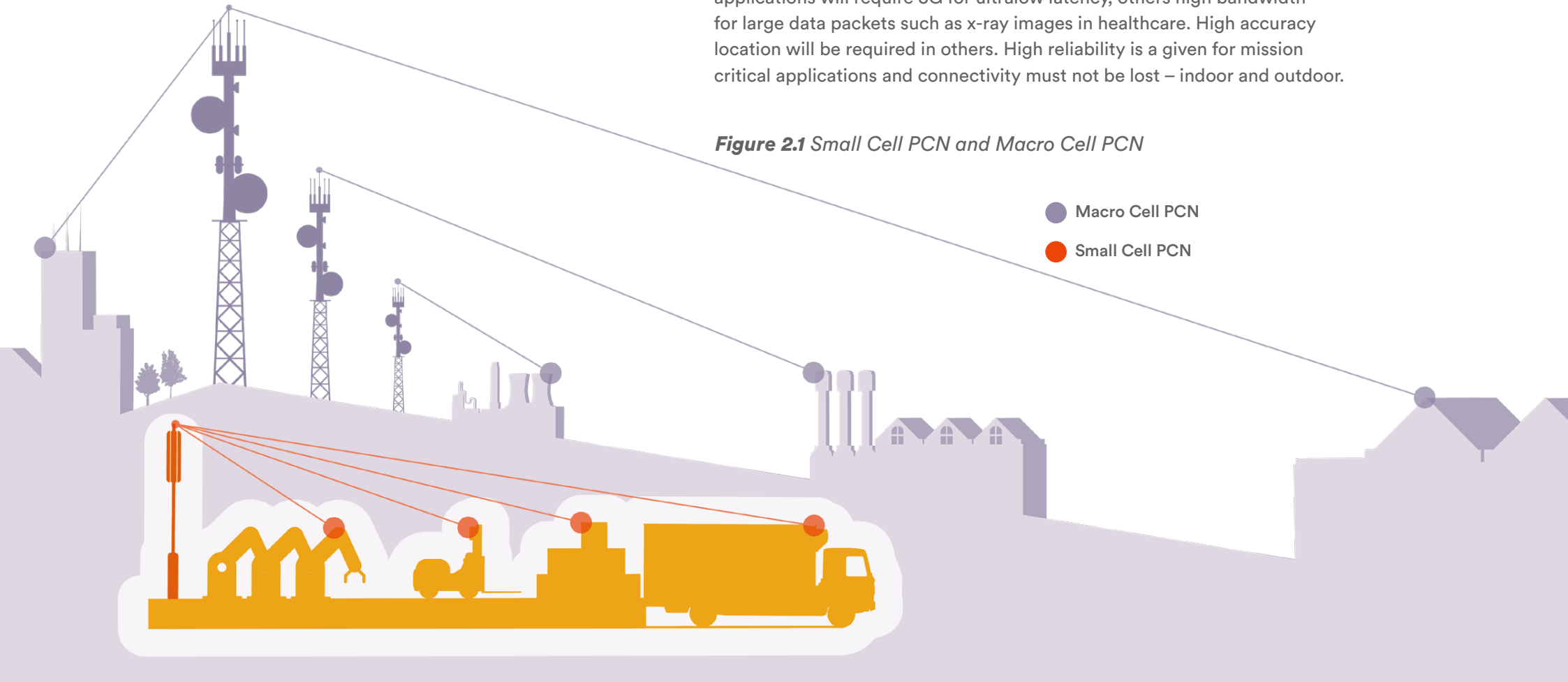


The chart on the previous page shows which application groups in Beecham Research's reference IoT World Map are relevant for private cellular networking. It puts into context the significance of private networking for the IoT market - involving all main business sectors.

In this section we briefly examine the IoT applications being delivered by Private Cellular Networks in fifteen distinct segments. These are primarily implemented in campus-like, circumscribed areas and settings, for example hospitals, airports, construction sites, ports, bus and railway stations, etc., and we refer to these as Small Cell PCN. We refer to applications deployed in much larger areas as Macro Cell PCN. An example of Macro Cell PCN is the private LTE network built by Rio Tinto, the Australian mining conglomerate, that encompasses fifteen mines and railway and transportation facilities.

Mission critical communications are essential for these businesses; some applications will require 5G for ultralow latency, others high bandwidth for large data packets such as x-ray images in healthcare. High accuracy location will be required in others. High reliability is a given for mission critical applications and connectivity must not be lost – indoor and outdoor.

Figure 2.1 *Small Cell PCN and Macro Cell PCN*



PCN application groups, showing typical on-site IoT applications within each group

Buildings, Smart City

- HVAC
- Environmental Sensing
- Video
- Vertical Transportation
- Lighting Management
- Energy Management
- Water Management
- Occupancy
- Municipal Systems **(Macro Cell)**

Construction

- Tool Tracking
- Video
- Drones
- Lone Worker Safety
- Equipment Monitoring
- Environmental Sensing
- Building Material Tracking
- Precision Positioning

Power Generation

- Operational Equipment Monitoring
- Lone Worker Protection
- SCADA
- Environmental Sensing
- Video
- Drone
- Distribution, Metering **(Macro Cell)**

Oil & Gas

- Tank Monitoring
- Lone Worker Protection
- SCADA
- Wellhead Monitoring
- Environmental Sensing
- Operational Equipment Monitoring
- Oil Platform Operations

Hospitals

- Tracking High Value Equipment
- Monitoring Patient Vital Signs
- Video
- Coordinated Emergency
- Environmental Sensing
- Operational Equipment Monitoring

Manufacturing

- Operational Equipment Monitoring
- Lone Worker Safety
- AR/Head Mounted Display
- Autonomous Robotics
- Digital Twins
- Asset Tracking
- Handheld Terminal
- Remote Equipment Control
- Precision Moveable Equipment

Agriculture

- Drones
- Pesticide Tank Monitoring
- Vehicle Telematics
- Environmental Sensing
- Equipment Monitoring
- Remote Control

Mines & Quarries

- Strain Gauges
- Vehicle Telematics
- Environmental Sensing
- Equipment Monitoring
- Remote Control
- Mobile Robots
- Drones
- Autonomous Vehicles

Public Safety, First Responders, Surveillance

- Video Systems
- Public Warning Systems **(Macro Cell)**
- Automated Response Systems
- Mission Critical Data – First Responders
- Drones

Water Utilities

- Operational Equipment Monitoring
- Lone Worker Safety
- Video
- Drone
- Remote Water Quality Monitoring
- Environmental Sensing

Airports

- Cargo Systems
- Flight Data Download
- People Moving Systems
- Video
- Environmental Sensing
- Sensing for Maintenance, Supply
- Operational Equipment Monitoring
- Apron Vehicle Navigation

Ports

- Crane Operation
- Autonomous/Semiautonomous Vehicles
- Environmental Sensing
- Docking Ship Communications
- Video
- Drone
- Operational Equipment Monitoring
- Remote Control
- Autonomous/Semiautonomous Robots

Bus & Railway Stations

- Video
- Environmental Sensing
- HVAC
- Lighting
- Energy Management
- POS Transactions
- Digital Signage
- Parking
- Luggage Systems

Warehouses & Logistics

- Asset/Pallet Tracking
- Autonomous Guided Vehicles
- Autonomous Mobile Robots
- Robotic Picking
- Autonomous Robotic Inspection
- Environmental Sensing
- Operational Equipment Monitoring

Large Retail, Stadia

- Tracking
- Video
- Kiosks/Beacons
- Environmental Sensing
- Sensing for Maintenance, Supply
- Automated Checkout
- POS Transactions
- Specialized Hospitality Applications

Each PCN application group examined in more details, together with example case studies

Buildings, Smart City

The challenges

'Smart Cities' are connected cities, comprising systems of systems for supporting all manner of city functions and operations for businesses and residents. Many components comprise 'smart cities', including:

- Public Street and Highways Lighting
- Intelligent Transport Systems
- Large buildings including public buildings, government offices and commercial industrial spaces
- Remote management from a centralised location, possibly using private cellular networks.

Cities around the world are continually developing and updating plans for the integration of emerging technology into their infrastructure. At the same time environmental imperatives are coming to the fore, including carbon reduction goals, reducing energy, water and other waste.

Applications

HVAC Heating, Ventilation, Air Conditioning in large buildings

Access control systems, facial recognition systems

Video surveillance for indoors and outdoors security monitoring

Remote Building automation systems control and monitoring

Vertical transportation – smart elevators

Environmental Sensing - Indoor air quality management, fire risk management; outdoor air pollution

Lighting management – indoors and in the street

Energy management

Occupancy management

Water Management (macro cell or hybrid small and macro cell)

Emergency management including coordination with emergency services, first responders – small cell PCN one part of hybrid solutions

Digital Twins for planning and other systems development

Intelligent Transport Systems, including smart roads infrastructure, digital signage for roads, in the longer-term vehicles that communicate among themselves and with roadside infrastructure

Traffic lights control, traffic management (macro cell)

Smart parking (public spaces)

Smart Bus timetables, digital signage

Municipal Systems (macro cell) – public services including waste collection and disposal, street cleaning, City wayfinding systems

Buildings, Smart City

Case Study – Murrey School District

2020 became a turning point for many schools around the world. The pandemic kept many parents home doing remote work while children were doing their remote class work with their teachers. Even households with broadband connections, the home network was not strong enough to support all the simultaneous streaming. This resulted in many children unable to participate in the real-time learning they needed.

Murray City School District (MCSD) was already going down the path to implement a Private Cellular Network to efficiently manage and stream footage from on-campus surveillance cameras. With the advent of the pandemic, the school district was able to extend their private cellular network to encompass distant learning for their students and provide connectivity for their teachers, ensuring a consistent experience for everyone.

MCSD rolled out a cost-effective private cellular network system utilizing Cradlepoint's NetCloud Service with more than 400 CBRS-compatible cellular edge routers. Coupled with a couple dozen eNodeB citizen broadband radio service devices (CBSDs) set up at strategically selected locations all over town, the school district has a PLTE network that students can connect to for free, high-performance Internet access with all the security requirements included.

Case Study – Organizations are increasingly deploying private 4G/5G networks

IoT data is the lifeblood for manufacturers, utilities, smart cities and other organizations. It is mission-critical information about the status of their infrastructure, usage of their services, insights into productivity and, in the case of industrial robots, step-by-step manufacturing instructions. If the flow of that data suddenly slows or stops, or if it's hacked, the consequences can be disastrous.

Those risks and rewards are why businesses and other organizations are increasingly moving their IoT data from public mobile networks to their own 4G/5G infrastructure. Private networks mean their data no longer competes with Facebook uploads, Tik Tok videos and other traffic for bandwidth. They also provide more data privacy and protection against malware because network access is limited to that organization's IoT devices.

Organizations have many options for deploying private 4G/5G networks. One key consideration is spectrum. For example, many European utilities use the 450 MHz band because it has lower capex: Signals travel farther at low frequencies, so fewer base stations are required.

In any band, the right antenna is critical for maximizing performance and reliability. For example, the Taoglas Apex IV TG.46.8113 is a wideband 4G/5G dipole antenna that covers all sub-6 GHz bands, including the 450 MHz spectrum that's increasingly home to private LTE networks in Asia, Europe and South America. With the highest wideband efficiency of any terminal antenna on the market today, the TG.46 is optimized for the 5G New Radio bands between 3.3 GHz and 4.2 GHz.

Another example is the Taoglas PCS.66.A, which is designed for private 4G/5G applications where low cost is a top consideration. Featuring support for all sub-6 GHz bands down to 600 MHz, the PCS.66.A also has a high-efficiency design to ensure that it provides the maximum throughput for any 3GPP 4G and 5G release that an IoT module uses.

Construction

The challenges

The construction sector includes all types of built structures, including critical infrastructure. Building sites, stadia, roads and highways, railways and bridges, all have their own special challenges.

Large construction projects involve the entire range of civil engineering design capabilities. Adding to the complexity is the fact that the multiplicity of contractors needed generally work to their own methodologies and software and hardware preferences. This makes overseeing a large project challenging, necessitating visibility and control over all activities through real time task management.

Health and safety imperatives are growing stricter with heavy penalties if staff are not protected from unsafe areas e.g. collapses.

Environmental concerns are also coming to the fore with meeting net zero commitments. For one, the cement industry accounts for 8 percent of human-caused greenhouse gas emissions. Concrete plays a key role in all major construction projects: hence concrete curing must be carefully monitored.

Analysts anticipate that 5G will play a greater role in the digital construction environment, as it provides more bandwidth for real time data acquisition in areas such as high definition imaging and video.

Applications

Digital Twins for the design process; this allows quality checking against the digital twin while installing a structural item, using current data

Risk analysis using data to mitigate risks that come to light on projects

Building Information Systems in standardised format, intelligible to all participants. Leveraging interoperable and accessible datasets enables informed, smart infrastructure management at every stage of a project from design to operations

Predictive maintenance of machinery, to detect the possibility of breakdowns before they occur

Telematics for vehicles used in construction sites

Time and materials management workflows

Site security – intrusion detection through cameras, site sensors

Drone surveillance/video for structural monitoring, to detect cracks or assess structural integrity

Remotely monitoring the concrete curing process. Temperature variations can compromise the strength and integrity of concrete, raising the risk of fractures.

Power Generation

The challenges

In addition to traditional fossil-fuel, nuclear, and hydroelectric energy sources, the industry increasingly includes renewable (solar, wind – onshore and offshore) sources and distributed generation, greatly increasing the complexity of grids and grid management, which must minimize outages even as overall grid infrastructures typically include mixtures of new and outdated equipment, all of which must work together.

The industry faces increasing consumer demand, new standards and carbon reduction targets. The International Energy Agency (IEA) has warned that major effort is needed to develop and deploy clean energy technology. Governments have been revamping power generation to be less carbon intensive through building more renewable power facilities and reducing the use of fossil fuels.

Security for mission critical applications is also an area of great concern.

Private cellular networks (small cells) are suitable for sites of centralised energy generation. Macro Cell PCN is suitable for more extensive power transmission and generation.

Applications

Flow metering

Asset management

Predictive maintenance, predictive analytics

Autonomous Robotics

Supply/demand management

Storage

Digital twins

Operational equipment monitoring

Lone worker protection and alarm generation – power plants are a particularly hazardous environment for workers

SCADA - Supervisory control and data acquisition - a control system architecture comprising computers and networked data communications for high-level process supervisory management

Environmental Sensing for leaks, ambient conditions control

Video for site intrusion detection

Drones for site inspection

Cybersecurity

Distribution metering (Macro Cell)

Grid operations optimisation (Macro Cell)

Demand response (Macro Cell)

Power Generation

Case Study – Connected Utility

Utilities must modernize their grids to meet aggressive decarbonization goals to enable clean and affordable energy for their customers while keeping workers and customers safe, especially with the rise of natural disasters such as violent storms and wildfires. Today's utility requires a new high-performing, predictive grid operating system that communicates in real-time with low latency situational awareness and responsiveness driven by more intelligent, predictive analytics.

Therefore, the key to this modern grid is the communications infrastructure. Utilities have many different types of communications networks; however, modernization efforts are pushing traditional networks to their limits. Today's grid cannot run solely on the old-fashioned networks of yesterday (e.g.,Wi-Fi, fiber private LTE). New, dedicated 5G private cellular communications networks that are hybrid (multi-carrier and multi-cloud) owned and operated by the utility are being required. These "private mobile networks" are becoming the new gold standard for the modern, connected utility of the future that needs an affordable, fast-to-deploy and easy-to-manage answer today.

Expeto partnered with a regional electric utility serving more than 2 million customers to develop an innovative approach to solve the challenges of the modern grid. Together, they built a 5G Energy Lab capable of testing the limits of cellular private mobile networks to support advanced use cases and technologies capable of early wildfire detection, enabling city-wide electric vehicle charging, and connecting workers to ensure timely and safe maintenance and service restoration. These networks, based on hybrid multi-carrier, multi-cloud solutions, have allowed PGE to have the best of 5G availability while still controlling costs and access to their sensitive data.

pod group
A Giesecke+Devrient Company

Own your IoT Network

- Gain control and visibility of your IoT connectivity, globally
- Your own network, customized to your application
- Managed services accessible via one easy to use platform
- One unified, secure domain across public and private networks

As the world's first Enterprise Network Operator (ENO), Pod Group, puts the ownership of the IoT network into the hands of the enterprise, combining the control and visibility of its own core network with the flexibility, customized services and global reach of a specialist in IoT connectivity.

ENO SIM

- Active element for device control
- eUICC (eSIM) as standard
- Multi-IMSI network profiles
- Intelligent SIM applets

ENO PLATFORM (PaaS)

- Deep integration
- Multiple white label hierarchies
- Over the Air (OTA) provisioning
- "One pane of glass" network management

ENO NETWORK (NaaS)

- Own core network/IMSIs
- Inherently secure
- Enables connectivity/roaming on private & public spectrum
- Private LTE as a stepping stone to 5G

Contact Pod Group today to find out more about our "ENO in a box" solution and take control of your enterprise IoT network

www.podgroup.com +44 (0) 1223 850 900 sales@podgroup.com

Why Expeto?

Enterprise First™ 5G Private Mobile Networks enable mission-critical mobility for your business.

Expeto creates unprecedented value for Enterprises:

- **Simplify:** Converge all networks across multiple sites into a single, global WAN
- **Configure:** Establish network policies for users/devices, data routing, and QoS
- **Control:** Manage networks from a control plane integrated with IT/OT systems

Expeto creates meaningful value for Mobile Network/Service Operators:

- **Differentiate:** Offer enterprises an end-to-end PMN solution to rival competition
- **Create:** Forge new connectivity, edge, and application revenue streams
- **Grow:** Drive high margin ARPU with low churn by meeting enterprise demands

expeto™

to learn more, visit us at www.expeto.io

Power Generation

Case Study – French nuclear power plant secured private network

Thales and Ericsson partner with EDF to bring mobile broadband connectivity to French nuclear sites, both in production and under construction. With this roll out, EDF is leading the deployment of secure private 4G networks on this scale both in France and internationally Successful pilot implementation at the Blayais nuclear site represents the first step in a deployment that will cover all EDF nuclear power plants in France

EDF, Thales and Ericsson have partnered on CONNECT, a project that will bring secure cellular connectivity to all EDF's nuclear energy sites in France. Thales, leaders in network design and operation, are deploying secure communications services while also guaranteeing the overall system integration and secure networking.Ericsson are providing innovative 4G private network solutions as well as the core network, to ensure high-performance connectivity, resilience, and security. Due to the specific needs of the energy giant, cybersecurity is a key element of the collaboration and has been integrated into every step of deployment. The new private network solution will enhance site performance, maintenance, operations, and logistics.The enhanced connectivity will allow EDF employees and their partners to have a remote access to all needed resources via secure terminals.The new network infrastructure has been built for EDF, ensuring that the specific needs of the nuclear power provider, such as scalability, flexibility, and cybersecurity are in place. An evolution towards 5G is possible in the long term. The first nuclear plant that has benefitted from the CONNECT project is Blayais. After a successful joint pilot, the connectivity solution at the Blayais site is now being operated independently by EDF. Rollout of the solution at EDF's other power plants is scheduled for 2021 at a rate of 2 to 4 plants per year.

https://www.thalesgroup.com/en/group/journalist/press-release/thales-ericsson-and-edf-deploy-secure-private-mobile-networks

Case Study – Private network connectivity reconfiguration over time

An electricity provider wanted to leverage wireless connectivity for its smart meter fleet via a two-fold objective of digitalizing its business via real-time consumer data and service monitoring, as well as securing its operations in case of an incident. Nevertheless, in the national context, technology and regulatory evolution are not in sync, industrial LTE or 5G currently being unavailable. This uncertain situation leads either to postpone the investment until a more predictable time or accept the need to perform costly field up-grades in future. The solution chosen by this electricity provider was to provide its smart meter fleet with connectivity capabilities and leverage its multi-profile reprogrammable 4G SIM, with subscriptions coming from the current MNO and provide a private network subscription for future use. These SIM profiles will be managed centrally by a set of business rules that cover radio coverage quality, financial conditions and eventually regulatory changes. Thus, the ability to reconfigure connectivity future proofs the system, secures operations and provides immediate digitalization transformation benefits by enabling control of the TCO of the connected energy infrastructure.

Oil & Gas

The challenges

Oil and Gas is a highly regulated industry and operates world-wide under widely varying conditions.

The industry was traditionally reliant on manual processes and characterised by ageing equipment and legacy infrastructure, and has suffered serious disasters across the world. It now operates increasingly in remote and offshore locations, which makes it costly to monitor operations manually and maintain safety levels for workers. That said, oil and gas has been one of the first verticals to begin the IoT digital transformation, moving from reactive to preventive maintenance. It has changed from heavy engineering and manual operations plagued by major accidents, to 'The Digital Oilfield', where technology drives operations.

EY's 2020 oil and gas digital survey showed that 90 per cent of industry executives agreed that investment in digital technology is needed for the industry to survive. The cost savings are critical for survival, as oil and gas companies look to gain greater operational efficiencies and drive productivity across the value chain. The survey found that data analytics and the insights derived from it are expected to positively impact business growth in the next three years.

Digital technologies are helping companies tap into oil and gas reserves that were previously considered unreachable, like the arctic. Here the equipment is becoming more sophisticated and complex, necessitating better monitoring and control systems to keep it working efficiently and safely. Protecting the health and safety of workers is also mandatory, as is compliance with carbon reduction goals. Increasingly, production facilities are obliged to reduce pollutants emanating from their operations.

Oil and gas production sites comprise both above ground and below sea platforms. IoT is critical at many stages of operations: site exploration, well operations and drilling, extraction and production, pipeline operations, transportation, and lastly, well decommissioning. Private cellular networks will support IoT applications by collecting large amounts of data from a variety of operations, and enable real time troubleshooting.

Applications

Geosensing – surveying the terrain to identify sites where deposits could be present; recording devices can evaluate rock, fluid and gas properties

Remote monitoring of well performance, remote troubleshooting in hard to reach locations, maintaining safe operations

Robotics for remote control of machines in hard to reach locations

Lone worker protection with alarms

AR/VR to help engineers identify problems by referring to knowledge sources

SCADA AI ML – remote data collection for monitoring and analytics; use of AI and ML to identify complex issues

Drone inspection of operational sites as well as underwater platforms; close-quarter flights near infrastructure assets, under oil rigs, in places with magnetic interference, absence of GPS etc.

Environmental Sensing for spills, leakages and pollutants including monitoring hydrocarbon spills, CO_2 emissions, as well as hazardous materials including Mercury, Arsenic and naturally occurring radioactive materials

Operational Equipment Monitoring in oil platform operations; e.g. fatigue monitoring from drilling

Fleet monitoring and Telematics for on-site vehicles

Geofencing and intrusion detection for on-site security.

Oil & Gas

Case Study – PK Solutions

Oil and gas companies use PK Solutions' digital inspection software, designed for in-field tablets, and an integrated workforce optimization software. The information is gathered from wearable devices to eliminate inefficiencies and maintain real-time communication and the utmost workforce safety at refineries. A variety of on-site devices require connectivity, including gas monitors, biometric monitors, tablets, and wearable devices.

PK must ensure network connectivity for works and devices inside towers, or vessels, that are hundreds of feet tall. When specialists wearing the devices are sent into these towers to perform inspections and repairs, safety is a major concern. The devices track a person's vital signs and environmental readings, while video cameras mounted inside help safety officers elsewhere remotely monitor the situation.

To ensure a reliable connected experience for its technologies that improve safety and efficiency, PK deployed a Private LTE system - leveraging CBRS shared spectrum – for its sprawling Wireless LAN. Private LTE system is fantastic because they can arrive at an oil and gas company's job site, put up temporary towers, and control bandwidth and who's using it.

Cradlepoint NetCloud Service is part of the overall Private Cellular Network that blankets these sprawling refinery sites with the secure, uncongested, and cost-effective connected experience their customers need for monitoring worker safety.

Hospitals

The challenges

Details vary from country to country, but many hospitals in many countries face significant cost pressures, aggravated by the Pandemic. Achieving greater efficiencies cannot be accomplished at the expense of providing positive patient outcomes, however.

The movement from paper-based patient records and billing to Electronic Health Records (EHR) has long been underway, leading to ever more comprehensive hospital IT systems connecting all areas.

Computers and computer networks are everywhere in hospitals. Programs and data include scheduling and billing and extend from patient admission through treatment and surgery to discharge and beyond, with data from test results, vital sign monitoring, radiology and imaging and various medical and surgical devices perpetually growing even as nurses, doctors, pharmacists, and various specialists constantly enter data manually.

Devices of all kinds are becoming increasingly connected, using a range of communication protocols, wired and wireless, serving both primary objectives simultaneously: Achieving greater efficiencies and improving patient outcomes.

The strengths of PCNs, well suited for mobile in-hospital equipment with greater bandwidth and offering simplicity compared with miles of Ethernet cabling suggest they will become a growing part of modern hospitals.

Applications

Tracking High Value Movable Equipment

Monitoring Patient Vital Signs

Video surveillance for security, intrusion detection, wandering patients

Fire safety monitoring, alarm generation

Coordination between emergency vehicles, ERs, ICUs, and other relevant areas

Environmental Sensing applications, including controlling the environment in the patient's room for optimum comfort including lighting and ventilation.

Operational Equipment Monitoring

Robotics for Remote Surgery

Manufacturing

The challenges

Manufacturing comprises a very large array of industries, including heavy equipment, consumables, high-tech - all made from a range of materials. Industry 4.0 refers to the current phase of computerisation of manufacturing processes, underpinned by artificial intelligence, machine learning, IoT big data, robotics, augmented reality, 3D printing, drones, 5G wireless, and edge and cloud computing. Manufacturing is one of the foremost industries to apply these technologies.

The availability of vast quantities of data and real-time information transmitted from machines enables a better understanding of how things relate to each other, and provides the basis for better decision-making processes. Coupled with the proper organisational structure, companies can react faster to new customers' requirements and today's dynamic markets, and conceive new business models.

Alongside these developments, the digitisation or digital conversion of business and industrial operations is ongoing. Several transformational digital technologies are contributing to opening up possibilities in industry, including the Internet and the Cloud, robotics, blockchain and additive manufacturing.

Private cellular networks are being deployed across many different parts of the industry. They ensure the secure distribution of IoT data traffic, while sensitive data stays on-site instead of going back to an operator's core network. Companies own, control, and manage their private networks, enabling their IT departments to determine performance, authorisation, and traffic prioritisation.

Applications

Predictive maintenance helps to reduce costs and downtime for all types of machinery. This requires investment in sensor infrastructure and the deployment of an analytics system together with specialised interpretive skills

Proactive, remote monitoring of machine operations leads to cost and time savings

Remote equipment control, material handling and precision positioning of heavy moveable equipment minimises accidents and errors

Asset tracking across the manufacturing process to keep track of machinery

Process optimization - with smart tools, businesses can collect usage data in order to locate strengths and weaknesses in the process and make adjustments accordingly

Worker safety monitoring using wearable alarms

Robotics - remote-controlled and autonomous robots; these will increasingly require low latency connectivity

Machine Vision combines a range of technologies to provide useful outputs from the acquisition and analysis of images for robot-based inspection and guidance. It is used to determine surface properties and defects, for example

Digital twins assist in the modelling and design of machines and processes

AR/VR -Augmented and Virtual Reality in head mounted displays allow designers to view their creation from the user's perspective and assess whether it will meet requirements.

The IoT M2M Council (IMC)

25,000 enterprise users and product makers that deploy IoT technology –
a platform for thought leadership, lead-generation, promotion, and research.

IMC EVENTS COVER...

- Edge Compute
- Private Networks
- IoT Security
- Low-Power Connectivity
- AI/Machine Learning
- New Business Models
- Consumer Markets
- CapEx vs. OpEx
- Industrial IoT

https://www.iotm2mcouncil.org/iot-library/event/imc-events/

Manufacturing

Case Study – Smart Manufacturing

ERICSSON

Atlas Copco Airpower manufactures compressors and related systems for customers worldwide. The company continuously strives to improve production and operations, and is transforming its factory in Wilrijk Belgium into a smart, connected, innovative factory floor for flexible manufacturing. Based on a co-creation model, Atlas Copco is collaborating with Ericsson and Orange Belgium to provide an intelligent manufacturing solution using 4G and 5G wireless connectivity.

The solution comprises a dedicated 5G-ready cellular network that enables wireless communication to connect devices on the factory floor and do away with the traditional cables. Ericsson's Industry Connect is a pre-configured dedicated private cellular network for industrial sites such as factories and warehouses. Starting with 4G/LTE servicing the existing device ecosystem, the company claims this is a future-proof solution with a clear path to 5G. Through Ericsson's Dedicated Networks system, autonomous guided vehicles are controlled wirelessly with cameras and environmental monitoring sensors across the factory. Portable tools, fixed tools and machinery can also be connected to the network.

The wireless connectivity network offers stable connectivity, supporting remote management and productive manufacturing. The smart and streamlined factory floor leads to improved production performance. Orange Belgium guarantees secure mobile connectivity and full 24-hour availability for the industry which manufacturers require for their critical business, in addition to data protection and data integrity.

Among manufacturing industries, there is an increasing trend to transition to 5G ready dedicated networks to enable intelligent manufacturing. Atlas Copco initiated its digital transformation at one of their largest facilities. Since spring 2019, Atlas Copco Airpower has been running the Ericsson Industry Connect network at its facility in Belgium and recently extended the deployment to connect the wider shop floor in 2020.

Case Study – Private/Public seamless network switch

THALES

This organization manages an archipelago of several large isolated industrial areas in a perimeter of hundreds kilometers comprising thousands of enterprises and workers. Some of these connected workers or the devices might go out of coverage in certain circumstances (being on-duty or going in and out of the PN perimeter). Fixing that issue implies using either dual capability equipment for each user or complex and frequent manipulations of an employee's handset, which was not suitable for most of the daily working situations. Thales provided a customised SIM triggered service that allowed private network users to switch automatically and seamlessly from one network to another depending on the most appropriate connectivity at the time. This solution provides switchable public-private connectivity without an additional end-device cost.

Agriculture

The challenges

IoT solutions are now widespread in all application areas of farming, including arable farming, livestock farming, barns, forestry and fish farming.

These have been developed to help address the current challenges to the industry worldwide, including demand to produce more food, labour shortages, water scarcity, soil degradation and run-off into waterways, the effects of climate change and pest control, among others. Cellular coverage from mobile network operators may not be adequate in remote areas.

Applications

Use of Drones for aerial monitoring of farmland and forests

Monitoring of fill levels for slurry, fuel, pesticide storage tanks

Irrigation systems control and wastewater management

Location/positioning for guiding harvesters and machines for seeding, feeding, weeding

Environmental Sensing – soil, water, air quality

Other Sensing – animal health, barn, greenhouse conditions

Equipment monitoring and predictive maintenance

Remote security cameras

Remote equipment control

Agriculture

ERICSSON

Case Study – 5G pilot for Forestry Research Institute of Sweden

Skogforsk, the Swedish forestry sector's Research Institute has commissioned Ericsson and Telenor Sweden to supply private 5G equipment for a pilot project. Ericsson is supplying 5G equipment, and Telenor is responsible for system integration. The project will look at ways to use 5G for the remote control of forest machinery; it will compare connectivity via local 5G stations with other methods including Wi-Fi and 4G to ascertain the distance at which remote control is possible, and which tasks can be done at a distance.

The Institute hopes that remote control can increase efficiency and strengthen competitiveness for both Swedish and Nordic forestry, fundamentally improve the working environment for operators, reduce accidents and lead to an increased interest in people taking up professions in forestry.

Remote control in forestry requires fast traffic speeds to transfer live video with low latency and high reliability, in different types of terrain and weather. Currently, Wi-Fi is used to a limited extent. The project leaders believe that 5G will be superior to Wi-Fi, and that applying 5G wireless technology could improve reach and effectiveness. A Private 5G network would provide large capacity and dependability in places where reception has been lacking or poor. The project is conducting tests with local 5G prior to rollout in the forestry environment.

Mines & Quarries

The challenges

The mining industry is moving towards sustainable operations, while at the same time it is venturing into ever more dangerous, remote locations. It is also moving towards increasing efficiency and automation, reducing the need for hazardous manual operations.

Carbon reduction goals are becoming a matter of urgency to comply with regulations. A United Nations report found that 26 per cent of the world's carbon emissions stem from the extraction and early processing of metals and other minerals. Environmental damage is also an issue for the industry, including damage to surrounding areas and the leaking of toxic materials.

Last but not least, worker safety and security issues are also paramount in this accident-prone industry and companies are constantly improving worker safety. Theft may be rampant, particularly in remote locations.

As competition in the sector intensifies and the availability of untapped resources decreases, IoT and private cellular networks could mitigate all the above risks, in both surface and underground mining. What is more, 5G would satisfy the requirement for real time and reliable data transmission in many of the operations.

Applications

Lone worker safety and alarm generation through wearables

Real time tracking of vehicles, requiring positioning accuracy

Environmental sensing: detecting gases and other toxic substances, and ventilation control of underground areas

Ground movement detectors, anticipating possible collapse e.g. after blasting

Intrusion detection, geofencing (against theft)

Equipment monitoring for machine downtime reduction –condition monitoring, predictive maintenance and fault diagnosis

Remote control of operations in hard to reach places, e.g. drilling; using mobile robots

Remote control of tools, e.g. strain gauges

Drones for site inspection and mapping; steering in flight and capturing live video streams necessitates significant bandwidth

Autonomous vehicles, particularly for haulage of material from the mine.

Mines & Quarries

Case Study – 5G for automation in mining

The Boliden open pit copper mine is located at Aitik in Northern Sweden and is the largest open pit mine in Europe. Boliden has taken part in a research project to co-create the mine of the future with a number of partners, including Ericsson.

To get to the copper ore, large amounts of rock must be removed. Automated and remotely controlled machines including drill rigs can perform repetitive tasks autonomously. One prerequisite for automation is the introduction of better connectivity including mobile connectivity. The project explored the role of automation in the industry in order to uncover the business value of using 4G and 5G technology, in terms of both economics and sustainability.

Automating a drill rig could enable Boliden to perform the same amount of blast operations with fewer rigs, while reducing the need for support operations and staff. The current technology used in the mining industry is Wi-Fi, which provides acceptable coverage and performance through careful configuration of Wi-Fi access points. Wi-Fi however is not designed for the wide area outdoor coverage needed by a mine like Aitik, and also severely limits the addition of other automated machines.

For supporting fully autonomous, remotely controlled equipment, high-performance communications are needed. A 4G mobile communication system would offer a secure, flexible and future-proof solution for Boliden; however only 5G however can comfortably handle the most demanding requirements – bandwidth, quality of service, latency and positioning. With such high-performance communications, a whole range of safety and efficiency measures become available to the mine. Boliden now plans more automation activities that handle several 3D video streams and manage highly complex tasks remotely. The remote control of machines and smart ventilation are perhaps the two most crucial use cases in improving safety and efficiency in the mines.

Preliminary results show that the application of automation reduced costs by 1 percentage point, with communications being the key enabler. Automating drilling and blasting showed an annual EUR 2.5 million net saving for the Aitik mine alone. There are a wide range of other use cases that the team is exploring, including video surveillance, man-down detection, and localization of machines, vehicles, things and people – highlighting the immense potential for innovation and productivity improvement within the mining industry.

Mines & Quarries

Case Study – Remote Mining

Enterprises located in remote areas such as mining or construction sites frequently suffer from poor cellular connectivity, and other technologies such as Wi-Fi or LPWAN may not be ideal for large outdoor areas where there are many moving assets. In these cases, a Private Cellular Network using spectrum acquired by the enterprise is often the best way to achieve the coverage, security and low latency needed for these types of applications. However, the reception of supplies and the distribution of materials from the site, as well as the need to track high value assets such as machinery to prevent theft means that the network cannot operate as a standalone "island", but needs to be seamlessly connected to the wider public WAN.

This was the case for a mining company, located in a remote area of Australia, which needed to track assets at all times in an area with no LTE coverage. The company acquired spectrum and this made it possible to install a private LTE network, comprising a local base station and small cells that replicated the larger public network, at the site of the mine.

Pod Group enables connectivity on both the private and public network. As an Enterprise Network Operator, Pod Group runs its own core network, providing seamless access to the IPX (IP eXchange) backbone network, which is a managed network environment. Data runs at Gigabit rates on the IPX and it doesn't touch the public Internet, so it's totally secure. The IPX network is accessed through four points of presence (PoPs), two in the USA and two in Europe. This allows Pod Group to operate its own distributed, secure IP core network and market innovative LTE/5G services.

LTE employs an Evolved Packet Core (EPC). This is a key component that can be implemented in software, which enables advanced public network functionality to be employed in cost-effective private networks. Pod Group's partner Expeto markets an innovative solution that provides seamless roaming between private and public networks. This is realised by expanding and extending EPC's functionality and by deploying it in a PaaS (Platform as a Service) model. Enabling EPC as a service is realised by splitting the core in order to enable the LTE home subscriber server to operate in different locations.

The solution has enabled the mining company to deploy a private network at the site of the mine, with the ability for devices to seamlessly roam onto the public network using a single SIM. This not only enables the enterprise to gather data at the remote mine and control devices and assets via its corporate data centre, it also enables it to monitor the whereabouts and status of vehicles entering and leaving the mine, all the way to their destination, using the public network infrastructure. The whole network operates as one corporate domain behind the enterprise firewall, making it intrinsically secure. In addition, the enterprise benefits from full visibility and management of its assets through a single platform.

Mines & Quarries

Case Study – Mining Company

When you think of technology advances with autonomous vehicles, your mind does not go straight to big pits and mining. Neither do you envision major technology advances coming out of the mining industry. However, you would be wrong. Innovation is happening at a very quick pace especially around automation of the most dangerous of jobs such as the giant vehicles that move ore around the mine.

Downtime is prohibitively expensive when the trucks are not rolling which includes fueling. Mines are now able to implement autonomous vehicles that are controlled, monitored, and managed centrally. This is all enabled by private cellular networks using the Cradlepoint dual modem solution in the R1900 with 5G. With VRRP, virtual router redundancy protocol, and dual modems provide the bullet-proof connectivity that is required.

Public Safety, First Responders, Surveillance

The challenges

Public safety organisations are facing extraordinary challenges in today's world, from preventing terror attacks to search and rescue if a catastrophic fire or flood occurs. In times of extreme threats and catastrophes, the demand for intelligent and reliable public-safety solutions is stronger than ever.

Reliable and rapid communications will be at the heart of any such solution. One area involves first responders in vehicles transmitting data to stationary systems as when an emergency medical vehicle approaches a hospital emergency room; the vehicle communications will be mobile but at that point must connect with static hospital systems, which could include PCN. Equipment in public safety vehicles is becoming increasingly connected – where is a certain item? Is it ready for use? Then there are the vehicles themselves – where are they? Are they operational? Images and location data must be transmitted, databases accessed, while many systems include voice, not just data. All of this will continue to generate increasing volumes of data while interoperability between a variety of systems and protocols for both mobile and stationary applications will be required.

Applications

Video surveillance systems

Public warning systems (Macro Cells)

Automated emergency response systems

Mission critical data for first responders

Drones

The connected policeman; biometric sensors worn by police and other first responders

Environmental sensing – e.g. toxic chemicals, gases

Public Safety, First Responders, Surveillance

Case Study – Private LTE Networks in Critical Infrastructure

The critical infrastructure sector is becoming increasingly vulnerable to security threats. The latest global threat report by Subex which monitors attacks on its honeypot network of over 70 cities worldwide, reported that 71% of cyberattacks in 2020 were on critical infrastructure. These alarming statistics and the complexities of securing IoT devices in multiple locations has led to many organizations in the sector looking to private networks as the answer, the ability to safeguard critical networks by keeping them inaccessible from the Internet is key to this strategy.

One such organization acquired private spectrum in the US market, with the intention of providing broadband services across private LTE networks for enterprises in the critical infrastructure space. However, as the private network was being rolled out, the organization required secure transitional connectivity services for its customers based on public networks. Key to the project was the ability not only to secure the data over public networks, but to ultimately provide a way for IoT devices to seamlessly move between public and private networks without compromising the security of the data they were transmitting.

Pod Group provided a solution based on eUICC connectivity. Since eUICC allows for multiple network profiles to be enabled on the same physical SIM card or embedded chip, it was possible to include both public and private network profiles which could be added, removed or updated Over The Air (OTA) without the need to access the physical devices. This meant that as the private network was rolled out, customers in the critical infrastructure space could transition seamlessly from public to private network access, and if the use cases required it, continue to securely roam on and off the private network. The implementation of Expeto's Evolved Packet Core (EPC) as a software within the private network ensures that data can continue to move between the public and private networks across the IPX backbone, meaning that data does not touch the public internet. Additionally, Pod has deployed its network monitoring and threat detection software, Pod Protect, to identify anomalies on the network. Since pLTE allows network slicing, if devices are compromised, they can quickly be quarantined in a separate network slice preventing threats from affecting the rest of the network.

Water Utilities

The challenges

The challenges to providing water to households and businesses today and in the future are manifold. They include

- Climate change –the long-term effects of flooding and drought
- Population growth and demand for more clean water
- Governments bring prosecutions against water companies for pollution incidents and regulate water quality standards
- Leakage from old pipes and infrastructure is costly; e.g. 20 per cent of the total water supply in the UK is lost every day through leakage.

Water supply networks in the developed world are coming under increasing scrutiny, making large scale replacement likely in the near term, while at the same time shortages of clean water are forecast worldwide. The construction of major infrastructure assets like new reservoirs and desalination plants is forecast for the near term, as well as new pipeline projects to support bulk water transfers between different localities. The overhaul is likely to require both civil engineering and smart digital technologies, such as the IoT, big data, artificial intelligence and digital twins.

Private cellular networks will assist in monitoring the activities of water treatment plants and sites, including sewerage works.

Applications

Leak detection using high-tech acoustic loggers and electronic sensors to pick up vibration

Lone worker safety in hazardous environments

Operational equipment monitoring

Drones for site inspection including storms overflows

Remote water quality monitoring e.g. treated water going back into rivers

Video for site security and intrusion detection

Environmental sensing for pollution incidents, environmental damage, leaks into groundwater etc.

Airports

The challenges

Airports need to be prepared not only for the continuous growth in passenger numbers, but also the demands of passengers. They must avoid safety breaches, comply with changing regulations, and ensure a stress-free experience for passengers. A 2020 report from SITA found that in 2019, 25.4 million pieces of luggage were mishandled around the globe, costing the air transport industry approximately $2.5 billion.

Airports comprise a complex environment in which very large numbers of objects need to be connected, often in real time. A smooth trip is largely dependent on data, from sharing travel documentation to monitoring the flow of baggage between airports. According to SITA, a passenger may interact with up to 10 different entities in a single trip - from airlines, government, ground handlers to at least two airports -- all of which requires the secure exchange of data on baggage, flight and travel documents. The use of real-time data allows airports and airlines to allocate their resources more effectively, which means gates, checkout counters and baggage centres can be properly staffed, and unexpected events such as weather and flight cancellations can be dealt with promptly.

The requirement to support large quantities of data transmitted reliably in real time makes private cellular networks a good choice for airport wide connectivity.

Applications

Cargo systems: Loading and tracking, including passenger luggage tracking

Asset tracking: Tracking the current condition, location, and operational status of other assets

Flight data download for airlines

Digital signage for flight schedules

Operational Equipment Monitoring, including predictive maintenance

People moving systems; sharing real time queue movement info enables improving the way that people move through the complex, reducing waiting times and queue related stress

Video surveillance – for security, detecting passenger overcrowding, etc.

Environmental Sensing: Clean air, temperature control

Apron vehicle navigation loading and unloading of goods, fuel on the tarmac

Drone hazard management – rogue drone detection

Airports

Case Study – Paris Airports

Groupe ADP develops and manages airports in France, including Paris-Charles de Gaulle, Paris-Orly and Paris-Le Bourget. In 2019, more than 108 million passengers passed through Paris Airports.

Groupe ADP, its subsidiary Hub One (an operator of digital technologies for businesses) and Air France have selected Ericsson to deploy a private mobile network covering the three Paris airports: Ericsson will develop the 4G/5G private mobile broadband network at all the Paris Airports in conjunction with Air France. This professional network will also serve an ecosystem of over 120,000 employees, who work at 1,000 diverse companies within the three Paris airports. The mobile network will be effective across all outdoor spaces at the airports by the end of 2020, and indoors across all public and reserved areas for professionals working at the terminals by the end of 2021. Ericsson's technology will also enable Hub One to comply with the new security requirements of France's National Agency for Security of Information Systems (ANSSI).

The programme represents a major step in the digital transformation of the Paris airports, and private 5G networks will enable and accelerate this transformation. It is expected to improve Hub One's operational performance in order to meet the expectations of customers and employees, through delivering the security, reliability and speed which are key to ensuring a good travel experience. Today's airports are fast evolving into smarter operations: becoming better connected improves their efficiency, allows them to offer a safer, more streamlined travel experience and helps to reduce costs.

Ports

The challenges

Ports are busy environments and becoming more challenging as container shipping continues to grow, even as the size and capacity of vessels increases, 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. Inefficiencies can cause expensive shipment delays. Security – "cybersecurity" and for goods -- is also major issue.

Port congestion can lead to additional safety and environmental challenges.

All of these challenges increase the need for port automation.

A large port may typically feature:

- Millions of containers shipped in and out in a year
- Thousands of trucks delivering and removing loads daily
- Daily train operations
- Hundreds of staff on-site with communication requirements for voice and data
- Potentially tens of thousands of sensors across the site
- A site covering tens of square kilometres
- Major port assets numbering in the hundreds, including cranes, RTGs, AGVs, etc.

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, on-site staff require voice and data communications. Sensors measure and monitor environmental conditions, tracking of assets and security across the site.

Applications

Autonomous/Semiautonomous vehicles (cargo moving)

Environmental Sensing

Docking Ship Communications

Video (Surveillance)

Drone (Inspection)

Operational Equipment Monitoring

Remote Control: Stationary machines e.g. cranes

Remote control – loading bays

Robotics material handling, warehouses

Bus & Railway Stations

The challenges

Bus and railway stations have to operate smoothly at all times, avoiding disruption, in order to create a smooth and safe experience for travellers. Monitoring and surveillance technologies are key to all activities, through facilitating arrivals, departures and everything in between.

For arriving passengers, systems for smart parking, wayfinding, point of sale transactions for ticketing, reservations and handling luggage are needed; in the station, safety, comfortable ambient conditions, temperature, lighting, current information displayed on digital signs, notifying passengers of platform changes or timings; on departing, finding onward transport by taxis and buses.

For staff, the incidence of abuse and violence against railway workers has increased of late. Some UK based stations have equipped staff with body worn cameras; studies have shown that violence is reduced because of the deterrent effect.

Railway stations are also a target for terrorists as they are crowded places, hence there is an increasing need for surveillance and readiness to summon emergency help.

Many applications require the collection and transmission of data in real time, either through fixed networks or wireless. Much of the data will feed into general logistics and station management systems. Private cellular networks fulfill needs for security, reliability and speed.

Applications

Environmental Sensing – temperature, air quality, ventilation

Lighting and heating; balancing efficiency and cost control with passenger comfort

POS transactions – ticketing and reservations

Digital Signage – keeping timetables in sync with actual arrivals and departures

Smart Parking – for motorists, notification by smart phone of free parking spaces and their location; smart bus parking also to avoid confusion

Luggage Systems tracking including safe storage of left luggage

Wayfinding of entrances and exits (including emergency exits), waiting rooms, cafes, facilities, platforms, taxi ranks, bus stops

Security – monitoring out of bounds locations, station perimeter trespass

Worker safety – body cameras, alarms

Vehicle Telematics – railway station vehicles, trolleys loading luggage

Video surveillance to monitor premises security, crowd behaviour

Facial recognition systems in case of suspicious behaviour

System for social distancing, Covid-19 compliance

Warehouses & Logistics

The challenges

Warehousing and logistics operations are moving towards increasing automation. This will fulfil several necessary goals for the industry, including timeliness, efficiency, rapid turnaround of goods and worker safety. All of this goes with the digitisation of previously paper-based and manual processes and the integration of data to connect with upstream and downstream processes. The desired goals include:

- Timeliness – rapid and error free flow of 'goods to box'
- Accuracy of location, with the help of QR codes, RFID tags
- Digitising previously paper based operations e.g. Bill of Lading
- Worker Safety, including avoiding injury from moving heavy vehicles and health risks from the Covid-19 pandemic
- Ensuring optimal conditions for products being shipped including for example, cold storage for medical supplies, foodstuffs. As shipments of temperature-sensitive merchandise increase, ever more stringent regulations are needed for their transportation.
- Greater automation: The use of robots is gaining traction, as humanoid robots with artificial intelligence, cognitive language and fine motor skills are being commercialised.

Robotics control can also be integrated with warehouse management systems and enterprise resource planning software.

5G in conjunction with private cellular networks will support the need for immediacy and reliability of data collection needed for these operations.

Applications

Vehicle Telematics to minimise fuel usage, ensure optimal working

Yard logistics– drones for localisation and inspection outdoors

Warehouse drones for inspection

Asset tracking including goods identification and data capture, smart pallets to track and trace goods and their containers, avoiding errors

Lone worker safety and alarm generation, avoiding risk of collisions with heavy moving equipment

Inventory management and smart freight management e.g. Digital Bill of Lading

Robotics for automating stacking, storage, retrieval, loading and transporting goods; improving efficiency, reducing errors, increasing speed of task

Indoor positioning systems where GPS signals are not available

Autonomous self-guiding vehicles

Environmental sensing, to maintain cold temperatures and to assure on-site air quality and comfortable temperatures for workers

Operational equipment monitoring in real time, with predictive maintenance to minimise downtime

Security and access control perimeter security geofencing.

A relatively recent type of application aids Covid-19 compliance and social distancing. This helps companies enforce Covid-19 site health and safety procedures for the workers. It verifies on-site social distancing compliance and helps enforce customisable device cleaning procedures while applying digital tracing to workers who have handled the merchandise.

Large Retail, Stadia

The challenges

Stadia are connected venues with the primary aims of ensuring safety and enhancing spectator experience. This includes security, ease of finding, comfort. Thanks to the universality of smartphones, apps are proving to be invaluable for engaging with fans at live events, from finding parking spots, locating seats, and ordering food, etc. Here connectivity is vital, not just for fans, but for venue staff and suppliers.

Likewise retail parks and shopping malls are involve enhancing and facilitating customer experience and safety. Both typically provide many wireless access points.

Like railway stations, shopping malls and stadia are crowded places when they are open, and potential targets for terrorism. Hence there is a need for surveillance and readiness to summon emergency help and ensure safe evacuation rapidly. Enabling immediate responses necessitates the availability of real time data. Transmission of images in real time necessitates high bandwidth.

5G, ultra-reliable and low latency communications will support large densities of connected devices. As enclosed spaces, stadia and shopping malls are good candidates for PCN networks.

Applications

Video surveillance for detecting overcrowded areas, perimeter intrusion; facial recognition technology for suspicious behaviour

Tracking – onsite equipment e.g. trolleys

Environmental Sensing – ambient temperature, air quality

Smart lighting

3D Wayfinding, omni channel indoor navigation – plus interfaces for locations, points of interest and services.

Digital signage, including Interactive maps and plans, intelligent signage for entry and exit points, facilities, etc.

Specialised hospitality applications e.g. gaming machines

Smart parking

Visualisation apps in retail: Providing customers with product information; AR and VR for immersive customer experience including virtual mirrors, virtual dressing

Specialised retail applications e.g. Electronic shelf labels

Intelligent Kiosks

Supply chain monitoring

Connected bluetooth beacons providing product and “flash sale” information to passing customers

Vending machine monitoring

Automated checkout

POS transactions, connected payment solutions, ATMs

Large Retail, Stadia

Case Study – Attraction Venue

Amusement Park attractions demand controls and sensors to ensure a consistent and uncompromisingly high level of safety – lives quite literally depend upon it. Traditional safety and control systems for attractions were based on Programmable Logic Controllers (PLCs), sensors and miles of wire to connect elements. While this used to be the gold standard, the total cost of ownership, reliability and ever evolving rider experience have pushed this design beyond its reasonable limit.

Wired communications for control systems and safety only work well when the attraction has a fixed route. However, modern attractions often offer dynamic experiences and routes based on rider input. Introducing additional technological elements – such as video streaming presented through augmented reality goggles – further complicates traditional control systems, as such elements can require high bit IP networks that Wi-Fi cannot satisfy. This is because Wi-Fi Access Points (APs) have a limited broadcast distance, making handoff between APs problematic in large areas. Additionally, Wi-Fi spectrum in the US is unlicensed, which allows for radio frequency interference.

In an effort to overcome these drawbacks of Wi-Fi, Expeto recently tested cellular capable PLCs running on Citizens Band Broadcast Radio Service (CBRS) at a major U.S. amusement venue. CBRS was launched in the U.S. within the last two years and allows virtually anyone to set up private cellular services. The test sought to find alternative wireless connectivity options to enable the mission critical operations of a large area attraction with a rider-determined route and augmented reality goggles.

Expeto found that our platform enabled cellular capable devices, including PLCs, to run a consistent traffic load with zero packet drops or disconnections according to the required intervals to meet the strict standards of this customer. This is because cellular was designed for transmission speed, secure connections, hand off between APs, higher transmission power, and licensed spectrum bands. As such, Mobile Networks based on cellular technology offer an excellent balance between cost of ownership and the engineering capabilities required to operate safely at high speeds with very high data bit rates in large geographic areas. This test demonstrated vast operational improvements delivered by Private Mobile Networks (PMNs) using cellular technology over Wi-Fi in an industrial setting.

Large Retail, Stadia

Case Study – Large retail complex

Retail locations take users beyond shopping. They are full entertainment complexes that usually coexist with sports venues like football, baseball, or hockey. They are small cities unto themselves. The fiber runs that would eventually be needed for security, digital signage, etc. are not known or designed for during the initial construction and are costly to put in after construction. This is where private cellular networks fit the bill.

These complexes are deciding to put private cellular networks in to provide connectivity and efficiency across multiple use cases such as parking lot open spaces, security video surveillance, ticketing machines, as well as other IoT uses across the entire complex. These facilities have extended the connectivity while providing greater visibility and control of the network traffic across the overall infrastructure. They are also experiencing greater performance while keeping the overall cost of the expanding projects low.

Your wide areas need Private Cellular Networks

Total control of your own network

The ability to completely control network performance while drastically reducing monthly costs and risk of data breaches makes Private Cellular Networks with Private LTE/5G routers the best available wide-area LAN option for many situations across a variety of industries.

- Cover the edge with enterprise-grade equipment
- Leverage cellular while paying nothing for data
- Roll out new levels of network security
- Guarantee excellent connection performance for all
- Maximize your IT team with centralized management
- Protect against the elements with ruggedized gear

IoT sensor data at distribution centers

Smart City lighting and meters

Distance learning for students at home

Safety devices at oil and gas refineries

Security cameras on school campuses

Telemetry on cranes at shipping ports

cradlepoint

Learn more at cradlepoint.com/pltenow

Primary Research

Exclusive series of interviews with senior management, from key businesses across all industry sectors, highlights the operational challenges being met by PCNs and where companies are successfully adding new value. Our unique survey of IoT buyers also highlights where businesses feel PCNs offer value add and complement existing solutions.

Industry Expert Interviews

- **Question 1.** What type of solution and service do you offer?
- **Question 2.** How has COVID impacted Private Network adoption?
- **Question 3.** What are the main drivers behind Private Networks?
- **Question 4.** How is the market developing?
- **Question 5.** Can Wi-Fi and 5G coexist?
- **Question 6.** What are the key verticals?
- **Question 7.** How is the CBRS market developing?
- **Question 8.** How will the 6 GHz band be employed?
- **Question 9.** What are the future trends?

CLICK THE QUESTION TO GO STRAIGHT TO THE ANSWERS

Question 1. What type of solution and service do you offer?

One of the oldest companies in the private networks space. Started with aircraft 20 years ago.

Senior Vice President, Marketing & Business development

A leader in development of shared CBRS capabilities, played an important role in the formation of the CBRS alliance.

Senior Director Technical Account Management

Leading global provider of ICT infrastructure and smart devices.

Chief Digital Transformation Officer LATAM

A large global company active in construction, transport, and solar power.

Antenna Product Engineer

Global company specialising in large private cellular networks for rail projects, mines, and public spaces.

RF Engineering Director, Central Europe

Global company based in US, specialist antenna supplier.

Sales and marketing

Enabling humans to interact in quasi real-time with cyber-physical systems in the real or virtual world over intelligent wide-area communication networks.

Systems Architect

City wide network set up a standalone company for a 5G testbed. The network must guarantee coverage wherever people may live.

Technical Manager

Specialist vehicle Manufacturer.

Manufacturing technology engineer

Global OEM partner in the production of more than 3.7 million vehicles in over 30 different models.

Process Engineer

Software provider based on 3GPP standards using 4G, 5G technologies.

Head of Business Development, North America

Leading player in the CBRS ecosystem, providing a portfolio of licensed and unlicensed wireless products.

Director, Solutions Architecture

Established connectivity and software solution provider.

Chief Executive Officer & Founder

Solution provider in private networks, private LTE in smart ports, rural wireless broadband, and emergency connectivity.

VP of Marketing and Business Development

Q.1 cont... What type of solution and service do you offer?

Enterprise Wi-Fi 6 solutions, private 4G/5G networks and LPWANs.

Co-founder and Executive Advisor

Major Neutral Host operator in the US.

SVP & Co-founder

Indoor and outdoor cellular and public-safety communication provider.

VP Business Development

Question 1 Summary...
The interviewees were all at senior levels of their organisations – CEOs or heads of departments. They included a broad range of companies from large manufacturing multinationals to smaller specialist companies including start-ups and software providers, engineering, and manufacturing companies. Activities included private networks, neutral host solutions, DAS solutions, CBRS technology and deployments, and Wi-Fi 6 networks.

Question 2. How has COVID impacted Private Network adoption?

The impact has been significant, positive as well as negative and it's nuanced. On the positive side the pandemic has highlighted the importance of robust, fast, low latency connectivity, which is needed to meet the demanding requirements of mission-critical applications.

Overall demand for 5G and private networks has been down slightly in North America and South America as well as Europe. In education and healthcare demand has increased significantly.

The pandemic triggered a rapid adoption of digital channels. People had to make changes fast and there was a surge in mobile connectivity. We had projects before the pandemic to provide a deeper and more seamless mobile Internet. This essential need is now widely accepted.

The restrictions on movement and quarantine time were an ongoing challenge but it did not slow down the rollouts of our projects. In fact, there is more widespread understanding now that modern networks directly affect how we can operate. It is no longer just a question of faster downloads; full coverage of remote areas and reliable, low latency uploads became a key a topic.

The pandemic has highlighted the need for reliable communication as cornerstone for business flexibility. Now there is an understanding that digital transformation is something that should have started much earlier, been more consequent, with people's needs and abilities at the centre.

Our campus solutions are operating and have been used for new projects during the pandemic. We could take advantage of the empty surroundings during lockdown and managed practical trials with visitors from other countries safely.

Q.2 cont... How has COVID impacted Private Network adoption?

- Communication over the internet have become essential in the pandemic. Our network keeps in touch efficiently and it has proven the right track to manage the funds for social needs, especially in changing times.
- We had to look after our staff differently and handle supply shortages. The demand for modern vans increased and neutral hosting became more important during the pandemic. The use of private networks expanded.
- The whole industry got stress tested last year and restarts have been challenging. There were big questions over supply resilience and the faster introduction of new products. There was a change in strategy for the rapid adoption of technologies that supported agile operation. The ability to handle more data over private mobile networks and to process and store data was a key enabler.
- Hospitality and hotels have been severely impacted. Recovery not foreseen before 2022. On the other hand, the educational market, which was almost unknown, practically non-existent, has really taken off, because of the need to provide broadband to students in rural areas.
- It has certainly had an impact on indoor networks, where we have seen an increased demand. It has also changed the focus on the use of Private Cellular Networks, now there are use cases that are being used to solve problems created by Covid. For example, cameras that analyse if people are maintaining proper social distancing.
- We have seen more demand in the public sector, e.g., education, to deliver connectivity and broadband access for students and distance learners. Governments have made significant investments in these areas. Hospitality have been severely impacted; nobody is investing.
- We have seen more market demand in distance learning over the last six months. In addition, there is a lot of interest from the industrial sector, mining and manufacturing in Canada and the US.
- The pandemic has slowed down private cellular network adoption. Companies were more focused on dealing with the immediate crisis than looking at longer term strategic choices. Overall, Covid has increased awareness of 4G/5G private networks to improve productivity, and to secure business critical operations. By the end of 2021 we expect demand to increase significantly.
- There has been an increased demand for fixed wireless access, bringing connectivity to rural areas such as schools. More momentum in smart city applications, e.g., social distance monitoring, occupancy sensing, and wastewater monitoring. Manufacturing will pick-up with 5G adoption, there will an increase use of computing vision capabilities combined with AI. It is going to be mission critical or at least business critical applications with high/low latency requirements. 5G will be required.
- The demand in DAS (Distributed Antenna Systems) has been stable. There was a slowdown in hospitality, but more demand in the healthcare sector, and a very high demand from universities. At the moment there is less demand for in-building coverage because more people are working remotely.
- High market demand, no slowdown. Five new networks built in the UK. Large scale private network deployments announcements in 2020 in industry, ports, and three major airports.

Question 2 Summary...
Covid's impact has been significant, positive in some sectors, negative in others. But overall market demand was high and there was no significant slowdown. There was increased awareness of 4G/5G private networks ability to improve productivity and competitiveness. The pandemic has also highlighted the importance of robust, fast, low latency connectivity, which is needed to meet the demanding requirements of mission-critical applications.

On the negative side there has been a significant impact on the hospitality industry, hotels and both business and holiday travel. Investments in 5G have continued and innovative solutions have been announced. And there has been an increase in the deployment of fixed wireless access solutions, which bring robust connectivity to rural areas such as schools.

Question 3. What are the main drivers behind Private Networks?

They come from the mission-critical requirements of businesses, which are very much IoT related. We are seeing more and more IoT cellular devices in factories operating in 4G and 5G networks. Covid has created new opportunities such as remote working. The transport and logistics sectors have been earlier adopters; they want to monitor high value goods and see where they are losing money. In the oil and gas industry companies predict deployments of IoT maintenance solutions that can fix issues in about four minutes. Four years ago, it took a week to get the engineers on site.

The need for connectivity is greater than ever. Private networks will increase quality of services in Industrial IoT sectors and minimise Wi-Fi interference issues. We are seeing demand for more automation across the manufacturing and warehousing sectors. Typical use cases are remote control of production lines with automated carts, robots, connected screwdrivers etc. In general the pandemic has accelerated the need for more automation and flexible manufacturing. and 5G networks, using either licenced or unlicensed spectrum, look set to accelerate the deployment of massive IoT systems.

Remote learning is moving at a very fast pace, particularly over the last year, given the events of the pandemic. It has a huge momentum right now, more in the US than in Europe. In North and South America, also in the UK, there is a lot of effort from the government to deploy LTE virtual networks in LTE because they want to introduce private networks in education and healthcare.

The main demand comes from enterprises and commercial buildings that lack good cellular coverage indoor. We see a demand for private cellular networks for 5G in the US and this is related to IoT applications, particularly in manufacturing and warehousing, and more recently to higher education.

There is a need to own the means for future productivity, especially in big companies, and there are bottlenecks regarding performance. For example, better handover for moving devices and wider coverage plus evolving network functions for low latency processing or low powered devices.

The drivers are as strong as ever and have to do with control over running costs, ability to negotiate, independent data processing, clear control, and performance gains by localising end to end solutions. Advanced cloud analytics can increasingly be used to run more distributed, complex networks globally.

Mobile network coverage needs to be extended. Indoor and underground coverage requirements for safety and automation require solutions that enable the use of those spaces. Private networks bring the operation together.

We specialise in 5G campus solutions. Our clients demand short latency processing mainly for robotic functions, testing and integrated mobile solutions. Current solutions pool together public and industrial spectrum for high performing reliable systems. Interference is kept to a minimum and local data processing shortens reaction times and lowers costs.

It allows scalable mobile robots and self-driving transport between production cells. It puts the academic concepts from nearby university into practice.

The city's project started as a push-to-talk project has scaled to support IoT and gaming, artificial intelligence, robotics, and virtual reality.

It is a vital part of the connectivity mix. Essential for agile manufacturing, mobile equipment and radar and video sensing throughout the factory. Many of our clients' vehicles have mobile cellular technology on board. We need to be able to develop, test and run complex manufacturing processes globally and need matching data processing and connectivity.

Q.3 cont... What are the main drivers behind Private Networks?

- Private video networks and robotics are the most active use cases that are being explored. We see much more IoT data than voice on private cellular networks
- One driver is dissatisfaction with the quality of service provided by MNOs (Mobile Network Operators). And in security, companies are embracing private cellular networks to increase security and the need to operate in a closed environment.
- We see more manufacturers using robots, security cameras and automated guided vehicles that requires high bandwidth, low latency. There is increased interest in agriculture where connectivity coverage is very low and there are international deployments in the shipping and transport logistics industries.
- Wi-Fi is a driver that is enabling increased automation in manufacturing. Wi-Fi 6 and Wi-Fi 6E are well suited for edge computing. Wi-Fi solutions are cost effective; DAS is too expensive. Wi-Fi deployed in hospitals enables Internet access to visitors.
- Many companies are deploying private networks to gain sovereignty in their operations, i.e., secure sensitive data. They are embracing private networks to increase security by employing a closed environment. The primarily objective is to have a dedicated, isolated, protected, and secure communication systems for their data needs.
- In buildings cellular phone coverage is often very poor. We can solve these problems with our DAS solutions. There is a high demand for bandwidth and more video controlling applications. With DAS we can integrate private cellular networks and public safety communications.
- A key driver for our enterprise customers is the need to and address Wi-Fi's limitations. Private cellular network benefits versus Wi-Fi are better performance, increased reliability, and enhanced security. AI enabled computer applications require industrial private networks. Private LTE networks deployed in ports are being used to lowering CO2 emissions, make them more efficiently, identify trucks arrivals, and verify containers using cameras systems.

Question 3 Summary...
Private networks are being deployed in all major industrial verticals. They facilitate the deployment of automated and remote operations, for which there has been an increased demand. Advanced applications such as machine and voice recognition are another driver. They leverage the benefits of edge computing, e.g., real-time analytics. Industry 4.0 is focused on productivity; uptime-downtime optimisation.

The huge increase in online shopping has resulted in growth in computer vision systems, needed to track the delivery of parcels and boxes. Connected healthcare is another key driver and large solutions have been deployed in hospitals in the Netherlands, where they are used to connect to nurse calls systems to improve patient outcomes. Healthcare's primary focus is on mission critical applications, looking to save lives.

People moving from big towns to small towns want to upgrade to better connectivity for remote working and data security is an important reason for investing in private networks. Another driver is dissatisfaction with the quality of service provided by MNOs. There is increased interest in agriculture where connectivity coverage is very low.

Question 4. How is the market developing?

- Private networks are making progress, with Germany leading the way. Some of the biggest enterprises, e.g., Volkswagen and Lufthansa are purchasing unlicensed spectrum, they are not subscribing to MNO services. It will be interesting to see if that approach to enterprises owning their network, buying their own spectrum, and deploying their own equipment evolves. The UK, Finland, and Holland are the most dynamic in terms of demand.

- France has been a little slower because the regulator decided to charge over 100,000 euros a year to access to spectrum. Therefore, the bigger players are involved; EDF, Air France, and Airbus. Italy is one of the biggest markets for fixed wireless access Two leading mobile operators have built solutions in the last six years.

- Many companies will employ 5G to make last mile connection for fixed wireless access to homes and small businesses. There will be an increase in migration from LTE to 5G since it is relatively easy. Interest in edge computing and AI that will use 5G is growing in manufacturing. Neutral-Host has not really started yet in Europe, but it might in 2022-2023.

- In North and South America, also in the UK, there is a lot of effort from the government to deploy LTE virtual networks in LTE because they want to introduce private networks in education and healthcare.

- CBRS (Citizens Broadband Radio Service) in the US has been very successful, and the ecosystem has rapidly expanded. There are over 10,000 deployments covering a wide range of use cases and they are set to grow significantly next year. Neutral Host was expected to provide a big portion of growth but there hasn't been much participation from carriers and has is slowing deployments.

- Port of Zeebrugge and Paris/Brussels Airports are having 5G network trials. Transport and logistics are the largest verticals that are testing 5G networks. Germany and Italy are the most dynamic countries for 5G personal cellular network trials. The German Federal government has responded to requests from the manufacturers to allocate spectrum slices for local private networks.

- Enterprises are being encouraged to build and use their private networks. Carriers do not have resources and bandwidth to deploy in building support for the six billion commercial buildings in the US.

- Companies and institutions changed their data strategies and existing technologies, which were often overstretched. Private networks are part of this stabilising response, they make information systems more resilient.

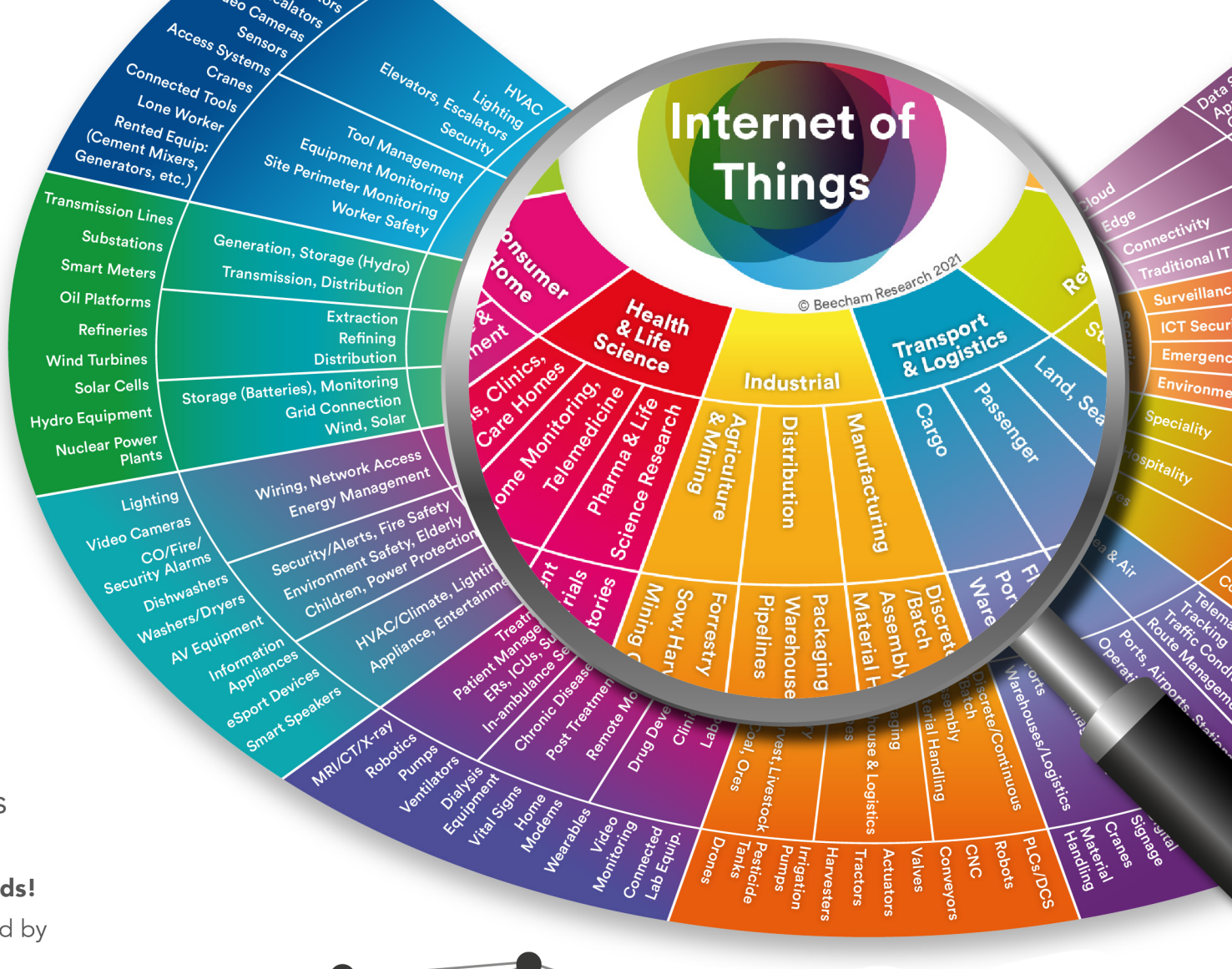
- The re-farming of TV spectrum in the UK finished before its deadline. 5G technology is now being used in low far-reaching bands of the spectrum and adds to the traditionally private networks of utilities in the 900MHz and 450MHz domains. Large projects for cellular rail networks and private cellular networks on ports are being build. On Campus networks all modes of private networks are being tested in the real world. Hybrid operations from 4G to 5G are widespread and the stand-alone installations have started.

- The need to communicate effectively in warehouses without dead zones and to look after employee's welfare has been mirrored in other business sectors. We have seen a need to overcome damaging isolation in healthcare and there has been a fast adoption of online consultation and monitoring.

THE IoT WORLD MAP

The first-ever interactive IoT World Map

The ultimate planning tool and marketplace for IoT buyers and sellers



Explore the world of IoT in the palm of your hands!

The entire ecosystem, every IoT application mapped by sector, type and 'things.'

Find the right product, partner or supplier in IoT

Click here

www.iot-now.com/world-of-iot

To get listed, contact Lauren Auret
e: l.auret@wkm-global.com

IoTNOW
HOW TO RUN AN IoT ENABLED BUSINESS

In association with beecham research

Q.4 cont... How is the market developing?

The market wants easy to use systems and interaction with intelligent systems became more important. We expect to see a major shift in how machines learn and interact with people. This requires changes in networking, computing, and interfacing. There has been a demand for high performing connectivity.

The partnership with local academia created a practical ecosystem. Our company has been transformed and high performing networks are at the core of future agility.

There is a need to produce more sustainable vehicles and answer the calls for advanced mobility. Physical transport systems have continuously driven communication technologies forward.

Neutral-Host has not really started yet in Europe, but it might in 2022-2023. Unless regulators pressure the mobile operators the market will be slow to develop. In the UK three or four banks were looking to deploy a neutral host system but, in the end, did not. One bank decided to go for a cheaper DAS solution.

Question 4 Summary...
Wi-Fi 6E has become a hot topic and there is a synergistic relationship with the new 6 GHz band, which provides a 1200 MHz bandwidth for both licensed and unlicensed spectrum. This opens up opportunities for virtual reality, video surveillance, robots, remote maintenance and drones. Demand for wireless is growing enormously and users want more bandwidth and faster speeds.

More companies and using edge processing and the edge decision making but it is not widely used in the US and Europe. Until 5G develops and this will take a couple of years.

Private networks are making progress, with Germany leading the way. Some of the biggest enterprises, e.g., Volkswagen and Lufthansa are purchasing unlicensed spectrum, they are not subscribing to MNO services. It will be interesting to see if that approach to enterprises having their own network, buying their own spectrum, and deploying their own equipment evolves. The UK, Finland, and Holland are the most dynamic in terms of demand.

France has been a little slower because the regulator decided to charge over 100 000 euros a year to access to spectrum. Therefore, the bigger players are involved; EDF, Air France, and Airbus. Italy is one of the biggest markets for fixed wireless access Two leading mobile operators have built solutions in the last six years.

Question 5. Can Wi-Fi and 5G coexist?

5G provides both wide area and local coverage with full mobility. It is the best fit in critical use cases requiring high reliability, low latency connectivity, enhanced mobile broadband, fixed wireless access, massive machine type communication and critical machine-type communication. Wi-Fi 6 is suited to indoor or local area deployments and uses cases demanding high speed, and best-effort traffic, and non-critical uses cases.

Wi-Fi 6 will increase network speed, reduce congestion and at a local level reduce interference in high device deployments. 5G will complement Wi-Fi in wide area solutions. 5G and Wi-Fi 6 will co-exist and the two technologies will improve the overall end-user experience. In the long term 5G will dominate. Coexistence will continue for the next five years.

We support all frequencies up to 6GHz, for any technology and develop product for future 5G bands.

It will create more demand and enables more diverse connectivity modes, mainly at the device level. There are a number of private networks in ports that employ cellular as well as Wi-Fi nodes at the same time.

Wi-Fi co-exists with cellular and other wireless technologies. Data often flows directly between different network technologies and there are new service offers that often depend on both.

Both technologies have broadened their capabilities and work best side by side. It is important to develop ecosystems.

They are a good match. The expectations for Wi-Fi 6 coming to homes and offices are high right now. That will impact fibre, air-link, cellular, copper and satellite networks. Our private network brings fibre like connectivity to the home or premise.

Both technologies have addressed a wider range of specifications and it will change what we want from networks, how we work and what is possible with our vehicles in future.

Wi-Fi 6 and 5G are the main wireless protocols in manufacturing. The in-car infotainment, C2X and future smart transport solutions will be built on both.

We have been successful with W-Fi 6 deployments and at the same time transitioning 4G private networks to the 5G technology band. We see the technologies as being complementary, for example Wi-Fi 6 being attached to the core of a 5G network.

Question 5 Summary...
Responses to this question indicated significant performance differences as well as coexistence for applications that require both types of connectivity. Wi-Fi 6 is ideal for indoor and local area deployments and non-critical use cases that require high speed, best-effort traffic. Cellular networks do not work well in buildings and will be mainly used to provide outdoor coverage.

Wi-Fi will become part of the 5G experience when Wi-Fi 6E operates in the 6GHz band. But it will not replace LTE and private cellular from a scale perspective, i.e., serve large numbers of users in a large area.

Question 6. What are the key verticals?

Industry is the biggest, oil and gas, green energy, manufacturing and mining, healthcare is the second. Fixed wireless access, that has become huge since Covid started. Education, with distance learning for students, has data connectivity issues. Neutral host is more difficult to develop because you need a partner that has a roaming agreement and mobile operators do not want to share their investment in coverage.

There has been a fast take-up of AR/VR on early adopter 5G networks. Traffic in this vertical is 4% on 4G networks and 20% on 5G networks.

Industrial applications are developing rapidly as manufacturers look to increase their automated operations. More real-time analytics is leveraging edge computing, there is increased of remote operations, preventive maintenance, and asset tracking of sensitive goods. Automation and robotics increase the demand for private networks.

Remote learning is moving at a very fast pace, particularly over the last year, given the events of the pandemic. It has a huge momentum, more in the US than Europe

Question 6 Summary...
Manufacturing emerged as the number one vertical; it includes robotics. Transport and Logistics was the second largest market; it includes drones. The third was the Public Sector. Other key verticals include: Healthcare, Airports, Ports, Smart Cities, Oil and Gas, Mining and Tourism.

Healthcare is a very complex vertical. Management is conservative; the deployment of advanced medical devices is very progressive; infrastructures are slow to adapt and change. Remote learning and working is a recent, fast-paced development because of the pandemic.

Question 7. How is the CBRS (Citizens Broadband Radio Service) market in the US developing?

CBRS is very successful, the ecosystem has rapidly expanded, we have seen more than 10,000 deployments covering a wide range of use cases. Three key cases have been identified: private cellular networks, neutral hosting, and fixed wireless access. CBRS has really helped the development of private cellular networks. Fixed wireless is the leading use case; there is a big market opportunity in smart factories, offices buildings, and warehouses, the objective being the modernisation of communication infrastructures.

Neutral Host was expected to provide a big portion of growth in CBRS, but we haven't seen a lot of participation from carriers. Hesitation from operators is slowing down deployments. I see the educational market expanding significantly because of the pandemic and I also expect to see the agricultural market expanding. Both markets are getting significant funding from the government, autonomous agriculture and 5G for in rural areas.

We see the advantage of spectrum homogenisation globally. The rules are different for the US and new models for interference and spectrum control might evolve for other bands.

Mid spectrum is a valuable resource, and the unique control mechanism provides opportunities for those bands in the US.

We use wider frequency bands dedicated for industrial, low latency applications to ensure continuous access for our clients. This opens up new ways of networking and closes the loop for advanced control systems.

It can help the US to not slip behind the connectivity challenges and will be a test bed for the three tiers within CBRS. We use wider frequency bands. The control mechanisms are of interest for new wireless technologies, especially for a mix of technology in truly unlicensed spectrum.

The details are very interesting. It's a way to access the mid-spectrum in the US. There are cellular networks on production sites that provide special services on only one carrier for cost reasons on relatively narrow frequency bands.
Fixed wireless access is growing. The industrial sector is still a learning curve on how to benefit from private cellular networks. Data security is an important reason for investing in this development, which gives businesses a lot more control and ownership on how they manage their data and make decisions.

The penetration of CBRS handsets at the end of 2020 was at 22%. By 2023 there will be combinations of CBRS spectrum with carrier spectrum. Enterprises are being encouraged to build and use their private networks, carriers do not have resources and bandwidth to deploy and support the six billion commercial buildings in the US.

Question 7 Summary...
CBRS will increase accessibility to connectivity at a low cost, on a pay as you go basis. It is still at an early stage; a lot of companies are not well informed, and some enterprises are not aware of this development. Some interesting statistics emerged re usage of the spectrum for private cellular networks. 29% think they will be developed and managed by operators and only 10% by companies.

Fully digitalized Distributed Antenna Systems (DAS) are being deployed, driven by the growth of IoT in US smart cities.

The penetration of CBRS handsets at the end of 2020 was 22%. There are some 60-70 devices that can use CBRS spectrum: sensors, smartphones, and specialised devices. By 2023 there will be combinations of CBRS spectrum with carrier spectrum.

Question 8. How will the 6 GHz band be employed?

- 6 GHZ is going to allow more of the same in a different spectrum band based on similar but slightly different technologies. Arithmetic frequency controllers will be needed for certain types of 6 GHz radios operating in unlicensed spectrum. All companies need more spectrum, so the market opportunity is very important. Whether it is private networks or those of mobile network operators. There are major opportunities virtual reality, video surveillance, robots, and remote maintenance.
- GSMA (Ericsson, Nokia, and Huawei) are having discussions with regulators, indicating that 6 GHz should be reserved for MNOs. In the US, Microsoft, Google, and modem vendors are promoting the idea that 6 GHz cellular should be assigned to Wi-Fi
- In the C Band the bandwidth is only 400 MHz of bandwidth. Operators can go directly to 24GHz-39GHz where there is a lot of bandwidth, but also a lot of deployment problems. Hence the need for an additional 6 GHz of mid-band spectrum. Spectrum issues are currently being discussed at the WRC-23 and at the GSMA.
- Now that the details are emerging, we can look forward to the new growth it will bring. The wider channels will enable the development of new devices. and we expect to see higher demands on networks for automation applications.
- It will give a big boost to last mile and point to point connectivity. We expect mixed technologies, just like in 5GHz, to scale up quickly, but there are challenges filtering between 5GHz and 6GHz.
- It is a vast amount of spectrum. It enables more data, and more devices. We do not see interference problems with the current power limits. The device support is impressive at this early stage. We do not offer cellular solution in 5GHz but will be watching wide channels in unlicensed mid and high bands.
- That is a major shift opening up large amounts of spectrum. We can start with less channels locally, as long as some channels can by 160MHz wide. It also allows very capable line of sight connections to link lower dedicated frequency use. We expect the use of wider channels to enable new practical solutions in robotics.
- We will start using the spectrum for indoor Wi-Fi. The parallel use of cellular technology is approved up to 5GHz as far as we understand.
- This is truly a game changer and will challenge back-haul as well as raise expectations. It is an exciting new development. The roll out of spectrum is under way, hardware components, devices and indoor solutions are becoming available.
- It allows a wider mix of connectivity options and is a big part of spectrum available. The propagation is similar to lower Wi-Fi frequencies. There are not enough details yet about the use of cellular in those bands.
- We see the 700MHz band as being more interesting, we are also preparing the 3.8-4.2GHz band. I am not sure that the eco-system is ready for the 6 GHz. It also is very challenging re the need to deliver the promises of 5G network slicing and massive type communications. In addition, chipset and modem suppliers are unlikely to enter this market until they see a big demand. This is a classic technology chicken and egg scenario.
- We foresee this band being used for: wireless robots that requires high capacity, drones, AR/VR, sensor networks and real-time video in smart farming, remote patient monitoring, digital signage, real-time connectivity for cranes in pots, and automated guided vehicles.

Question 8 Summary...
The 6 GHz band provides 1200MHz of bandwidth for both licensed and unlicensed use as well as faster speeds. Demand for wireless is growing enormously. 6 GHz provides a good balance between coverage and capacity for 5G, and it can support large contiguous blocks. Arithmetic frequency controllers will be needed for certain types of 6 GHz radios operating in unlicensed spectrum.

Reservations were expressed about the industry being ready for the 6 GHz. It is being challenged on the availability of 5G network slicing and massive type communications. Slicing capacity is not infinite, approximately five layers can be handled, so this limitation may influence the development of private networks.

Question 9. What are the future trends?

- Future trends include enterprise Wi-Fi 6 solutions, private 4G/5G networks and LPWANs. Applications include smart cities, Wi-Fi in schools, 5G network trials with mobile robots, self-driving vehicles, push-to-talk, push-to-video, real-time sensor data and drone communications.
- Neutral host and interconnected private LTE/5G networks, in-building connectivity using CBRS, private networks for enterprise communication and IoT applications.
- Higher frequencies have become a focal point for 5G and DOCSIS. Our solutions have no effect on LTE and sub-6 bands. Indoor coverage of 28 GHz can be enhanced without affecting legacy wireless frequencies. Customers will expect seamless switching from one connectivity technology to another.
- Lower frequencies are key for low powered devices and narrow band applications. We expect a swift scale out of networks using milliammeter wave frequencies. Some of those line-of-sight links will be later strengthened by active fibre. PON use will be optimised to give a better end user experience.
- Hubs that combine processing and connectivity will enable ecosystems. This will accelerate expectations for seamless wireless solutions.
- Challenges in visual computing, data security, software engineering, distributed systems, and robotics. Networks will automate onboarding and optimise range and latency for critical applications. A holistic approach to 5G system design is needed advancing hardware, wireless interfaces, networks, edge clouds all the way up to Tactile Internet applications.
- We expect a fast roll out for smart motorways, integrated transport solutions, defence, and medical assistance, plus repurposing existing telco-towers and fast expansion into uncovered regions with reliable meshed wireless networks.
- Manufacturing will become more flexible and connectivity will be a high priority for effective changes in operations to enable new smart production methods.
- Easier access to services and seamless transfer between connectivity technologies are going to be more important in future. Automation of networks will improve onboarding, scaling and user experiences. Automation of production will focus on flexible workflows and much better ergonomic interactions.
- The energy and utility sectors have not been fully explored. The providers are increasing their real-time energy control generation, extending their international network, and making greater use of private networks. The health sector is employing private 5G networks in hospital and between hospitals, but they continue to rely on public networks.
- Outdoor applications include smart transport systems, smarter motorways, and transmitting information directly into cars. Also charging points and energy storage systems.

Question 9 Summary...
Expect to see more companies partnering to offer a single private network solution. This market is taking off and big players are entering it. For example, Amazon has announced a partnership with Arris' Ruckus Networks division, Federated Wireless and Athonet to deliver a cloud-based private LTE network solution based on CBRS.

Right now, the 5G focus is on deployments but as more services roll out various trends will emerge as well as ecosystems created to leverage network slicing, massive machine-type communications, and ultra-low latency.

Ericsson Private 5G

What sets Ericsson apart?

ERICSSON

What sets Ericsson apart for CSPs?

- Easy integration to existing Radio assets
- Operation integration with existing Ericsson Network Manager

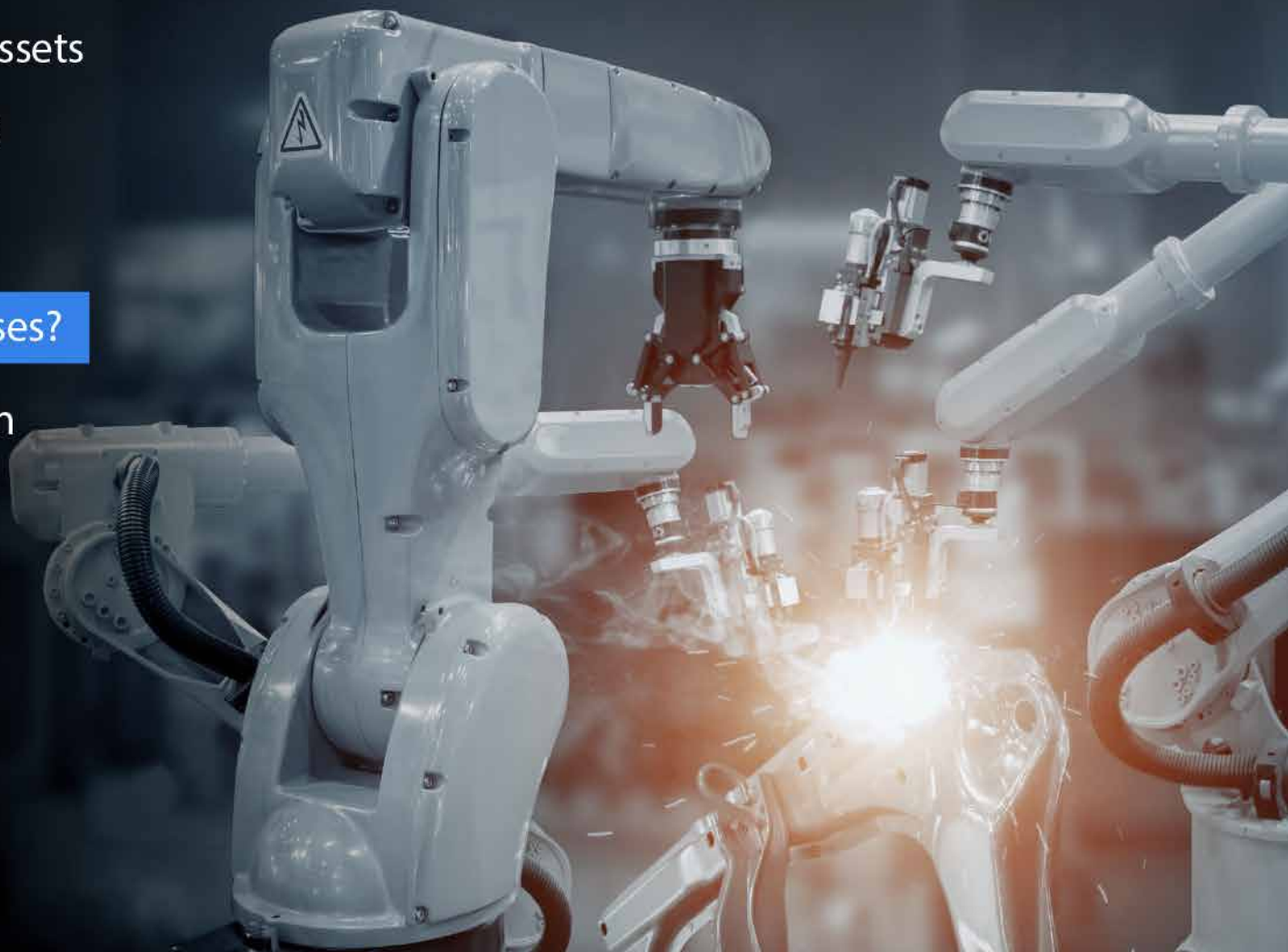
+ More

What sets Ericsson apart for enterprises?

- Easy to install fully managed system on single server
- Enterprise UI and easy to use API to allow for easy integration into IT/OT environments

+ More

Find out more here



User Survey of the Market

Introduction

As part of the research for this report Beecham Research conducted a user survey. This was aimed at verified IoT buyers (also referred to as adopters, meaning adopters of IoT solutions) from all sectors and all geographies. The commentary for this also draws on some of the one-on-one interview findings earlier in this section to add more depth.

All major sectors were represented, as shown in **Figure 3.1** – what is your business unit's primary business? **Figure 3.2** illustrates the geographic spread of respondents and **Figure 3.3** shows their company size in terms of number of full-time staff.

Figure 3.1 *What is your business unit's primary business?*

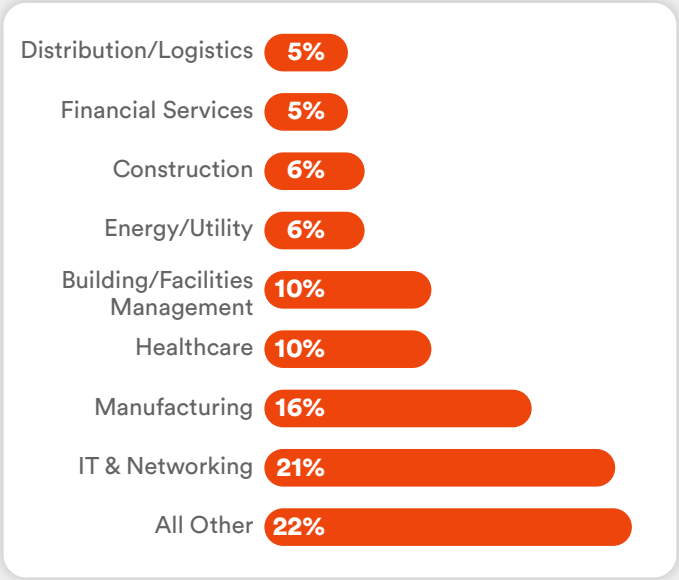


Figure 3.2 *What region is your business unit in?*

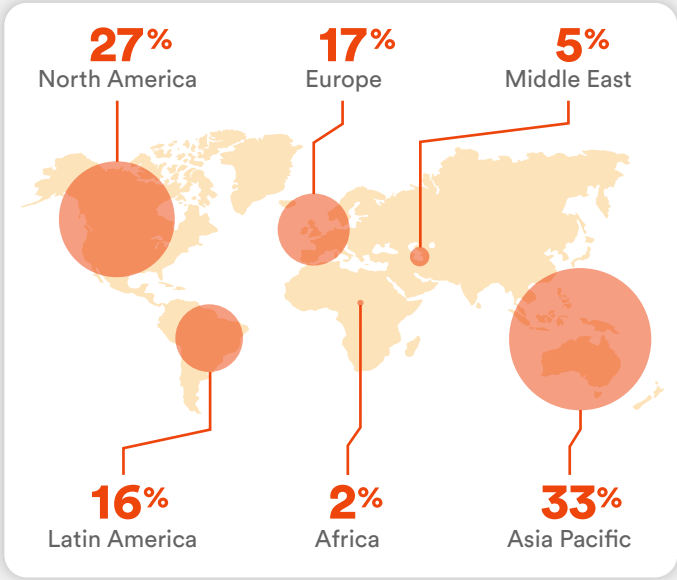
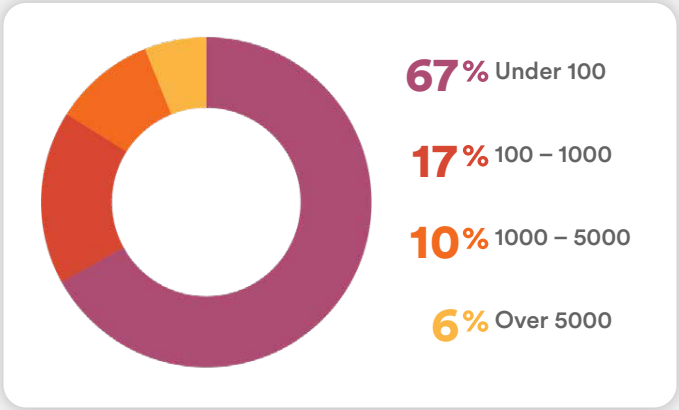


Figure 3.3 *How many staff are employed by your business unit?*



Applications and data usage

Respondents were asked about their use of IoT application types. Within that, as shown in **Figure 3.4**, the most popular application types reported by adopters were to do with monitoring at 40%. Tracking was then at 24%, closely followed by control at 23%. Of these, we would expect applications requiring control to be the most dependent on real time operation, followed by tracking and with monitoring less likely to require that.

Regarding the number of connected IoT devices deployed as shown in **Figure 3.5**, 78% of the respondents had deployments of under 100 devices, with 11% covering 100-500 devices and 10% with larger deployments of over 500 devices. This shows a wide variation in deployment numbers that varies partly by company size and partly by applications used.

Use of Wireless Connectivity

As shown in **Figure 3.6**, regarding wireless connectivity technologies used, 86% of respondents were using Wi-Fi followed by 48% using cellular. This shows that Wi-Fi clearly dominates – often due to low cost and controllability compared with current cellular. The reported high use of Bluetooth at 43% is specifically for short range connectivity and is likely to supplement Wi-Fi and cellular for local operational use, such as connecting bar scanners to hubs. The use of LoRa was also well-represented, emphasising the faster growth of low data rate applications. Sigfox use also featured. Both of these technologies offer wide area connectivity, so are more in competition with cellular than with Wi-Fi.

Figure 3.4 *What types of IoT applications are you currently using?*

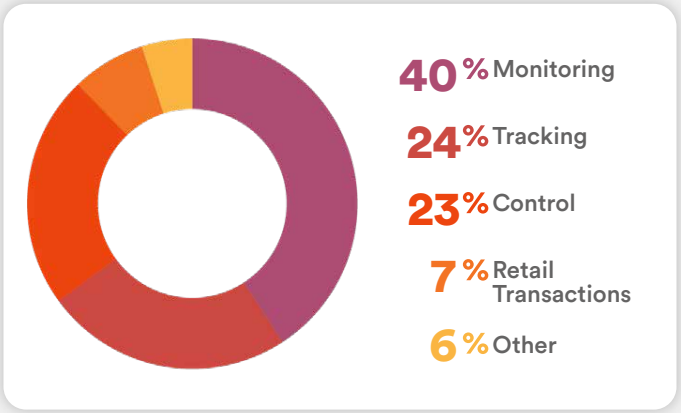


Figure 3.5 *Roughly how many IoT devices and/or terminals are connected to the wireless networks?*

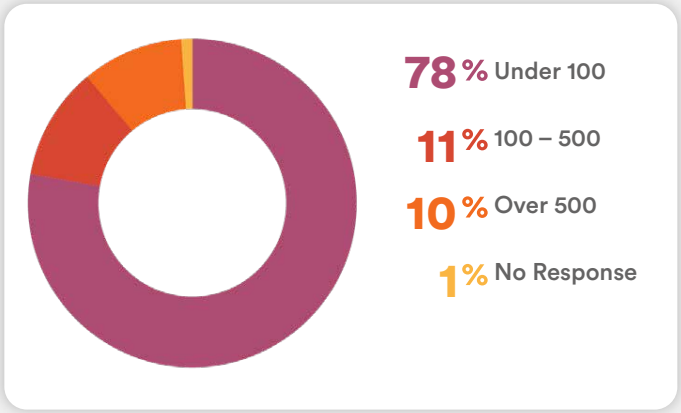
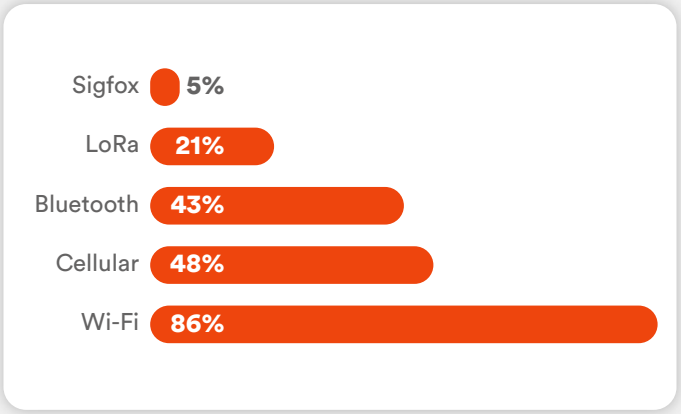


Figure 3.6 *Which connectivity technologies do you currently use for these?*



Wi-Fi network experiences and limitations

Use of Wi-Fi was investigated further, as shown by the series of responses in **Figure 3.7**. The purpose of these questions was to determine how successful use of Wi-Fi is in industrial environments. The findings of these follow-on questions were:

- 59% of respondents stated that their Wi-Fi network needed to operate outdoors, but onsite. Of these, some 56% believed that it had difficulties in achieving this.
- 63% of respondents stated that their Wi-Fi network needed to connect with moving vehicles, yet 94% of these indicated that sometimes as a result there was a loss of connection.
- 54% of respondents considered that there were blind spots on site with no Wi-Fi coverage
- 50% believed there were other interference problems with their use of Wi-Fi
- Meanwhile, 70% believed their Wi-Fi installation to be secure.

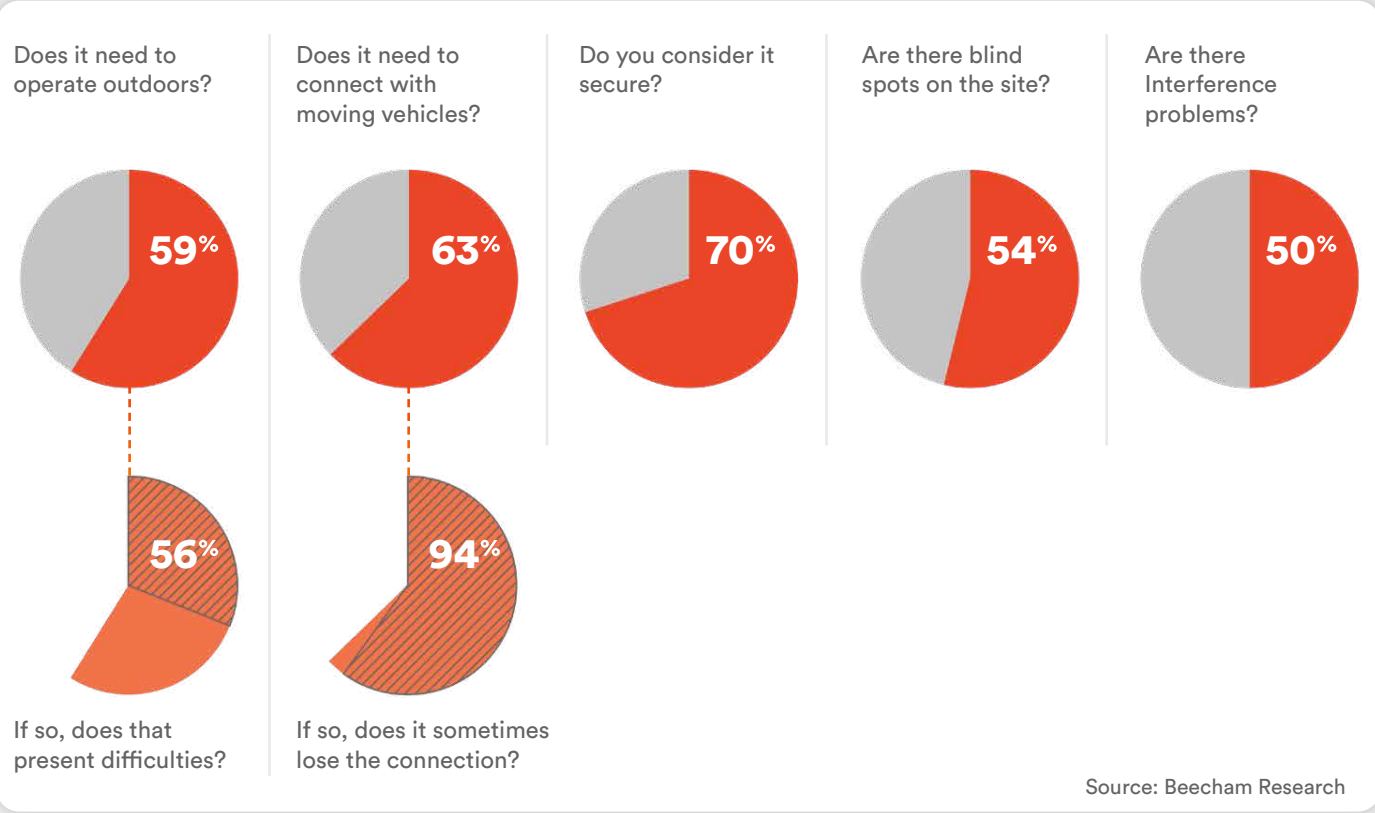
These findings indicate significant ongoing issues related to using Wi-Fi for connectivity of Industrial IoT applications. It should be noted that 70% believing their Wi-Fi installations to be secure was low. Expectations for cellular were higher than 99%.

From the one-on-one interviews, several companies indicated coverage problems in warehouses using Wi-Fi which could be overcome but enabling a seamless switch-over was difficult. Wi-Fi was the default technology for most devices at events, particularly outdoor events. Another interviewee indicated that in large sites it is more costly to install several Wi-Fi networks than a PCN and that clients appreciated the ease of installation compared to Wi-Fi. Also, Wi-Fi technology was not designed for mobility.

Another interviewee emphasised that Wi-Fi systems are not very stable and that there are compatibility challenges when operating with different service providers, for example loss of signal. Also that bandwidths are very unstable and maintenance costs are high.

These findings indicate that WiFi use for Industrial IoT applications is often seen as problematic.

Figure 3.7 *Regarding your Wi-Fi networking use:*



Source: Beecham Research

PCN expectations and challenges

As illustrated in **Figure 3.8**, 94% of respondents expected PCN to address Wi-Fi's limitations and 56% were considering using a PCN.

Regarding the main reasons for adopting a PCN, the main findings were as follows:

- 59% expected PCN to provide better on-site coverage.
- 63% expected better security
- 70% expected avoidance of network congestion or improved use of bandwidth
- 54% believed there was a benefit in owning and managing their own network, rather than relying on a third party such as a Mobile Operator
- 50% considered that owning their own network was more consistent for their longer term RoI

As shown in **Figure 3.9**, the survey showed that 52% of respondents saw technical resources as a substantial challenge, which was closely related to size of company. Those representing smaller companies were by far the major element. A slightly larger 59% saw capital expense as a major factor, while 70% considered operating cost to be the key challenge. Operating cost is likely to include the cost of own technical resources.

These findings indicate that, particularly among smaller companies, the desire to have complete control of their private network is not as great as their concern regarding technical resources and costs. It therefore appears possible that many would be attracted to a managed, private network facility where technical resources are provided by a service provider and costs can be controlled as part of a service offering.

***Figure 3.8** Private Cellular Networking*

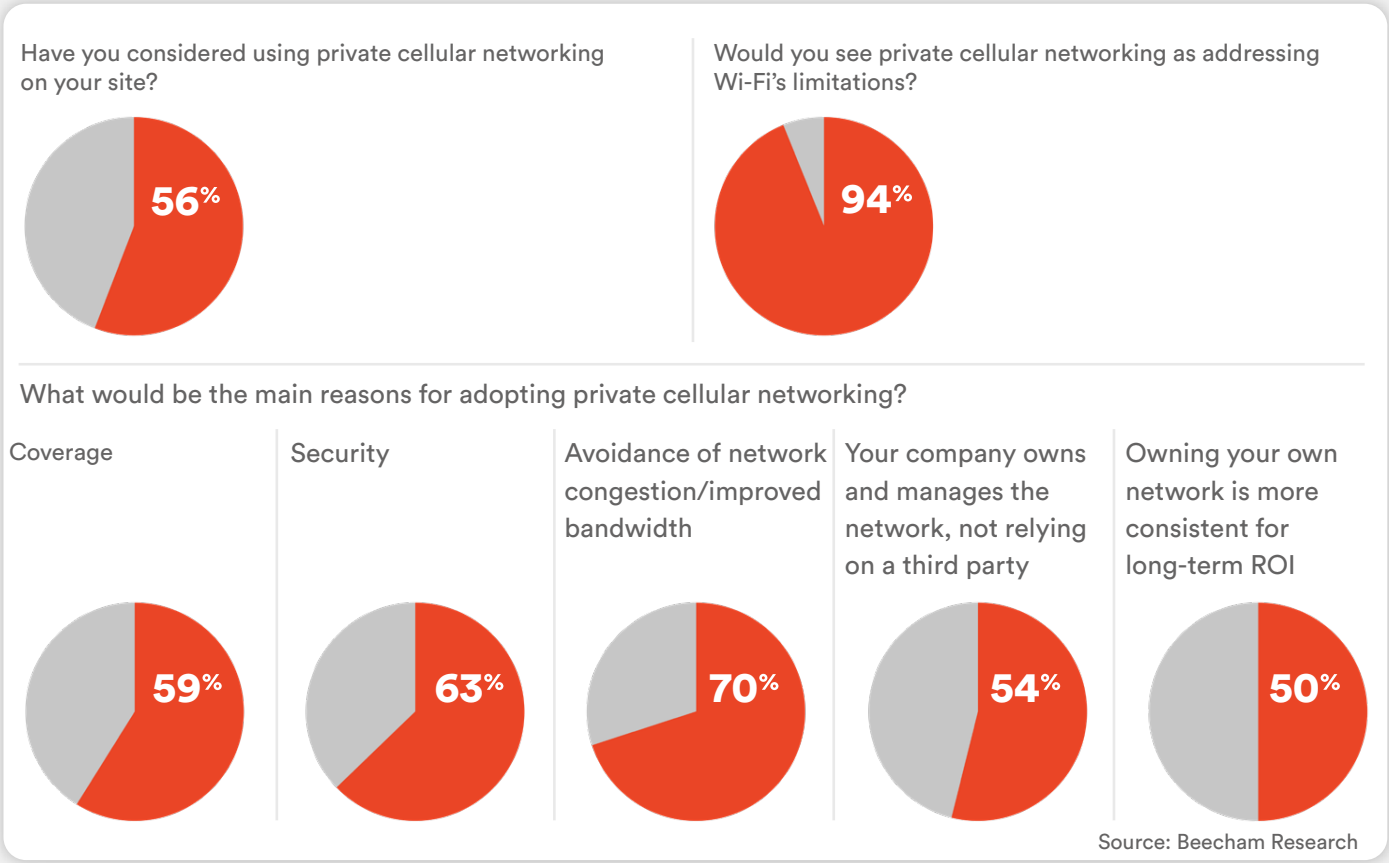
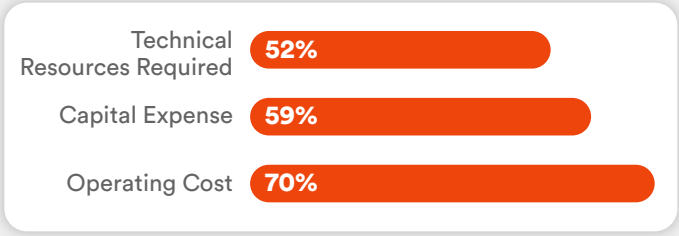


***Figure 3.9** What would you see as the main challenges in adopting private cellular networking?*



Cross-tabulation findings

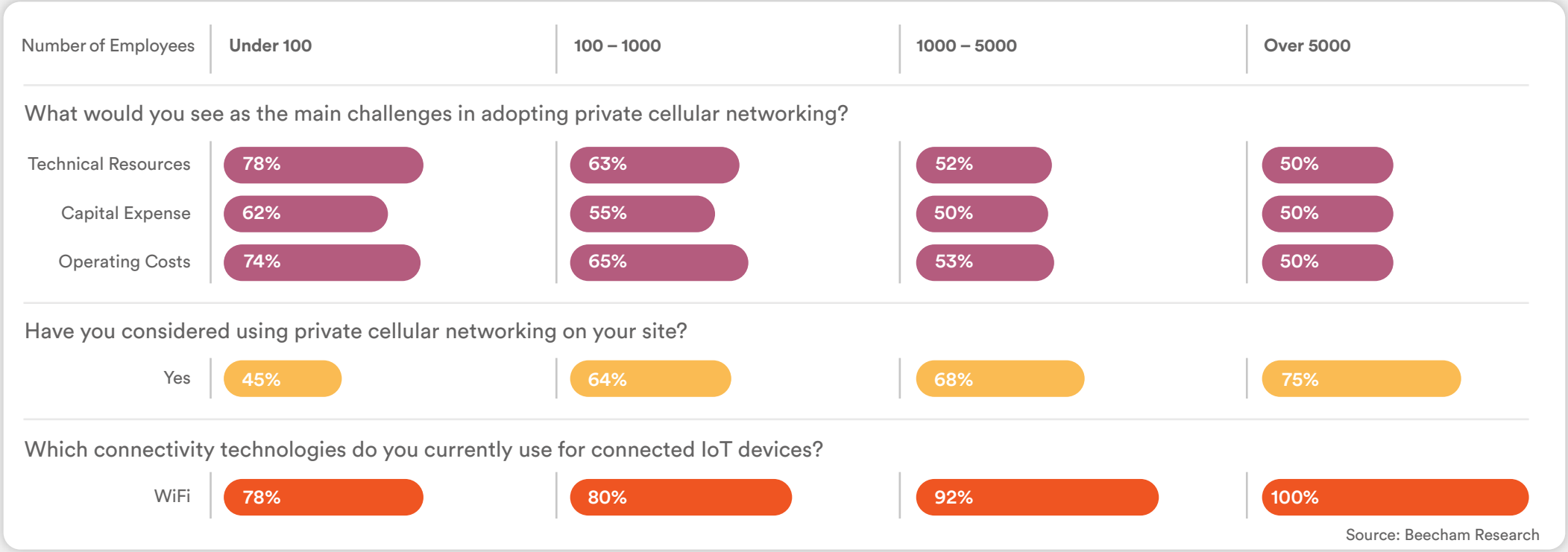
Figure 3.10 shows a cross-tabulation of business sectors vs use of WiFi connectivity. While WiFi use was generally high, it was noticeably lower in Construction and Healthcare and below average in Manufacturing. While not a strong finding, it was also clear that those not using Wi-Fi for Construction and Healthcare had all experienced issues in using Wi-Fi for either coverage or mobility reasons. In addition, Construction is primarily outdoor use and this is also a notable failure point for Wi-Fi. The lower score for Manufacturing was partly due to coverage and mobility issues, but also interference. These are indicators of the limitations of Wi-Fi for IoT and that these issues are not going to go away with Wi-Fi 6. It lends weight to the argument that the increasing availability of private 4G – and subsequently 5G – are likely to have a positive effect on development of the enterprise IoT market.

Further cross-tabulations against company size are shown in **Figure 3.11**. Regarding main challenges, this confirms the conclusion above that technical resource is seen as the main challenge for smaller companies.

Figure 3.10 *Business sector market share and their current use of WiFi connectivity.*

Further cross-tabulations against company size are shown in **Figure 3.11**. Regarding main challenges, this confirms the conclusion above that technical resource is seen as the main challenge for smaller companies.

Figure 3.11 *Business sector market share and their current use of WiFi connectivity.*



Source: Beecham Research

Use of Private Cellular Networking

Figure 3.12 indicates that, for those investigating use of PCN, 49% would expect to implement and manage that using in-house resource. 40% would use an external solution provider. It is not clear from the findings if there were sufficient technical resources in-house to achieve this result, but it seems likely to be questionable. There was clearly some reluctance to use external resources to assist.

Figure 3.13 assesses the use of PCN for voice as well as data, with 52% saying they would include voice. When examined further in **Figure 3.14**, 76% expected voice traffic to be less than 50% of network traffic, with 33% expecting it to be less than 20%.

Figure 3.15 then looked at the constituent elements of the data traffic, with 46% indicating this would include admin data and 51% indicating it would include Internet access for phones, tablets and laptops. A full 79% expected to including IoT traffic, including broadband use for such activities as CCTV surveillance.

Figure 3.12 *Who would you envisage designing/implementing/managing private cellular networking on your site?*

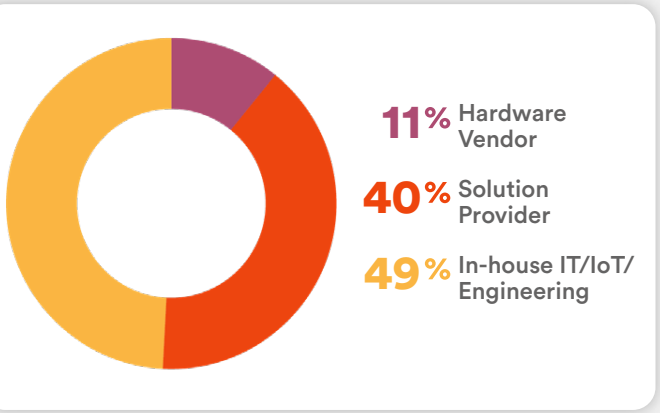


Figure 3.13 *Would you use private cellular networking for voice as well as data?*

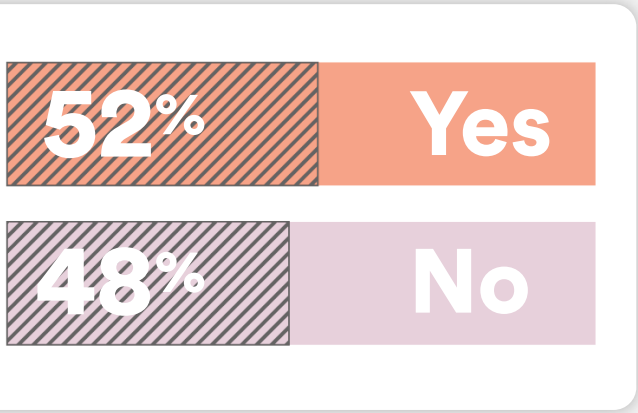


Figure 3.14 *What percent of network traffic would be used for voice?*

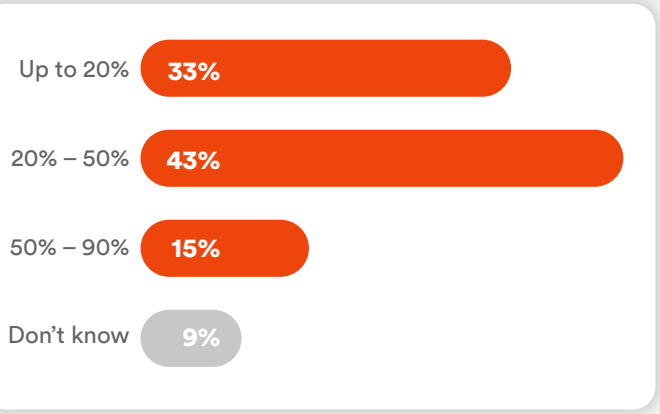
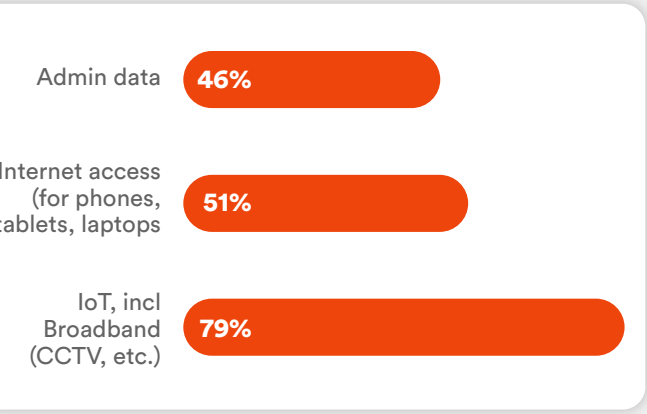


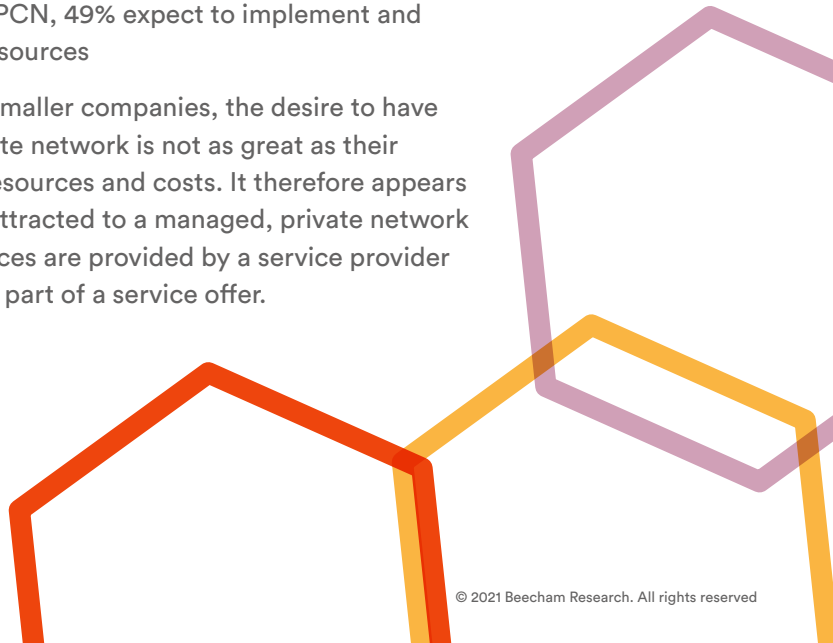
Figure 3.15 *What data would be included in your private network traffic?*



Conclusions

The main conclusions from the user surveys were as follows:

- There is increasing use of applications requiring real time operation, or low latency. This is consistent with a growing need for edge processing and this is a driver for PCN.
- The amount of data accumulated in operations is increasing. In addition, a major challenge is the speed of data processing required for this, which is also increasing. This also supports the growing need for edge processing
- Respondents agreed that data volumes will increase, but more importantly the volume of connected objects in a critical context is also expected to increase quickly
- It is considered that MNOs are not currently investing sufficiently in PCN technologies, although this is clearly beginning to change.
- Use of Wi-Fi for industrial operations is reaching a limit. Wi-Fi currently dominates at the local level but is prone to challenges when operating outdoors and when working with moving vehicles or objects. It is also difficult and costly to use across large sites.
- Companies view PCN as essentially complementary to Wi-Fi with both co-existing. PCN works well outdoors, is inherently designed to cater for moving objects and can easily and cost-effectively be used across large sites.
- This is particularly the case for large sites like airports, mining and shipping ports but also for use cases like hospitals where there is an increasing need for more more 'joined up' solutions across all activities on a site.
- In addition, PCN is seen as versatile – it can be used for different use cases on one site efficiently and effectively.
- As a result, a very high proportion of respondents (94% of those using Wi-Fi) expect PCN to address Wi-Fi's problems and 56% of respondents were considering using a PCN.
- Large percentages of respondents believed that PCN would improve coverage, improve security, avoid network congestion and improve use of bandwidth
- 54% believed there was a benefit in owning and managing their own network rather than relying on a third party such as a Mobile Operator and 50% considered that owning their own network was more consistent for their longer term RoI.
- For those investigating use of PCN, 49% expect to implement and manage that using in-house resources
- However, particularly among smaller companies, the desire to have complete control of their private network is not as great as their concern regarding technical resources and costs. It therefore appears possible that many would be attracted to a managed, private network facility where technical resources are provided by a service provider and costs can be controlled as part of a service offer.



Essential Elements of a PCN Solution

A private network solution focused on IoT applications has two main parts – the radio part that provides the connectivity infrastructure and the IoT part that handles the data. This section outlines key issues associated with both of these – starting with the radio part.

Overview

Private Cellular Networks (PCNs) can use licensed or unlicensed spectrum. PCNs may use local licensed spectrum in some locations (for example in Europe) with restrictions defined by regulators, while the same spectrum may include licensed and unlicensed use for both PCNs and public networks (See CBRS below).

There are two basic types of PCNs: Those similar to public networks covering large geographical areas complete with multiple cell towers, and much smaller PCNs covering limited areas – say an airport, a shipping port, or a manufacturing facility.

Large private networks, requiring major financial resources, are few in number. Southern Company, a gas and electric utility located in the southern U.S., built its own network to provide reliable, wide-area wireless communications for its operating companies in 1996, using Motorola's iDEN technology. The network covered approximately 127,000 square miles and was managed by Southern Linc, a subsidiary. With mission critical data growing, Southern Linc began replacing the narrow-band iDEN network with an LTE network, using its own licensed spectrum in the 850MHz band. The network began operating in 2016. Although built primarily to serve Southern Company's utilities, Southern Linc offers connectivity to other businesses, making it a regional carrier.

Rio Tinto, an Australian mining conglomerate, provides another example. It built a private LTE network for its 15 mines and railway and transportation facilities that went live in 2013, using 1800 MHz spectrum under a special arrangement with local regulators.

Figure 4.1 *15 Private Cellular Network application groups.*

These large private networks were built before a convergence of changes made smaller, much less costly PCNs practical. For clarity, we refer to first as Macro Cell PCNs, the second as Small Cell PCNs. An early example (2019) of a Small Cell PCN is the private LTE network deployed by the Port of Rotterdam using spectrum licensed by the Dutch regulator for local usage.

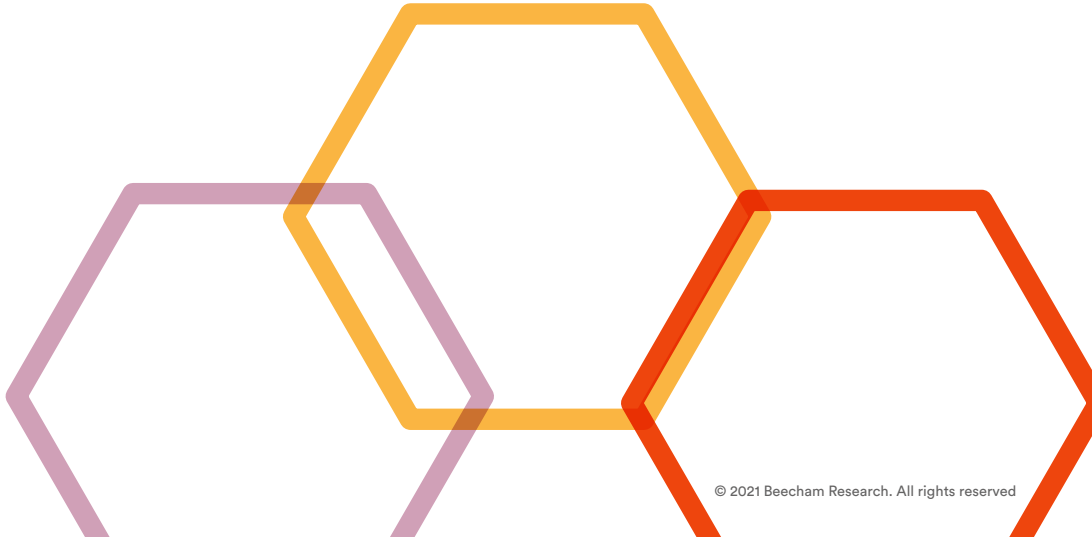
Changing software-based network technology changes also enable another emerging category, hybrid mobile networks that may combine different networks of various kinds – public, private, those using licensed or unlicensed spectrum, small and macro cell.

Ownership of a Small Cell PCN provides enterprises with greater control of their communications resource compared to using a Mobile Network Operation (MNO)'s network. The cost of a PCN can be amortized as a capital expenditure even as operating expenses are greatly reduced. A caveat: Deploying a PCN is not trivial, as it involves many issues and choices. One primary issue is whether an enterprise IT department includes any cellular networking expertise. If not, who will manage PCN infrastructure?

Although some PCNs provide mostly voice communication – especially when used as an alternative to a Distributed Antenna System (DAS) in a building – or broadband access, a use case that accelerated during the pandemic, they are also well suited for IoT applications, more so as 5G is rolled out.

Changes that have made Small Cell PCNs practical and relatively inexpensive include hardware and software developments arising from both the newer, all-IP core networking architecture that arose with LTE, and the continuing miniaturization of electronics, resulting in computer components that are smaller, more powerful, and use less energy than their predecessors. Large, expensive, purpose-built networking equipment made by specialized vendors is not required to support PCNs; small and fast off-the-shelf computers will do. Closely related: Software versions of the Evolved Packet Core (EPC) at the heart of modern cellular networks – Virtual Evolved Packet Core (vEPC).

These developments have arisen during the transition from LTE (4G) cellular to 5G and as spectrum is being reallocated all over the planet for both licensed and unlicensed cellular use and facilitate the growth of IoT, not just the growth of all web traffic or voice. PCN also offers a number of advantages for IoT applications compared with competing networking technologies.



Transition from Long Term Evolution (LTE or 4G) to 5G

Wireless cellular communication standards are developed by the 3rd Generation Partnership Project (3GPP), a consortium comprised of seven telecommunication standards organizations as primary members and a number of associated members. The "3G" is no accident; 3GPP was established in 1998 to develop specifications for a 3G mobile phone system based on the 2G GSM system, within the scope of the International Telecommunication Union's (ITU) IMT 2000 specifications. 3GPP's offices are located in the headquarters of the European Telecommunications Standards Institute (ETSI) in France. 3GPP's specifications are submitted to the International Telecommunication Union (ITU) for approval.

3GPP issues its specifications in releases. Long Term Evolution (LTE or 4G) was introduced in Release 8, "frozen" in December, 2008. Current 3GPP releases concern the 5th Generation (5G), in a world in which "IT" has become "ICT" as computing, the Internet, and mobile communications have merged, a world with billions of smart phone users.

5G is not just about smart phones; evolving specifications include details intended to enable and/or enhance IoT applications. 5G 3GPP specifications are currently at Release 16; parts of Releases 17, 18, and 19 are scheduled for this year, next year, and into 2023, somewhat delayed by the Pandemic.

Each release includes a number of new features and enhancements to previous features. Those interested in the details can find these on the 3GPP website at https://www.3gpp.org.

5G NR (New Radio) refers to the new radio access technology (RAT) developed by 3GPP for 5G, designed as the global standard for the air interface of 5G networks.

The first 5G NR specification became available by the end of 2017. With the 3GPP 5G standardization process in process, industry began efforts to implement infrastructure compliant with the draft standard.

5G NR uses two frequency ranges:
Frequency Range 1 (FR1): Includes sub-6 GHz frequency bands (some of which are includes bands used by previous standards) and extended to cover new spectrum offerings from 410 MHz to 7125 MHz.

Frequency Range 2 (FR2): Includes frequency bands from 24.25 GHz to 52.6 GHz.

Initial 5G NR launches use existing 4G LTE infrastructure in non-standalone (NSA) mode, with specifications delivered in 2017. 5G NR NSA uses the control plane of an existing 4G LTE network for control functions with 5G NR used exclusively on the user plane. Spectrum can be dynamically shared between 4G LTE and 5G NR in NSA.

The standalone (SA) mode of 5G NR applies to both signaling and information transfer and includes the new 5G Packet Core architecture instead of 4G Evolved Packet Core, to allow 5G deployment without an LTE network.

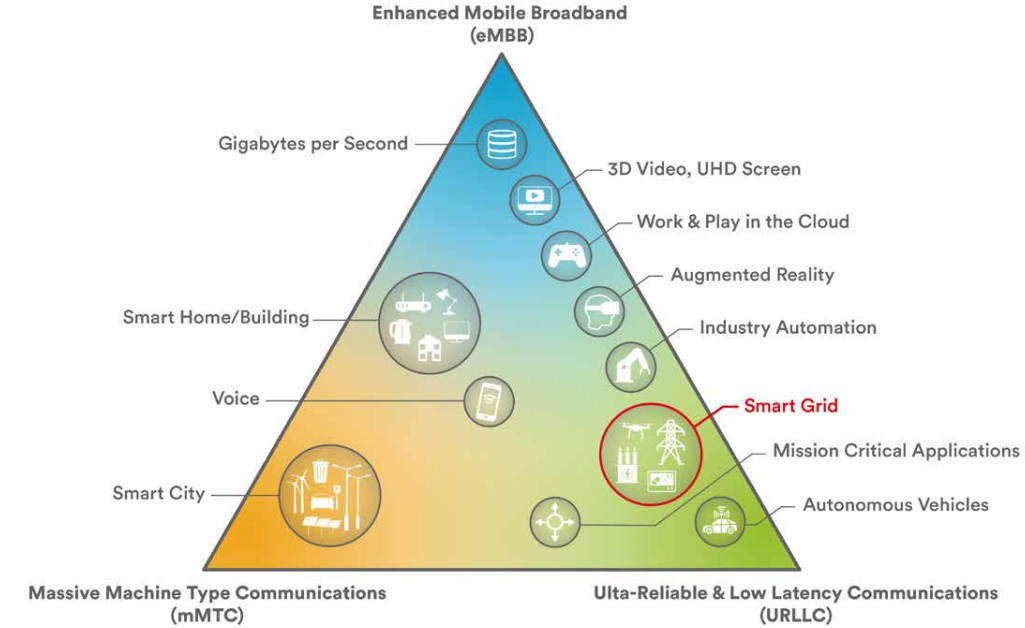
About 5G Generic Services

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 specifications, 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.

Release 16 also enabled 5G NR operation in unlicensed spectrum (5G NR-U), targeting the 5GHz and 6GHz mid-bands and 24+ GHz high-bands (mmWave) for unlicensed use. (Discussed below.)

Figure 4.2 *The three generic services of eMBB, uRLLC and mMTC services, together with typical IoT applications they enable.*



Spectrum Allocation and Reallocation

Radio spectrum is finite, first allocated by governments long ago in a pre-digital era. In the US, the Federal Communications Commission first allocated spectrum for celluar usage in 1982.

Different countries use different licensed frequency bands with associated bandwidths as well as combinations of bands. Each frequency band is allocated a number to aid identification and they are all licensed. Until recently, the industry prioritized about 40 bands. The continents and large countries employed two or three bands, the U.S. and Canada together employed four. Interoperability was (and is) realised by devices that recognise different bands, 28 in the case of iPhones.

Figure 4.3 *Global snapshot of allocated/targeted 5G Spectrum. Dec 2020 (Source: Qualcomm)*

	1GHz	2GHz	3GHz	4-7GHz	24-30GHz	37-50GHz	57-71GHz	>95GHz
	600MHz(2×35MHz) 900MHz(2×3MHz)	2.5/2.6GHz(B41/n41)	3.1-3.45/3.45-3.55GHz 3.55-3.7/3.7-3.98GHz	5.9-7.1GHz	24.25-24.45-25.25GHz 27.5-28.35GHz	37-37.6-40GHz 47.2-48.2GHz	57-64GHz 64-71GHz	>95GHz
	600MHz(2×35MHz)		3.475-3.65GHz 3.65-4.0GHz		26.5-27.5GHz 27.5-28.35GHz	37-37.6GHz 37.6-40GHz	57-64GHz 64-71GHz	
	700MHz(2×30MHz)		3.4-3.8GHz	5.9-6.4GHz	24.5-27.5GHz		57-66GHz	
	700MHz(2×30MHz)		3.4-3.8GHz		26GHz		57-66GHz	
	700MHz(2×30MHz)		3.4-3.8GHz		26GHz		57-66GHz	
	700MHz(2×30MHz)		3.46-3.8GHz		26GHz		57-66GHz	
	700MHz(2×30MHz)		3.6-3.8GHz		26.5-27.5GHz		57-66GHz	
	700MHz	2.5/2.6GHz(B41/n41)	3.3-3.6GHz	4.8-5.0GHz	24.75-27.5GHz	40.5-43.5GHz		
	700/800MHz	2.3-2.39GHz	3.42GHz 3.7GHz 4.0GHz	5.9-7.1GHz	25.7-26.5GHz 26.5/28.9/29.5GHz	37GHz	57-66GHz	
			3.6-4.1GHz	4.5-4.9GHz	26.6-27GHz 27-29GHz	39-43.5GHz	57-66GHz	
	700MHz		3.3-3.6GHz		24.25-27.5GHz 27.5-29.5GHz	37-43.5GHz		
			3.4-3.7GHz		3.4-3.7GHz	39GHz	57-66GHz	

● UNLICENCED/SHARED ● LICENCED ● EXISTING BAND

That picture is changing rapidly with new spectrum auctions and the opening up of unlicensed spectrum.

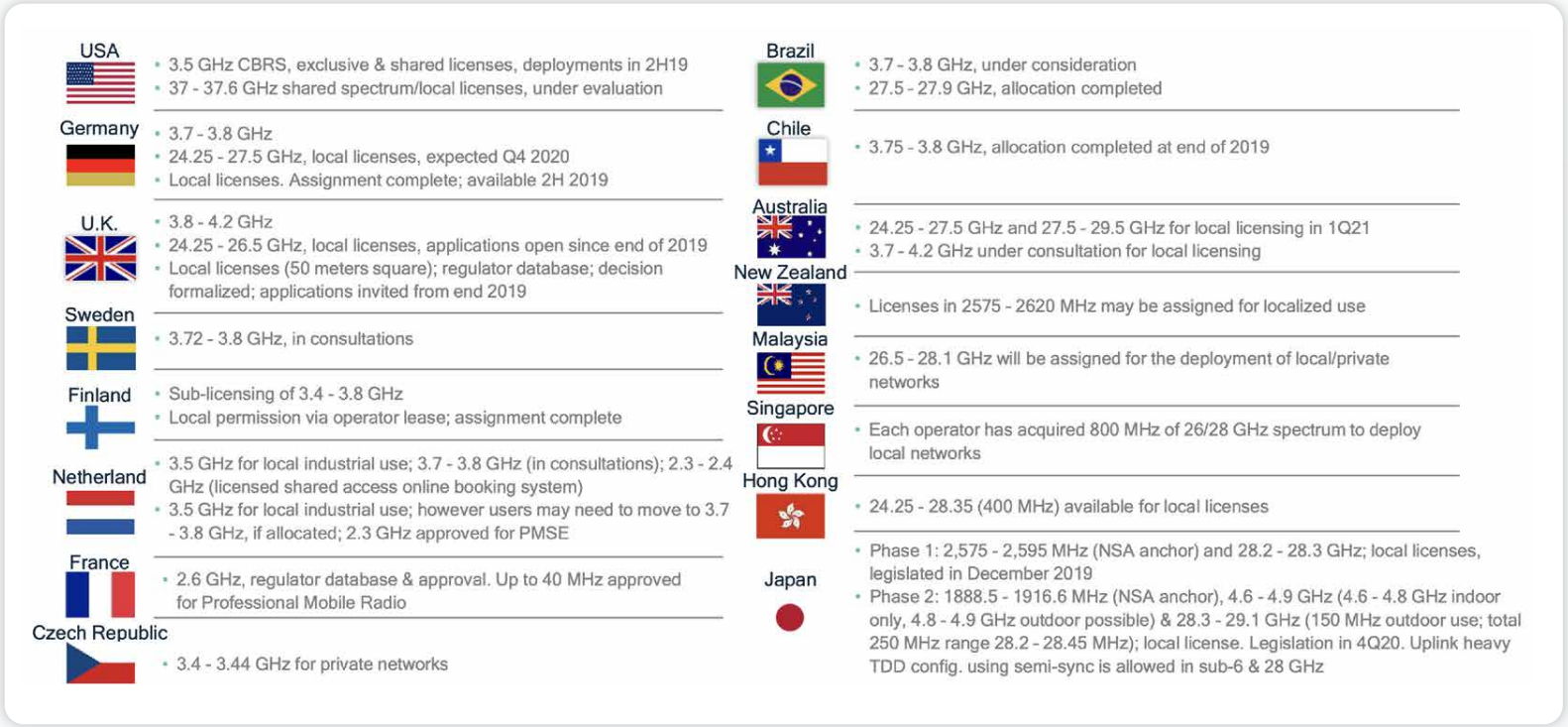
The reallocation of spectrum for both licensed and unlicensed use is an ongoing global process. As with the transition to 5G, it is driven by ever increasing data traffic volume and numbers of broadband mobile users, but the use of particular spectrum bands, particularly those in unlicensed spectrum, is not restricted to cellular devices or communication protocols.

In the U.S., spectrum reallocation began in 1996 to update rules created in 1934 and free up spectrum then used for analogue television broadcasting, an arduous process that wasn't completed until 2009.

Global spectrum reallocation is complex and unpredictable, with various competing parties including entire industries, incumbent users, consumers, and speculative entities, overseen by government agencies often headed by political appointees; no one can know in advance when particular spectrum might become available or what the results of spectrum auctions will be.

The spectrum picture for PCNs varies from country to country. Germany began offering corporate license fractions of 3.7-3.8GHz wireless spectrum for 5G services in November, 2019, as a spur to 5G PCN development.

Figure 4.4 *Global snapshot of spectrum optimized for industrial IoT/vertical/private network use – local licensing or sharing (Source: Qualcomm)*



These 'local' licenses are suitable for Small Cell PCNs in industrial settings. The UK's Ofcom's new licensing system, introduced in July, 2019, covers localized access to the 3.8-4.2GHz band and 1800MHz and 2300MHz shared spectrum. This spectrum is already licensed to mobile operators but is not being used or planned to be used in particular areas immediately. Working with Ericsson, Anterix will use its licensed 900 MHz spectrum to build PCNs for electric utilities in the U.S. (In the spring of 2020, the FCC made six megahertz of 900 MHz available for broadband, reserving four megahertz for two-way voice communications and similar narrowband applications that constitute the primary existing uses of the band.)

At the moment, reallocated unlicensed spectrum includes 1.9 GHz (sXGP) in Japan, 3.5 GHz in the U.S., and 5 and 6 GHz in various countries.

Interference and Shared Spectrum: Cellular and Wi-Fi

As spectrum is reallocated, new devices must share it with 'incumbent' devices already using bands within the spectrum. Examples include satellite ground stations, naval ship radar installations, microwave links, etc. In addition, wireless devices using different communication protocols may operate in the same existing or newly unlicensed spectrum, for example Wi-Fi and Cellular technologies operating in 5 or 6 GHz spectrum bands.

Without remedies, both situations would cause interference. Mechanisms for eliminating or minimizing interference with incumbents must be developed and approved by regulatory bodies prior to operation. (See the CBRS and MFA sections below.) In the example of Wi-Fi and Cellular technologies, standards organizations for the two technologies reached agreement on relevant specifications that can then be incorporated into chipsets.

Comparisons between Wi-Fi and PCN are inevitable. The first Wi-Fi specifications were issued in 1997, the most recent, Wi-Fi 6, approved this year. Wi-Fi is ubiquitous with over 3 billion Wi-Fi equipped devices shipped globally every year and vast numbers of 'hotspots.'

Using chips manufactured in such large volumes, the initial cost of Wi-Fi networking is low, but any total cost of ownership comparison must examine Wi-Fi's limitations.

Unlike cellular, Wi-Fi was not designed for mobile assets. Coverage is more limited than cellular, a concern for large site deployments. Interference, particularly in outdoor applications, is another concern, while network congestion may result when many Wi-Fi devices attempt to communicate simultaneously, increasing latency. Although Wi-Fi 6 offers improvements over earlier versions, Wi-Fi does not match the performance of cellular technology in terms of security and network reliability.

Both Wi-Fi and PCN will be used for IoT deployments into the foreseeable future, including solutions using both protocols. This can be seen as coexistence – a complementary rather than competing situation. However, it is expected that PCN will predominate over the longer term, as IoT applications become increasingly central to business operations.

CBRS

The Citizens Band Radio Service (CBRS) is a 150 MHz wide band with 7 licensed and 8 unlicensed channels between 3550 and 3700 MHz (usually referred to as the 3.5 GHz band) approved for use in the U.S. in early 2020. An additional 500 Mhz may become available in the 3.7 to 4.2 GHz band. Shortly afterwards, the OnGo Alliance (formerly the CBRS Alliance) announced completion of specifications that support specific OnGo configurations for 5G New Radio (5G NR).

As an experiment in using shared spectrum suitable for PCN, CBRS is a success, with growing deployments, well-developed distribution channels, and a growing list of certified devices (see for example https://docs.celona.io/en/articles/3484781-cbrs-capable-devices-in-the-market) that include not just tablets, laptops, and smartphones, but also gateways and routers suitable for IoT applications.

Work on specifications and the certification process began at the Wireless Innovation Forum (WInnForum) in 2015 (the CBRS Alliance, focused on commercialization, was organized in 2016) – CBRS didn't spring up instantly.

The Federal Communications Commission established a three-tiered, spectrum-sharing framework for the CBRS band to enable shared spectrum use with incumbents that include naval radar systems – coastal or offshore; the U.S. Navy uses only about 1% of available spectrum in the 3.5 GHz band at any given time -- and fixed satellite service users.

The first tier is the cloud-based Spectrum Access System (SAS). Five SAS administrators (Amdocs, CommScope, Federated Wireless, Google, and Sony) maintain databases of all OnGo base stations, including their tier status, geographical location, and other pertinent information to coordinate channel assignments and manage potential interferences.

The other two tiers are an unlicensed portion of the band, General Authorized Access, and Priority Access Licenses (PAL), which entitle holders to prioritized access over unlicensed users within their geographic license area. Note that Verizon recently purchased a large number of PAL licenses to augment its existing public network.

Commercial deployments are validating the concept of spectrum sharing as a model that can be used in other countries using different frequencies, licensed or unlicensed. One indication of the market traction CBRS is gaining is a recent announcement by Federated Wireless and the Learning Alliance saying they will work together to issue over 2,000 Certified Professional Installer (CPI) certificates for CBRS over the next two years, greatly expanding the number of available technicians.

MFA: MulteFire and Uni5G

The MFA (MulteFire Alliance) is an international organization that is championing the global industry use of private cellular networks in unlicensed spectrum – combining the performance benefits of LTE and 5G with the simplicity of Wi-Fi type deployments – using MFA-defined MulteFire specifications for LTE and Uni5G technology blueprints for 5G.

The purpose of this is to ensure that, with Uni5G or MulteFire, enterprises can efficiently deploy their own optimized, reliable and secure private network in unlicensed spectrum or complement their existing private network deployments in locally licensed or shared spectrum.

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

Uni5G is a technology blueprint that leverages 3GPP 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. Uni5G leverages 3GPP 5G NR standards, particularly those for IoT use cases. 3GPP's 5G NR-U standalone variation, relying solely on unlicensed spectrum (for control and user plane traffic) was standardized by 3GPP with significant inputs from MFA members.

The success of CBRS PCNs, with a new experimental mechanism for minimizing interference with incumbents but only in the 3.5 GHz band and in one country, bodes well for MFA's more ambitious global, multiple spectrum efforts.

Although MFA's LTE MulteFire technology has been successfully commercialized in Japan, using the 1.9 GHz band and referred to as sXGP, its 5 GHz version has been slow to take off but is now starting to gain traction as certified devices become available. Unlike 3.5 GHz, billions of Wi-Fi devices (including the new Wi-Fi 6) operate in 5 GHz spectrum. A solution to potential interference had to be worked out between two different technologies and the standards organizations behind them (IEEE and 3GPP). The solution was to incorporate new listen-before-talk (LBT) procedures into specifications.

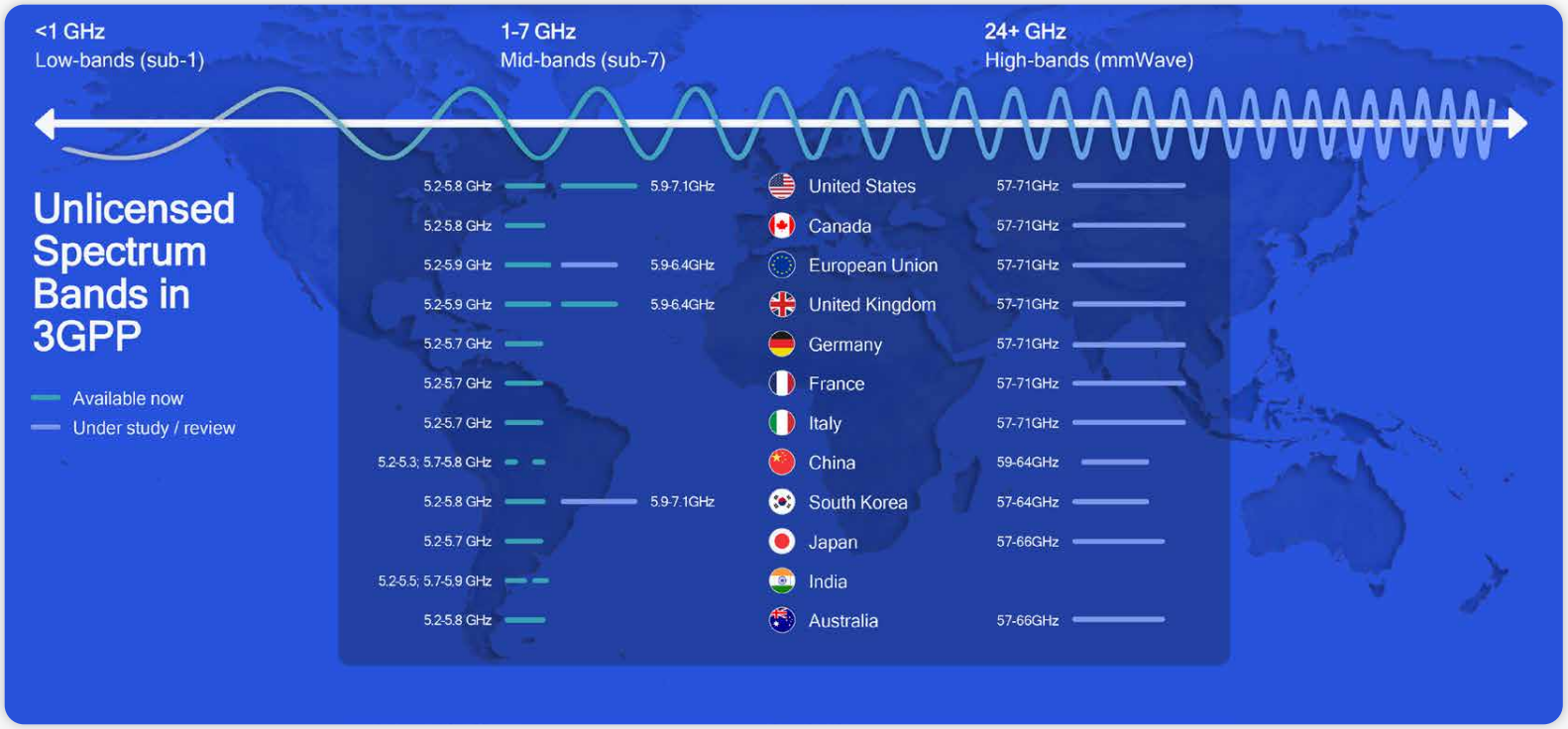
Resolving this was important for MFA's technology, especially now that 6 GHz unlicensed spectrum, with lots of bandwidth, is becoming available. MFA's solution is well suited for 6 GHz but cellular technology will encounter Wi-Fi technology here, too, with Wi-Fi's 6E version.

5G NR-U

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 Quality of Service 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 many private network sites where there is a controlled network environment. The authority controlling the network 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.

Figure 4.5 *5G NR-U standardized in 5G NR Release 16. The first global cellular standard with both license-assisted and standalone use of unlicensed spectrum (Source: Qualcomm)*



6 GHz Regulatory Frameworks

Unlicensed 6 GHz spectrum has its own incumbents – fixed satellite service earth-to-space links and point-to-point fixed service links. Regulatory frameworks that will limit signal energy near incumbent receivers haven't been finalized everywhere but regulators have created three relevant classifications for 6 GHz RLAN devices:

TAOGLAS

The 6 GHz Opportunity for 5G Private Networks

One fundamental difference between 5G and its predecessors is spectrum. 5G is designed for use in far more bands than 4G, 3G and 2G, including ones at higher frequencies than cellular has ever used. This difference creates a host of new opportunities and considerations for private network operators.

For example, the higher the frequency, the higher the data rate it can support. That's why many public 5G networks are using millimeter wave (mmWave) spectrum. The downside is that signals don't travel as far at high frequencies, so the operator — public or private — will need a much higher density of base stations to cover a given area, such as a city or a manufacturing facility. High frequencies such as mmWave also struggle to penetrate physical obstructions such as walls. Lower spectrum, such as traditional cellular bands at 850 MHz and 1900 MHz, requires fewer base stations and provides better in-building penetration, with the tradeoff of lower data rates.

These factors are why many private operators are choosing the 6 GHz middle ground. (The band starts at 5.9 GHz and runs to 6.4 GHz or 7.1 GHz, depending on the country.) It's high enough to support bandwidth-intensive Internet of Things (IoT) applications such as video surveillance, but without the capex and opex of a high-density network.

For private operators, another key benefit is the amount of spectrum available at 6 GHz. In the U.S., for example, 1200 MHz is available for 5G use — and without a license. Private operators also benefit from public 6 GHz deployments because their mass-market scale increases the selection of devices and infrastructure while driving down costs.

"The 2023 World Radiocommunication Conference (WRC-23) will play a decisive role in determining future access to the upper 6 GHz range (6425-7125 MHz)," the GSMA says. "It provides the opportunity to harmonize the band across large parts of the planet and help continue development of the 6 GHz ecosystem. Balanced decisions on the use of this range can allow license-exempt technologies, when needed, to make use of the lower part of the band where required while reserving the upper portion at 6425-7125 MHz for licensed 5G."

There's already a growing selection of modules and antennas for 5G at 6 GHz, enabling private operators to take advantage of the spectrum immediately. One example is the Taoglas MA9917 Guardian X, which combines 17 antenna elements into a single, low-profile, heavy-duty, IP67-rated enclosure. It supports 5G MIMO at 6 GHz and a wide variety of additional bands, as well as Wi-Fi 6 MIMO at 6 GHz.

The MA9917 also highlights the role of MIMO in 6 GHz 5G. Bandwidth-intensive applications such as HD video require fast uplinks, downlinks and sometimes both. High-efficiency and high-gain MIMO antennas are critical for achieving both the signal-to-noise ratio and throughput required to support these demanding applications. Another key consideration is high isolation between the MIMO antennas to prevent self-interference, which undermines performance.

Low-loss cables also are important to optimize efficiency over long spans. Smaller MIMO antennas with low-quality, thin cables have reduced efficiency and isolation, all of which significantly undermines system throughput while increasing dropped signals — when they might make a connection at all. All of these considerations highlight how MIMO directly affects the ability of 6 GHz 5G networks and devices to support mission-critical and other demanding applications.

Expanding 5G Coverage in Dense Urban Areas

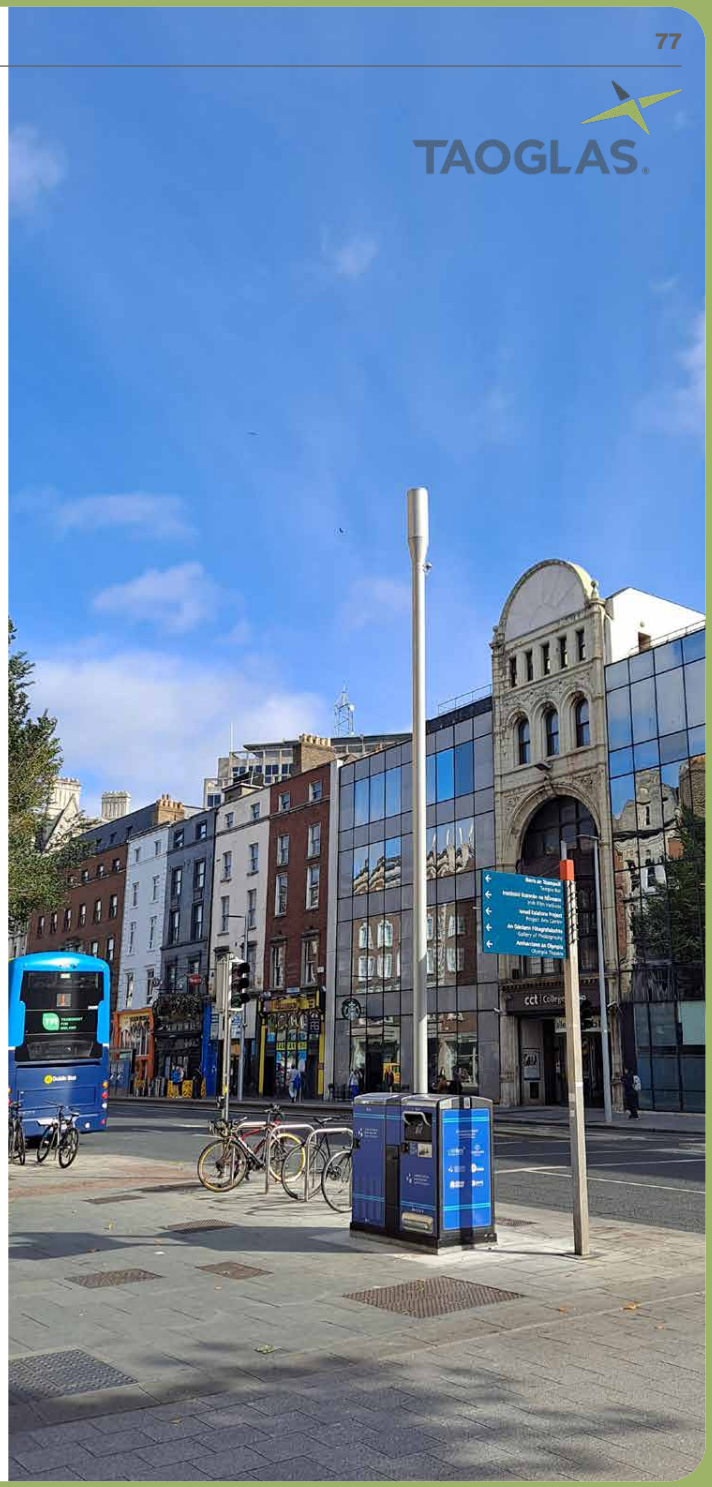
Taoglas has recently added a new “Connected Smart Services” business unit to its global organization after aquiring Smartsensor Technologies. This business unit provides end-to-end IoT solutions -- including managed services and analytics -- to municipalities and enterprises. Part of its proven offering includes smart waste services in collaboration with Bigbelly and new initiatives to roll out their Telebelly offering with 5G infrastructure as an integrated option is gaining market adoption.

Bigbelly is the world leader of smart waste and recycling solutions for public spaces. Communities, campuses, and enterprises deploy smart, sensor-equipped waste and recycling stations that communicate their real-time status to streamline waste management operation and improve overall public space aesthetics.

Communities and broadband providers around the world share the challenge of how and where to deploy information and communication technology (ICT) infrastructure, including 4G and 5G small cells, in public spaces without adding additional clutter or negative aesthetic impact. Public spaces benefit from wireless applications that improve quality of life, public safety, and economic development while keeping streets, sidewalks, and beaches clean and delivering robust connectivity to the residents, businesses, and visitors.

The Bigbelly Telebelly is a fully customizable multi-purpose platform for enabling ICT applications in publics spaces. In addition to modernizing a core city service, its ubiquitous form factor is optimal for hosting additional ICT equipment. It is easy to access and can “hide ICT technology in plain sight.”

Telebelly stations are located where the people are, which is exactly where cell coverage, or improved wireless broadband, is needed. Small Cells are hidden from public view inside the Telebelly platform. This avoids the need to erect single purpose poles and visible electronics or adding more to existing poles that are already cluttered with attachments and reaching capacity.



Elements of a PCN IoT Solution

As part of an IoT solution, PCN infrastructure, beyond choice of spectrum and mechanisms for minimizing interference with incumbent users in unlicensed spectrum, includes:

- **Radio Access Network** (RAN)
- **Evolved Packet Core** (EPC)
- **Routers, Modems, and Gateways**
- **Cellular Modules and SIMs/eSIMs**
- **Antennas**
- **Backhaul**

The IoT solutions supported by the PCN infrastructure are usually provided through an IoT platform. End-to-end security is also required.

Radio Access Network (RAN)

A RAN in a public network, for example, is the final link between the network and a phone (user equipment, or UE). It includes base stations and a series of antennas which then connect the phone to other parts of the network. The base station connects to the core network, typically through fiberoptic "backhaul." An IoT PCN RAN is similar but connects to a local core network. PCN base stations are typically smaller and less powerful transceivers than those in public network cell towers.

Open RANs have come about to reduce dependence on proprietary functionality of a few network vendors. In an Open RAN environment, the RAN is disaggregated into three main building blocks – the Radio Unit (RU), the Distributed Unit (DU), and the Centralized Unit (CU).

Radio frequency signals are transmitted, received, amplified and digitized in the RU, located near or integrated into the antenna. Computation in a base station is done in the DU and CU, prior to sending the digitalized radio signal to the core network. The DU is physically located at or close to the RU while the CU can exist closer to the core network. By "opening" the various protocols and interfaces between these RAN components, different vendors can offer interoperable parts of the RAN, a change from having a single vendor offering all components.

Evolved or Enhanced Packet Core (EPC)

EPC is key to the core network architecture of 4G LTE. It was standardized in 3GPP Release 8 as a framework for combining voice and data using Internet Protocol (IP) service architecture, an evolution of the 3G system beyond traditional circuit-switched core technology and the packet-switched architecture used in General Packet Radio Service (GPRS) and the Universal Mobile Telecommunication System (UMTS).

Combined with Software Defined Networking (SDN) and Network Functions Virtualization (NFV), virtualized EPCs (vEPC) running on general purpose computing hardware/platforms now exist, a situation comparable to the "opening" of RAN in that multiple vendors – not just the preeminent telecommunications network equipment providers – can offer EPC.

This can benefit Mobile Network Operators (MNOs) but is also favorable for PCN adoption, where the network core is typically local – close to the RAN – and limited in various ways compared to MNO core network functionality; vEPCs can reduce the costs of PCNs and are key to PCNs using unlicensed spectrum such as CBRS.

Routers, Modems, Switches, and Gateways.

Traditional networking equipment has become "smarter" as CPUs and memory units have become smaller with greater speeds and capacities and reduced power requirements. This applies to all networks, not just PCNs, and cellular networking equipment. IoT applications, whether mission critical or business critical, may rely on this equipment for a range of functions, from aggregation of device data to connecting local or small vehicular mobile networks or Wi-Fi (or other protocol networks) to the PCN network.

Cellular Modules and SIMs/eSIMs

Sensors and devices must connect to a PCN. This is enabled by a cellular module and a Subscriber Identification Module (SIM) that identifies and authenticates a device. Form factors have evolved since the first SIM cards, including small form factor versions soldered onto IC boards, and can now be remotely provisioned Over the Air (Embedded SIM or eSIM). This is a more suitable solution for many IoT applications and essential for a large IoT deployment. A recent development, iSIM, enables hardware OEMs and processor design companies to design system-on-a-chip (SOC) architectures with integrated embedded SIM functionality.

Antennas

Antennas are an essential component of devices and base stations. Antenna design has becoming increasingly complex as UE must often communicate over multiple spectrum bands, especially on the consumer side, where antennas compete with other components for space in smart phones and be compatible with newer cellular standards as 4G/LTE transitions to 5G, where Multiple Input, Multiple Output (MIMO) antennas may be required. An IoT PCN may not operate over multiple spectrum bands but antennas are part of the challenges of siting devices and base stations in a PCN environment. Devices may have to operate inside, outside, or both; a PCN inside a hospital will impose different antenna design constraints than a PCN used for agricultural applications in open fields.

Backhaul

Connection to the core network and Internet -- backhaul -- from a cell tower that is part of a macrocellular network will typically rely on fiberoptic cable. Backhaul in a PCN will be of a different nature – a local EPC running on a server can be connected to the equivalent of tower base stations ("access points" in DAS or Wi-Fi) with Ethernet cabling. In most situations, the PCN will still have to be connected to the Internet and, possibly, a public network – many IoT deployments require access to the cloud for processing data. Depending on the location, this can be accomplished in a number of ways, including satellite for remote locations lacking any other means of connection.

Roaming between public and private networks is an important consideration, especially for activities like mining and ports where there is substantial traffic moving on and off site.

A partnership agreement with Expeto allows Pod Group to market an innovative solution that provides seamless roaming between private and public networks. Cellular networks employ an Evolved Packet Core (EPC), a key component that can be implemented in software and which enables the advanced functionality of public networks. Expeto has expanded and extended the functionality of its EPC and enabled it to be deployed in a PaaS (Platform as a Service) model. Enabling EPC as a service allows the network's home subscriber server to operate in different locations.

Pod Group's cellular communications infrastructure is a software replication of a regular MNO network. The partnership with Expeto allows the company to deploy a purpose-built, containerized EPC software solution that can be installed as a small footprint behind the firewall and be managed by the enterprise from the cloud, the edge of the IoT network or on site. This functions across private enterprise networks as well as public networks following agreements with MNOs. The result is the single, secure unified private domain in which the entire IoT network operates like the corporate LAN. Policies, network configurations, QoS and native security policies can be managed across all networks and devices.

In addition this solution retains secure communications when roaming between the private network and public networks. This is by providing seamless access to the IPX (IP eXchange) backbone network, which is a managed network environment. It is used by carriers and service providers and is traffic-engineered to support specific IP services at specific quality levels. Data runs at Gigabit rates on the IPX and it does not touch the public Internet, so is totally secure.

The network is accessed through four points of presence (PoPs), two in the USA and two in Europe. When enterprises work with an ENO such as Pod Group they connect their network to the nearest PoP and can then use IPX services to route traffic using private, dedicated connections between private data centers and public cloud platform providers like AWS and Microsoft.

Various service providers use the IPX backbone network. Pod Group customers can pick one and use their service to change bandwidth and duration on the fly, for example, boost capacity when it is needed, maybe just for a matter of minutes.

IoT Platforms

An IoT Platform is required for any IoT solution involving IoT devices connected through a PCN to an IP (Internet Protocol) network. Three key elements that must be managed:

1. The connected IoT device itself, which may be one sensor measuring temperature, location or some other parameter or an asset such as a vehicle that has many sensors each measuring something different. Device management aspects may include device identity in the IP network, provisioning for use of the network and secure over-the-air update of device firmware. These and other related areas are part of Device Management.

2. The connection, from the IoT device to a server to which the data is transmitted for processing. That may be a short-range or long-range connection, wired or wireless, or a combination thereof. The server may be at the network edge, in the cloud, or in both for different needs. Some of the areas that need managing are connectivity options, coverage, network protocol support and billing/usage. These and other related areas are part of Connectivity Management.

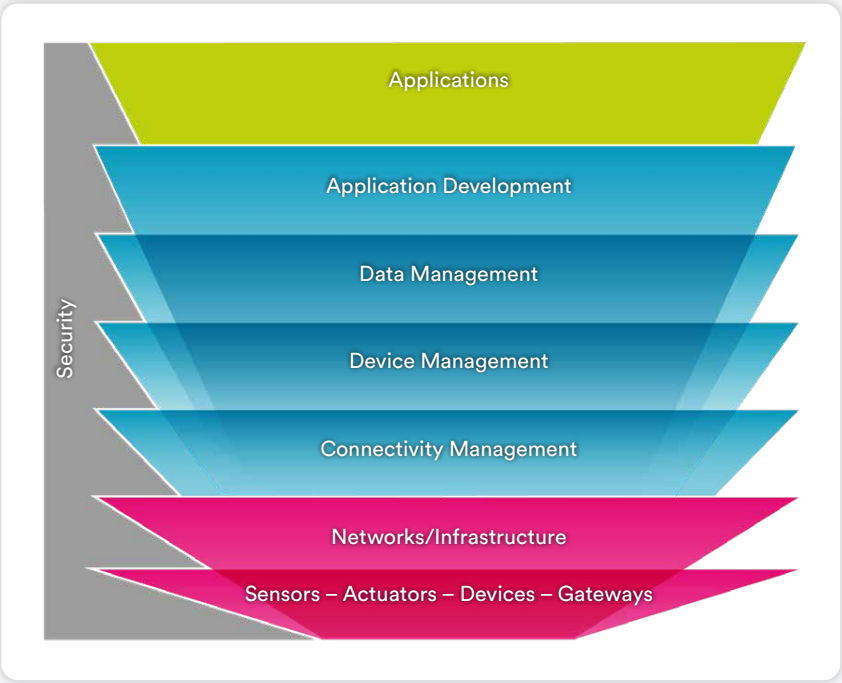
3. The data generated needs to be stored, processed – sometimes in real time – either on its own or in combination with other data, to create the required results. Additional areas that need managing are: workflow handling, visualisation, orchestration and data analytics. These and other related areas are part of Data Management.

In addition to these, an application usually needs to be developed or provided to make specific use of the data created. All of this must be carried out securely so that the device itself and anything that is using the data, such as a controller, is not compromised. Security needs to bind together all the other elements so that potential attack surfaces are minimized.

These elements can be illustrated as in **Figure 4.7**, where they form a stack that sits above the sensors and network infrastructure. Since Device Management requires the connectivity to be in place before it can function for remote devices, it sits above Connectivity Management.

These are then also the main elements of an IoT platform, which is essentially a software middleware suite that facilitates secure monitoring, control and analysis of device and sensor behaviour in the field. In essence, it provides an enabling layer between these connected devices/sensors and user applications.

Figure 4.7 *Architecture of an IoT platform*



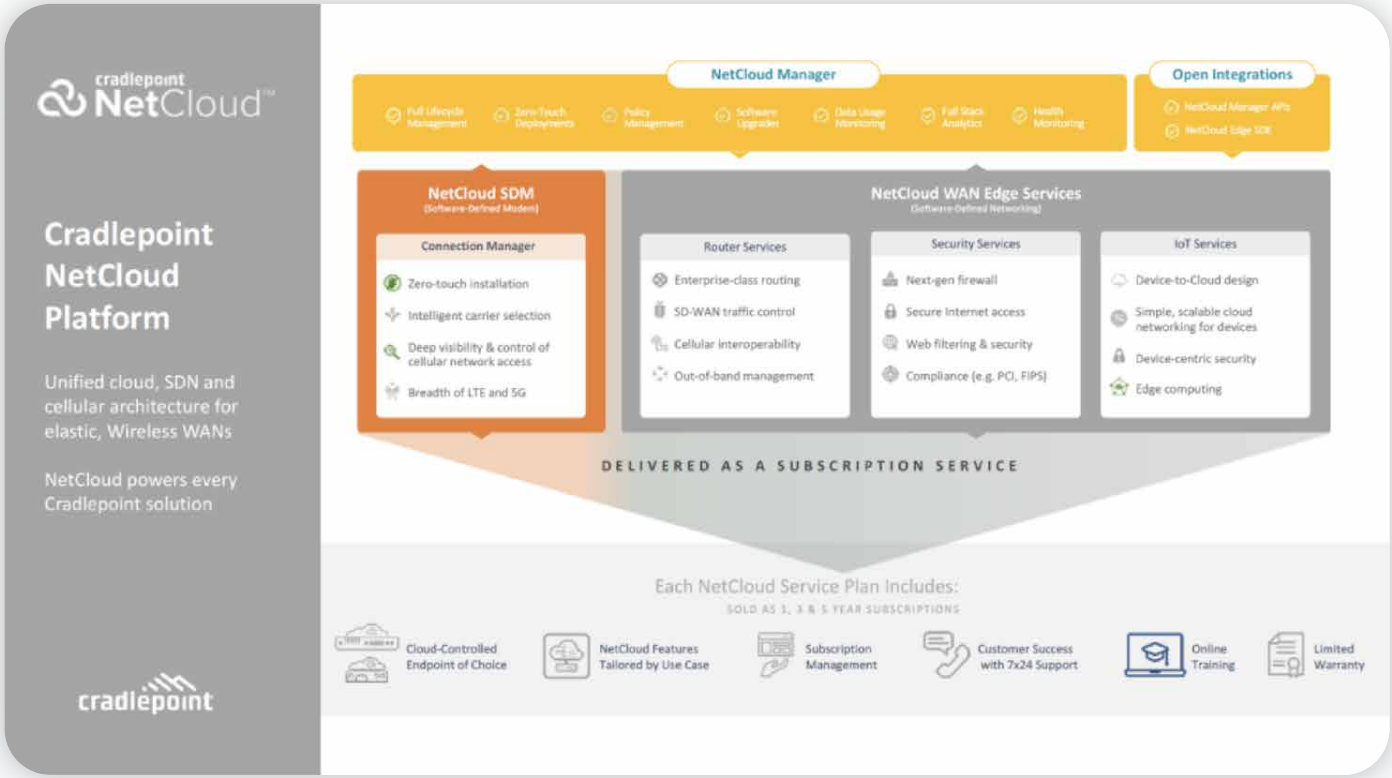
NetCloud platform covering several layers of the platform stack is Cradlepoint's NetCloud, working in close harmony with Cradlepoint's own on-site edge routers.

NetCloud Manager (NCM) is a cloud-based service designed to ensure success of small and large networks alike. NCM combines centralized management, intelligent and reliable multi-carrier connectivity, and extensibility for mission critical mobile and operational applications. This enables organizations to do more with fewer resources, by utilizing a single cloud platform to configure, deploy, and manage all wireless edge gateways from anywhere – across multiple sites.

Through NCM, administrators can utilize Out-of-Band-Management (OOBM) over cellular for troubleshooting and remote access of third-party devices. NetCloud management connectivity includes the ability to determine the status of any network component, independent of the status of other in-band network components. Out-of-Band Management allows the network operator to establish a trusted and secure boundary in accessing the management function to apply it to network resources.

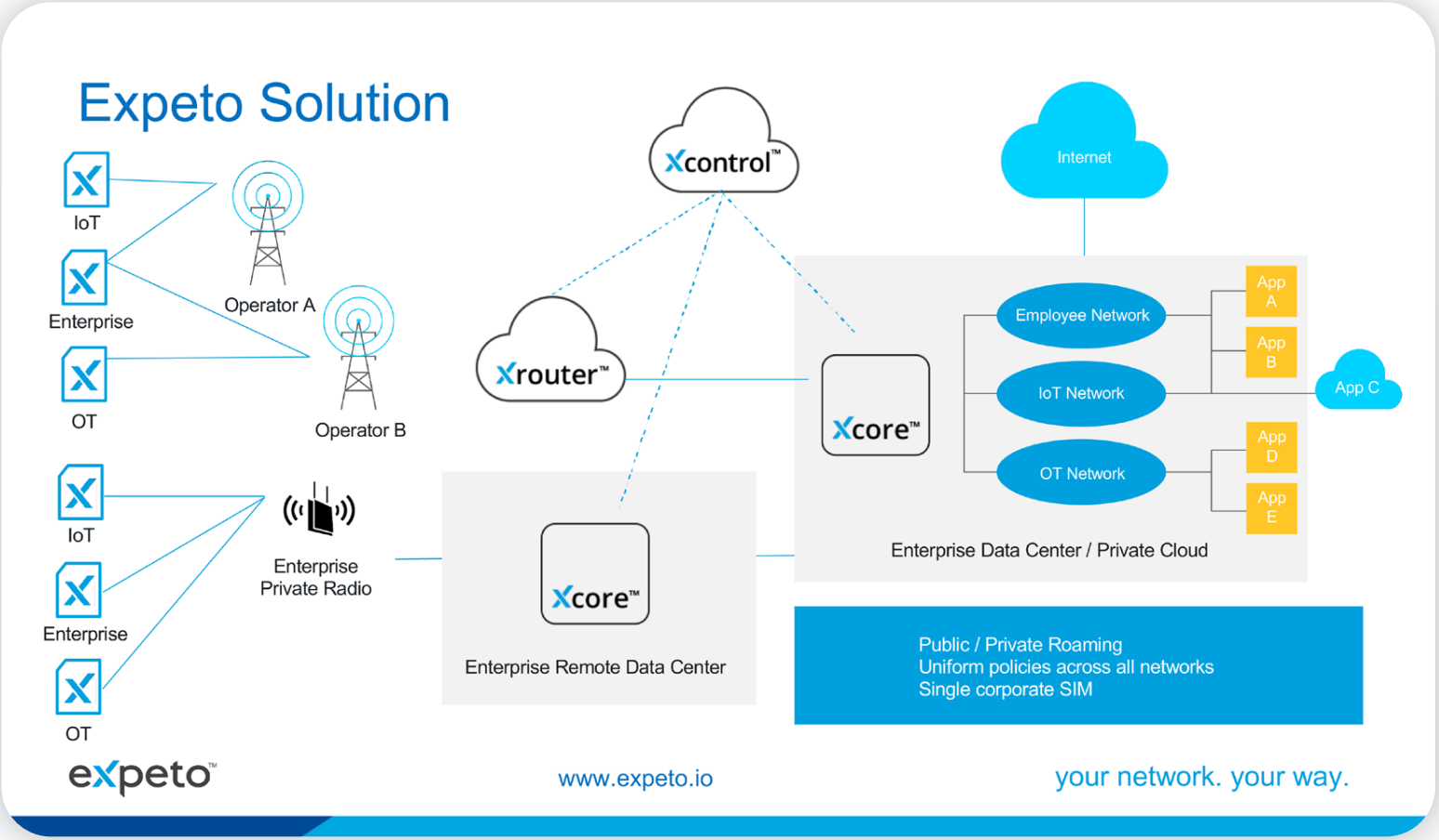
The Cradlepoint Verify application simplifies the installation, reduces the time to deployment, eliminates errors, and includes detailed analytics and reporting. Cradlepoint Verify allows the operator to install the Cradlepoint gateway while verifying Wide Area Network (WAN) and cellular checks, antenna placement, and produces an installation summary report which can be sent back to network administrators. This application allows for zero-touch deployments and greatly reduces the number of errors that can occur while having an operator install the gateway in the field.

NetCloud also offers a Full-Stack of analytics (Layer 7) allowing IT teams to gain insight into applications, network health, and security data through intuitive dashboards and actionable alerts that provide a full picture of their Wireless WAN, applications, and network usage. NetCloud simplifies network management by making it easy to access online education tools, and connect with other customers. Another rich feature of the NetCloud Service and Cradlepoint endpoints is the ability to access network data that third-party applications need to provide higher levels of insights and control. NetCloud Service extensibility makes this rich data available in a variety of ways to meet user requirements.



The Expeto platform enables enterprises to design, to deploy, and to grow private 5G/LTE networks to meet evolving business requirements. The platform integrates subscribers with private 5G/LTE subnets/segments within hybridized private and public cloud deployments. It allows for global implementation with centralized command and control over critical networking elements and data behind a corporate firewall.

Cellular connectivity is deployed as an entirely private infrastructure or integrated with existing mobile network operator networks. Network flexibility and scalability is achieved through containerized microservices which can be orchestrated, distributed, and elastically deployed anywhere from a Public Hyperscaler Cloud to the Customer far edge while ensuring Enterprise command and control. The containerized nature of the components allows



installation of multiple instances in different combinations across the network, enabling global coverage, high availability, performance scaling, low latency, and network evolution.

Three key components of the Expeto platform are:
Expeto xControl is a multi-tenant cloud-based application accessed through a web browser GUI or REST API calls. It provides a single control plane for SIM management, networking, security, and routing of all devices and data across private and public mobile networks world-wide. The GUI interface features include an interactive dashboard, intuitive navigation, real-time updates, and deep search. As an administrator, you create and manage the systems, customers, and subscribers/things of your sites. Set data routing to get valuable information to ensure the insights to take timely and valuable actions. You monitor network health and subscriber status, data usage and throughput levels. You set thresholds to enforce data limits, create profiles and groups, initiate QoS policies and relevant network routing, and assign custom network parameters. Provided as a managed service, xControl can be integrated with various Enterprise applications and customized using the API.

Expeto xCore, installed inside the enterprise in a data center or cloud, securely supports both private and public RAN. The private RAN implementation of Expeto xCore is a complete 3GPP compliant network core providing networking over a 3G/4G/5G Mobile Network. It includes fundamental 3GPP components that are fully compliant with 3GPP specification standards.

In the public RAN implementation, Expeto xCore connects to the Expeto xRouter service which enables access to the public network. Devices seamlessly roam between public and private networks with policies set by the enterprise while maintaining complete data visibility and routing control for the enterprise.

The Expeto xCore flexible architecture allows for public only, private only, or hybrid public/private networking.

Expeto xRouter is an application service managed by Expeto that supports traffic redirection from select mobile network operators. With instances deployed in multiple countries, the xRouter acts as a global “home network” for registered SIMs. The xRouter authenticates subscribers, applies policy management, and determines network routing before establishing an IPsec tunnel and forwarding traffic to the Expeto xCore.

From the Subscriber point of view, the experience is seamless roaming between public networks, regardless of geographic boundaries or networking type.

End-to-end security

Concerns about IoT security are not new, but they have grown in line with device deployments, which continue to proliferate. Moreover IoT now encompasses an increasing number of business-critical activities, in particular in private networks. As a result, the business community's need for secure end-to-end solutions and maintenance to a high security bar has never been greater.

IoT solutions are normally attacked at the various interfaces: between devices and gateways, gateways and the cloud; and cloud to the enterprise. In addition the devices and gateways are vulnerable, as are IoT platforms. High levels of security can only be realized if security mechanisms are an integral component of the overall architecture.

Protecting operational technologies is already critical. Adding IoT devices to this in a PCN setting, fueled by 5G capabilities such as hyper scalability, ultra-low latency, support for machine communications, predictability, agility and high precision, raises significant challenges of a fast-growing attack surface. There are many different architectures for deploying PCNs, which vary based on the enterprise and industry requirements, use cases and range of regulations and allocations per country. A company looking to build its own PCN should start by assessing its cyber maturity and be aware of the skills and technology required to detect, block and respond to cyber threats.

Some points to consider when designing a secure 5G private network:

- Security needs to create a virtual air gap in production environments to protect against threats, contain and limit their progression and impact. This usually involves micro-segmentation and access control of the different production networks and devices.
- Industrial devices are often not updated in time to avoid jeopardizing the availability of the production process. They may continue to have a well-known vulnerability for weeks or even months. In this case, the security infrastructure in place should provide a remedy to prevent vulnerabilities being exploited until the devices are updated.
- Predictable low latency is also a key aspect. If security measures add extra milliseconds that slow a production process down, this can bring to a halt or even harm an entire production line if the inputs and outputs used by the industrial control application arrive too late to be usable.
- Security elements need to have a low footprint and in some cases be able to work in environments of high temperature or humidity, which may require ruggedized solutions.

It is well known that factories and logistics hubs are very attractive targets for denial-of-service attacks, ransomware raids, disruptions or industrial espionage. As a result, operators and industrial players are making cybersecurity an integral part of their 5G private network in order to avoid risking losses greater than the network investment they are making or the productivity gains 5G is bringing. Segmentation, access control and network-wide visibility are all key to securing these private mobile networks.

THALES

Connect and Secure Your Private Network

Convenience & Trust

For employees or « things », Private Networks have to offer a seamless and secure User Experience, at the first initial connection and later, for all recurrent daily use.

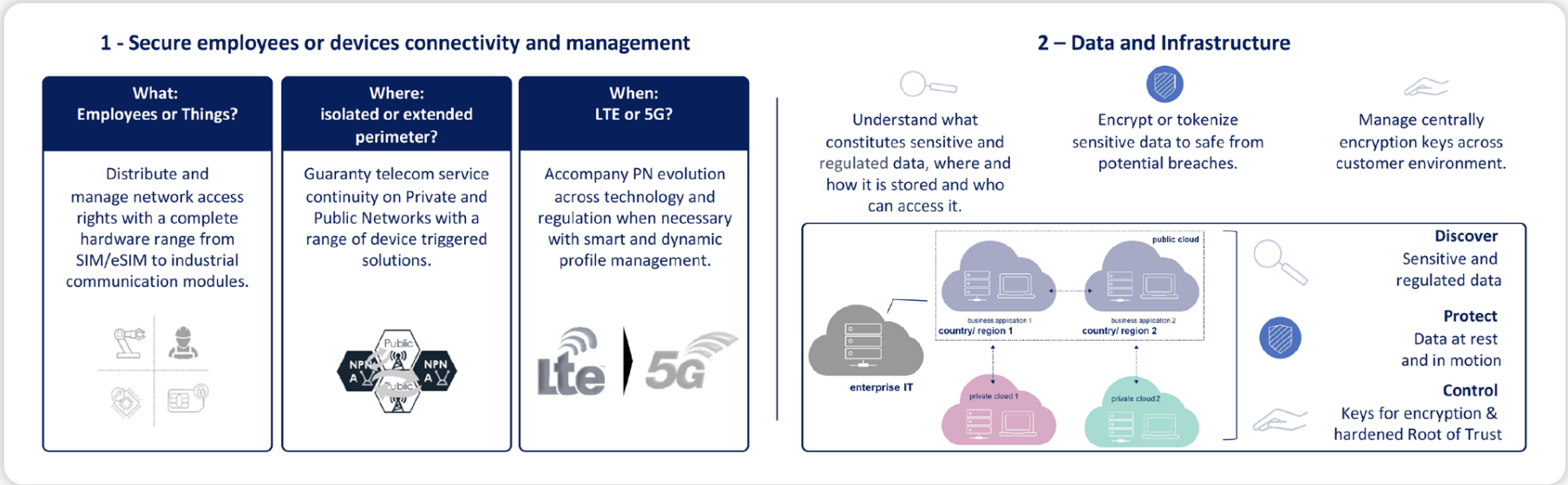
Trust has also an important role to play. By design Private Networks are pervasive and get access to a wide range of intimate and critical IT resources: inventory, production flows, digital twin, employee's list with their empowerment, customer's data and all the corresponding production and accounting applications. These application and applicative data can be shared between public and private cloud, and data are constantly exchanged on the air or on a dedicated slice.

What is at stake with Private Network cyber protection?

These new use cases increase significantly the exposure to different cyber threats with different consequences according to your stakeholder's position.

- Enterprises are responsible for their data and applications across the processing cycle, particularly when it comes to data that has specific legal requirements.
- CSP have to secure their core network and provide the appropriate security tool box to their B2B customers,
- System Integrators have to advice, accompany and coordinate the different stakeholders so at the end everything works, safely and according to customized SLA.

Figure 4.8 *Thales are deploying 2 folds Value Propositions for an enhanced connectivity and cyber protection*



PCNs and Data: Edge Computing and AI in IoT Solutions

PCNs are not the only connectivity solution for IoT applications, but the combination of present and future features, including low-latency and high bandwidth, make them well suited for IoT applications relying on other rapidly developing technologies, including those used for processing data, especially at the network edge, where IoT devices reside.

Edge computing

Edge computing – processing data at the edge of a network – is not new. Embedded systems, in which a microprocessor, memory, and i/o devices are "embedded" in a larger piece of equipment or machinery, controlling it, have existed since the 1960s in some sectors, most notably in manufacturing operations. 98% of all microprocessors manufactured in 2009 are estimated to have been used in embedded systems. If the equipment or machinery with an embedded system is connected to the edge of a network, edge computing is taking place.

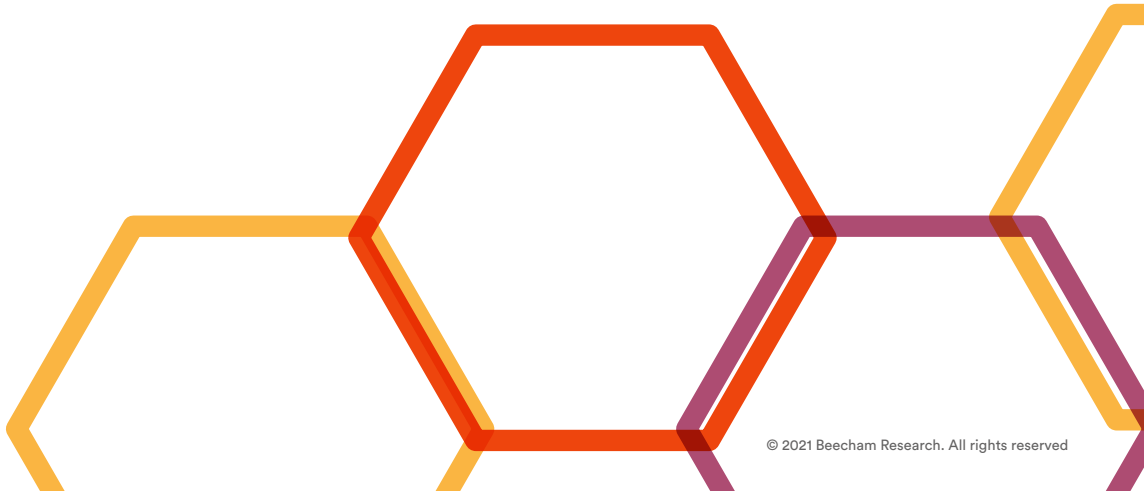
What has changed, and continues to change, is the size of microprocessors and memory – both have become very small compared to their predecessors, greatly reducing power consumption even as the computing power of CPUs has drastically increased.

At the same time, sensors used to acquire data for IoT applications have also become much smaller, less expensive, and require much less energy. Meanwhile, technologies for processing and analysing data have also rapidly developed, leading to a great increase in awareness of the value of data and what can be accomplished with it. These data technologies were initially confined to the cloud and local computer systems but with tiny, powerful, CPUs in edge devices (or in gateways and routers that may be used to aggregate data from multiple devices and sensors), this is no longer the case.

This has greatly increased the potential use of edge processing for controlling operations in an increasingly wide range of applications, including those most relevant for PCNs.

The underlying developments are visible in all areas of computing and telecommunications, not just in IoT, and also underly the whole process of spectrum allocation and reallocation and the perpetual transition from one generation of cellular technology to the next – greater amounts of data are being transmitted, from all devices of all types, and mobile networks must carry it.

On the consumer side, compare handsets (a kind of edge device) of ten years ago and the networks they utilized to today's situation. On the IoT side, compare devices and their capabilities (and mobile networks they were connected to) from ten years ago to today's. What is possible today was simply not possible or practical a few years ago – edge computing in IoT has not only become possible; it is also becoming necessary for all but the simplest applications.



Cloud and edge computing together

Cloud computing has grown no less than edge computing. Even if data can now be processed at the edge for real time control of operations, massive amounts of data can be processed in the cloud for such purposes as trends analysis across one or multiple locations. The extent of processing at the edge or in the cloud is a balance that varies according to individual application requirements at any particular time.

IoT edge computing can be and is used to reduce the amount of data sent to the cloud, reducing costs and complexity. In addition, an increasing range of applications in all sectors require very low latency – sending data from them to the cloud and back would create unacceptable delays for local control and automation; not so with edge processing.

PCNs and Edge Computing

Increased edge processing capabilities were initially seen as a way to reduce data in order to facilitate IoT applications at a time when wireless connectivity was constrained, but data assumed increasing importance even as edge processing capabilities continued to increase. The features of cellular connectivity in PCNs, including greater bandwidth, reduced latency, and high reliability and security, are well suited for this newer phase of edge computing -- the two developments go hand in hand.

Multi-Access Edge Computing (MEC)

Multi-access Edge Computing (MEC) is an international standard developed by an Industry Specification Group (ISG) within ETSI to advance and elevate edge computing's role by giving content providers and software developers cloud-computing capabilities that are close to the end users. Basically, it formalises the creation of the small, local data centres.

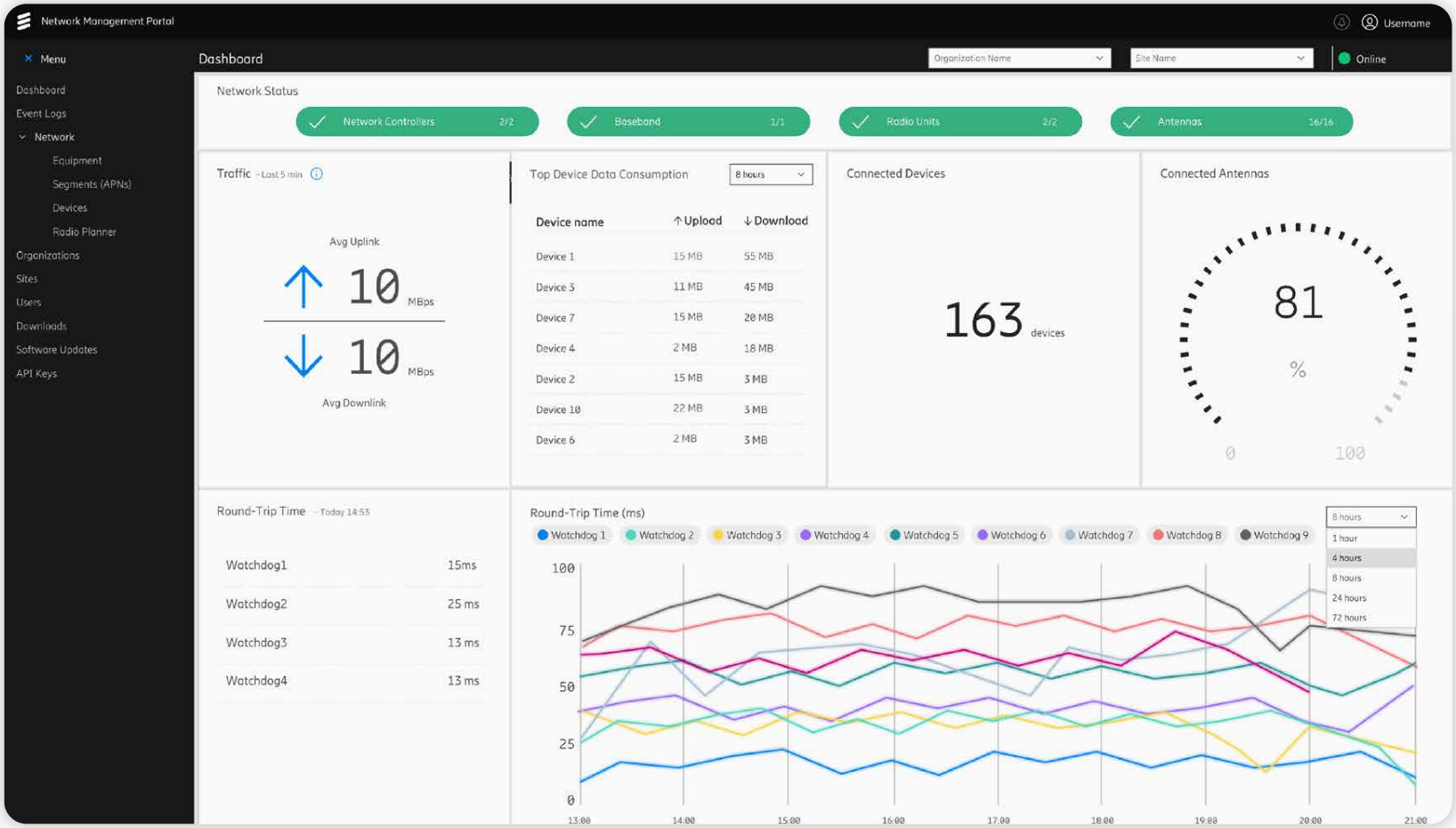
Current MEC uses cases are not restricted to IoT. They also include: Video analytics, Location services, Augmented reality, Optimized local content distribution, and Data caching.

Multi-access Edge Computing is a consequence of the convergence of IT and telecommunications networking. The MEC system combines the environments of networking and computing at the edge of the network to optimize the performance for ultra-low latency and high bandwidth services. It enables the creation of a standardized, open environment that will allow the efficient and seamless integration of applications from vendors, service providers, and third parties across multi-vendor MEC platforms.

Local Management Control of PCN

Private networking provides local site management with the ability to control their own network resources. An example of this is Ericsson's Network Management Portal (NMP). This is a user-friendly interface that enables an IT administrator to manage an Ericsson Private 5G cellular radio network.

Figure 4.9 *Example dashboard of Ericsson's NMP*



ERICSSON

The following tasks can be performed using the NMP:

- Installation
- User management and role-based access permissions
- Device and network management
- Monitoring
- Maintenance tasks
- Support access

Looking at a few of these in more depth:

Configuration and Device Management
The following network parts can be defined and managed using the NMP:

- Organizations: companies, corporations, and public organizations
- Sites: an Ericsson Private 5G cellular radio network at a customer location such as a factory or warehouse
- Segments: network segments within a site, also known as Access Point Names (APNs)
- VLANs: handle integration with customer enterprise network VLANs
- Devices: write SIM cards, add, and manage devices
- Support access grants: create and revoke support access to a site
- API access: create tokens that can be used for integration with other systems such as Industrial Internet of Things (IIoT) platforms and Network Management Systems (NMSs)

User Management
The NMP implements Role-Based Access Control (RBAC) and Task-Based Access Control (TBAC). Permission to view, create, and edit sites, organizations, and partners through the NMP is granted based on user roles.

Organization Account Manager
The Organization Account Manager role can access multiple organizations and sites associated with one partner and has the following access rights and responsibilities:

- Add and manage organizations
- Add and manage Organization Account Manager, Installer, and Support Tier 1 user accounts
- Locate and handle dormant Installer and Support Tier 1 user accounts

Installer
The Installer role can access multiple organizations and sites and has the following access rights and responsibilities:

- Set up and configure sites
- Add Site Admin user account
- Full access to organizations associated with one partner, when granted by an Organization Account Manager

Site Admin
The Site Admin role can access sites within one organization. The main access rights and responsibilities of the Site Admin role are as follows:

- Add and manage users with access to a site
- Manage network equipment
- Add and manage devices, segments (APNs), and VLANs
- Add and manage API keys
- Schedule software updates

Other areas accessible through the NMP include: Support for Tier 2 and Tier 3 roles, additional support for Tier 1 roles, Security Administration, Device Administration, Viewer role and Network Controller Software Updates.

Data analytics

Data is the fuel that powers the IoT, but its value comes from analyzing and using it to deliver tangible benefits, e.g., boost operational efficiency, cut costs, and enable the development of new business models. Preventative maintenance programs employ real-time data to deliver insightful information on manufacturing equipment and processes, a development that industry now takes for granted.

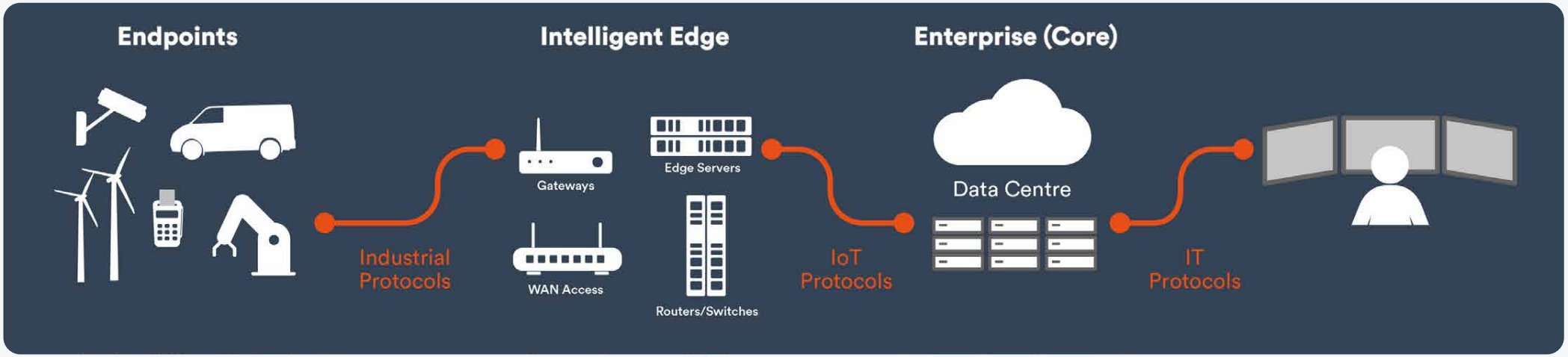
Data analytics divides into long term analytics employed in a central facility, typically the cloud, where historic data is used to discover hidden patterns, unknown correlations, market trends, customer preferences and other useful business information, and analytics performed in a local facility at the edge of the network, where it is employed to generate near real-time intelligence on operations in the local environment.

Figure 4.10 illustrates that division within the value chain. Data analytics starts at the end points where data is generated and finishes at a private data centre or the public cloud. And a private network can be employed to provide robust, secure end-to-end communications.

Combinations of long-term and real-time data analytics are used to enable predictive analysis, which is based on historical data, and it relies on human interaction to query data, validate patterns, create, and then test assumptions. It is used to reveal hidden patterns, unknown correlations, market trends, customer preferences and other valuable business information.

Data analytics can be used in different ways to realize different objectives, but the baseline technology is the same – processing data to enable a transition from data to information and knowledge and on to productive outcomes.

Figure 4.10 *Data is processed and analysed at the edge of the network, where intelligence is employed to deliver near real-time information. Cloud computing processes and analyses IoT and related business data at a central facility.*



Machine learning

Machine Learning (ML) is the technology that enables computers to "learn" without being explicitly programmed. It focuses on a specific task and enables decisions to be made with minimal human intervention. ML analyses historic data, makes assumptions, learns, and provides predictions at a scale and level of detail that would be impossible for mere mortals. It's an extension of the predictive analytics model but can make assumptions, test, and learn autonomously.

The technology employs algorithms that predict outcomes based on input data and the accuracy of the prediction improves over time as the result of new input data. It's an iterative process: as models are exposed to new data, they can adapt. They learn from previous computations to produce reliable, repeatable decisions.

ML and Machine vision

Machine learning techniques can be applied to a wide range of machine vision image processing tasks. It is becoming cost-effective to add machine vision capabilities to an increasing variety of IoT products that perform complex tasks reliably and consistently. For example, in industrial environments machine vision provides visual quality control inspection of identical items being transported on conveyor belts at high speed. In transportation, a company is building a rail track monitoring system to detect obstacles on the tracks, e.g., people or material. In addition, the system's thermal camera sensor detects hot spots caused by electrical faults.

In this innovative use case, the key benefit of deploying ML at the edge is the capability of showing events, anomalies and inconsistencies that may not be spotted with the naked eye or be able to be interpreted and understood by humans at the high speed the train is travelling.

The combination of machine learning and machine vision delivers real-world operational improvements. They include:

- Higher product quality: Inspection, measurement, gauging and assembly verification.
- Increased productivity: Routine, repetitive tasks can be performed quickly and automatically, freeing staff for higher value activities.
- Lower costs: Adding machine vision capabilities to equipment can improve performance and extend service life. Machine vision systems in a factory setting also take up less room than human operators and don't require the same level of safety infrastructure.
- Wearing a helmet.

Artificial Intelligence

The ability to learn autonomously has also resulted in some confusion between machine learning and Artificial Intelligence (AI). Machine learning is a branch of AI that enables decisions to be made with minimal human intervention.

At a very high level, artificial intelligence can be split into two broad types: narrow AI and general AI. Narrow AI is what we see all around us in computers today: Intelligent systems that have been taught or have learned how to carry out specific tasks without being explicitly programmed to do so. General AI is problematic, controversial, and currently of marginal relevance to IoT.

AI automates repetitive learning and discovery through data. Instead of automating manual tasks, AI performs frequent, high-volume, computerized tasks, reliably and without fatigue. Because AI algorithms learn differently than humans, they can notice relationships and patterns that escape us, although ov f course humans are needed to set up an AI system.

As indicated earlier, real-time data is processed at the network edge, historic data in the cloud or a private data centre. AI can be deployed in both locations, using different algorithms in order to realise different objectives.

AI chipsets

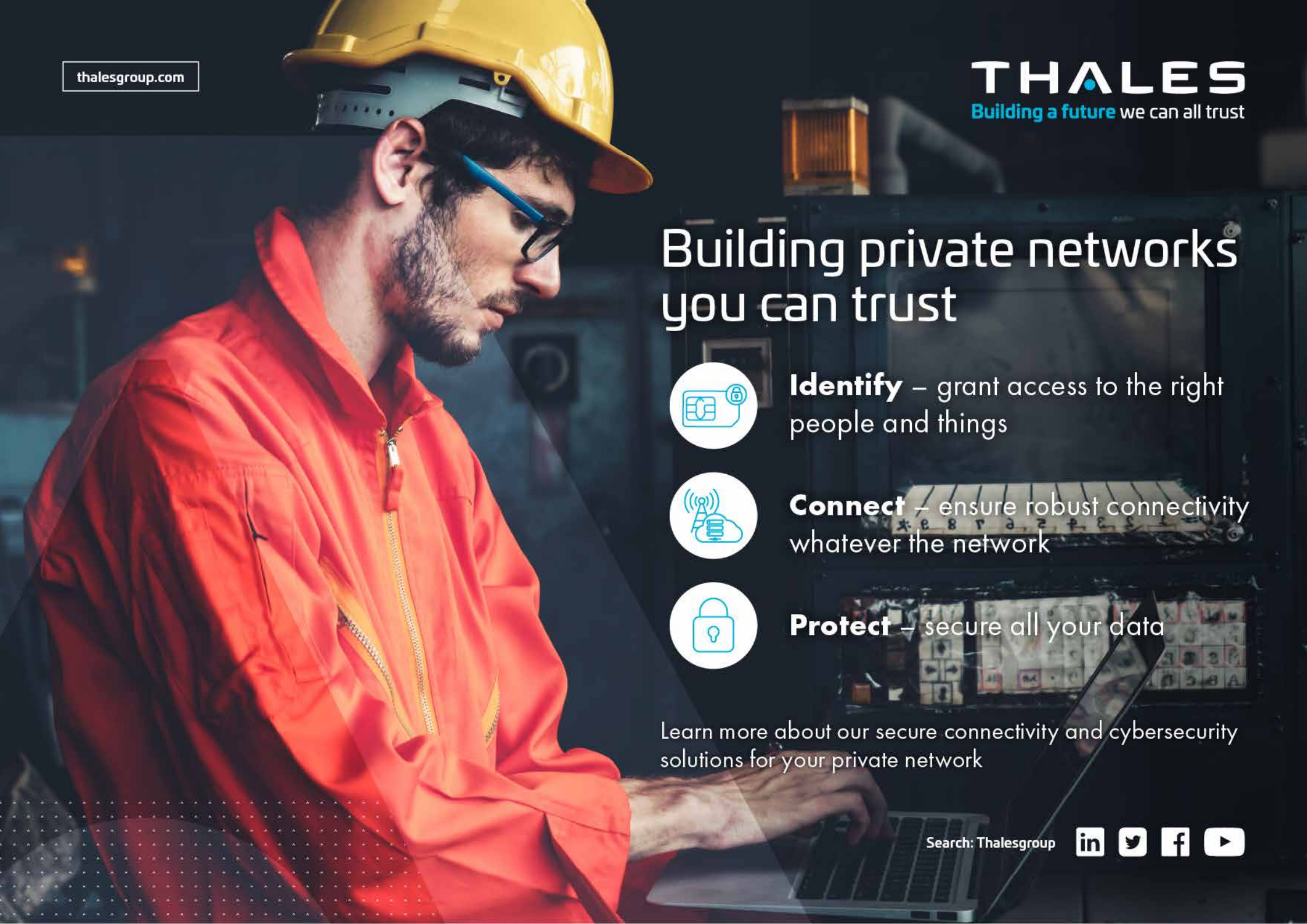
Edge and cloud computing perform different tasks, which can be enhanced by different AI chipsets. A cloud AI chipset generally has higher computational power, higher power consumption, a larger physical footprint and is therefore relatively more expensive. Edge AI chipsets are smaller and less expensive.

AI and edge computing combine to identify issues that can lead to system failures and then route the information to local personnel. Voice recognition increasingly relies on edge AI, and there are industrial uses where AI-enabled cameras and other sensors can monitor production and initiate immediate adjustments without having to be connected to the cloud or a private data center. Moreover, edge AI can function without a network connection should it become unavailable. If there is a connectivity malfunction, the edge device will continue to perform.

Key benefits of edge AI include:

- Providing predictive insights for proactive and pre-emptive troubleshooting.
- Enabling higher uptime as information processing can take place even without a network connection.
- Local filtering of relevant from irrelevant data
- Enhanced privacy and security, for example with some medical patient data being processed at the edge to ensure privacy.
- Less data needs to be sent to the cloud, reducing power requirements and cost for some applications.

The benefits reflect the functionality that allows edge AI to be used for next-generation applications. For example, GPUs (Graphics Processing Units) in security cameras can run recognition software locally instead of centrally. In a smart city AI-enabled cameras could employ their local intelligence to help manage traffic and perform other advanced functions in addition to recognition tasks.


thalesgroup.com
THALES
Building a future we can all trust
Building private networks you can trust
Identify – grant access to the right people and things
Connect – ensure robust connectivity whatever the network
Protect – secure all your data
Learn more about our secure connectivity and cybersecurity solutions for your private network
Search: Thalesgroup

Summary

PCNs, boasting high reliability, security, coverage, and suitability for moving assets, are rapidly emerging as ideal IoT connectivity solutions for specific industry segments even as 4G LTE cellular technology transitions to 5G technology and spectrum is being reallocated everywhere to enable ever greater quantities of data to move over wireless networks.

Parts of that transition (3GPP 5G releases 17, 18, 19) have been delayed by the Covid-19 pandemic even as the pandemic has led to the creation of new IoT applications as the adoption of IoT itself continues to grow.

This is happening as changes in cellular networking infrastructure technology such as Radio Access Networks (RAN) and Evolved Packet Cores (EPC) have made PCNs practical as small cell alternatives to macro cellular networks, using on-site general purpose computers instead of expensive proprietary hardware located in distant centers. Enterprises can choose to own their own site-specific cellular networks.

The reallocation of spectrum requires mechanisms or frameworks for minimizing interference with incumbent users in newly available unlicensed spectrum. In the U.S., Citizens Band Radio Service (CBRS), using freed up 3.5 GHz spectrum, served as an experiment in this direction. Its success points the way towards using PCN in other newly available spectrum but also for PCNs, period, including those typically being deployed in industrial settings in Europe using location-limited licensed spectrum and those that will be using other unlicensed spectrum bands.

Two other trends feed into this:

1. The long-term trend of the miniaturization of electronic components of all types; and
2. The increasing use of data for achieving business outcomes leading to a much greater appreciation of the value of data and the development of new technologies for analyzing it.

Both trends connect with the rise of edge computing in which greater computational power (and memory) can be embedded in IoT edge devices for data analysis, either preliminary analysis before being sent to the cloud, for on-premise data analysis, or for a hybrid solution.

Associated networking equipment (routers, modems, switches, and gateways) have become much more “intelligent” as CPUs and RAM have become smaller, faster, and more energy efficient, part of IoT solution infrastructure in all PCN sectors.

The heightened awareness of the value of data for IoT applications has enabled rapid growth in the various data analysis technologies – data analytics of all types and newer machine learning and AI technologies, including the development of AI chipsets.

In short, PCNs are in the middle of a perfect storm.

Sponsors' IoT Offerings:

Short profiles of our research sponsors and some of their offerings in the PCN market. For more detail, please contact them direct.

WEBSITE

ERICSSON

Networks dedicated to the needs of enterprises

Pre-integrated solutions for fast and flexible deployment

Modernization and digital transformation have increased the need for stable connectivity, which is fundamental to business operations today for those wishing to optimize operations and security, and open up new revenue streams.

Digitalization of business operations and the evolution of the Industrial Internet of Things (IIoT) requires both integration and connection of machines, people and other devices across a wide range of use cases. As neither Wi-Fi nor public networks can offer the reliability or security needed, connectivity through cellular technology is foundational to this digitalization.

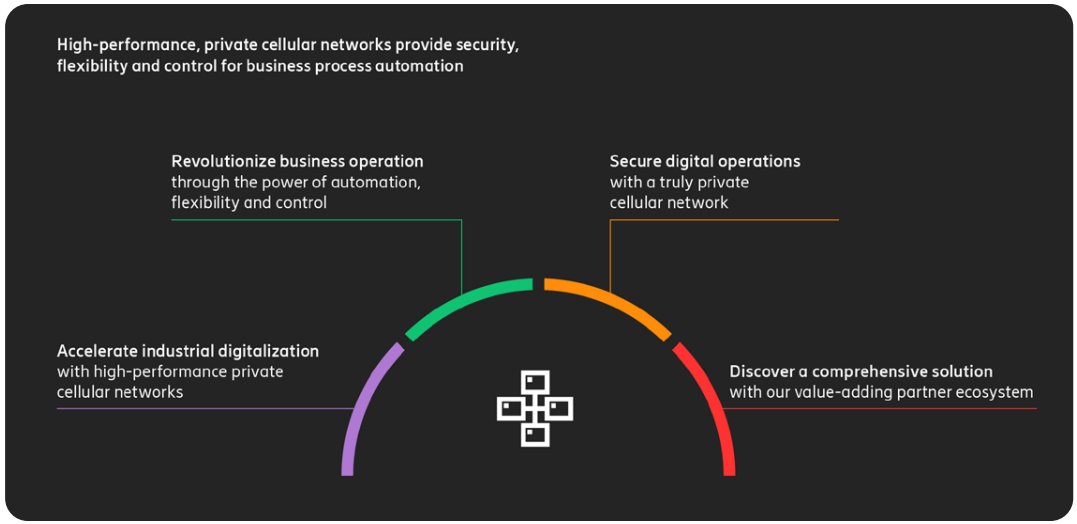
Many enterprises in industry sectors, such as manufacturing and airports, are pursuing operating models that improve productivity through analytics, automation, and machine or device communications, making security and data confidentiality crucial for connectivity solutions. Facility automation, control of automated guided vehicles, smart grid solutions and high-definition video surveillance are examples of high-performing and reliable wireless networking solutions that are fundamental to business operations.

The need for network coverage with high performance, security and reliability is therefore integral for enterprises to be effective within the Industry 4.0 landscape. Ericsson has a complete portfolio for local cellular connectivity with dedicated 4G and 5G networks.

Many connected endpoints within enterprise operations are entirely new – autonomous mobile robots, cooperativerobots (cobots), augmented reality (AR), modern human-machine interfaces and PCs – and would benefit from cellular connectivity. With Wi-Fi and public networks, enterprises often lack a stable platform to connect these devices, so it is harder to monitor and control, which opens up security threats. Connectivity can be unpredictable, and the downtime caused by connection loss can be enormously expensive.

A dedicated private network is the perfect solution, providing a reliable connection and tighter security to maintain industrial data and Operational Technology (OT).

Our Dedicated Network offerings provide private cellular networking solutions for industrial enterprises positioned to start adopting these technologies and benefiting from innovative use cases. The sectors poised to take advantage of these revolutionary technologies are manufacturing, ports, airports, mining, energy utilities, and oil and gas. We offer solutions to the current connectivity restrictions and complexities of IIoT by using a single on-premises cellular network to connect assets, ensure workflows and allow enterprises to dynamically redesign their operations with flexibility, safety and efficiency.



WEBSITE

ERICSSON

Functionality and setup of dedicated networks

Ericsson has one complete portfolio for local cellular connectivity, available through communications service providers. It consists of modular Ericsson Private Networks and pre-packaged Ericsson Ericsson Private 5G to address the needs for industrial facilities and campus network deployments.

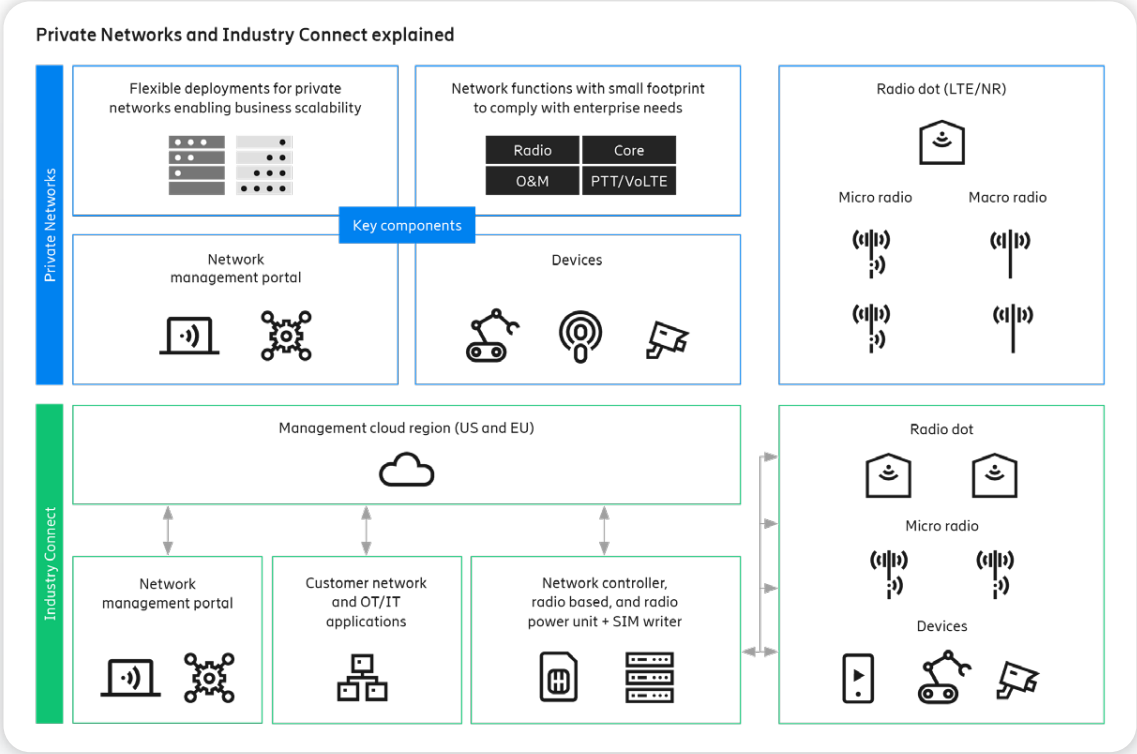
A private network is locally set up and utilizes dedicated radio equipment to serve enterprises with cellular connectivity. Its radio coverage is therefore independent of public mobile networks provisioned by mobile operators.

The main benefit of this is a guaranteed quality of service tailored to business and application performance needs, with 4G or 5G capacity that encompasses high device density and predictable latency.

Private networks are easy for IT and OT professionals to operate and manage in industrial environments.

Our Dedicated Network offerings
Ericsson offers reliable communication solutions for private networks with any business-critical demand, providing the reliability, device density and security that current wireless solutions using unlicensed spectrum struggle to achieve. We have two prime offerings: some cases can be covered by the pre-packaged

Ericsson Private 5G product, while others require our modular and flexible Private Network solution.



Both are available through operators who will also provide the spectrum.

Private Networks – a customizable private cellular connectivity solution capable of addressing any industrial facility requirements.

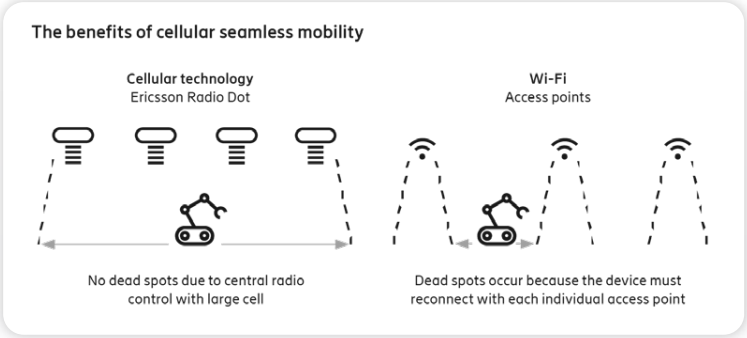
- Pre-integrated, designed for extensive standalone facilities with complex operations
- Addresses connectivity challenges in industrial campuses and their adjacent outdoor areas
- Enables a wide variety of industrial use cases for a smooth transition to 5G

Ericsson Private 5G – an easy-to-use, pre-integrated and pre packaged private cellular connectivity product, purpose-built for industrial environments. It is designed to be a simple, stable and secure product.

- Product designed to be easy to use for IT and OT professionals
- Addresses connectivity challenges in industrial campuses and their adjacent outdoor areas
- Enables a wide variety of industrial use cases for a smooth transition to 5G

ERICSSON

WEBSITE



Solution overview and benefits

Dedicated networks offer a host of advantages compared to competing technologies and applications, such as public networks, fiber, ethernet, Wi-Fi, Bluetooth and WiMAX.

Guaranteed coverage

A private network guarantees fullcoverage in the enterprise's operations area, both indoors and outdoors as required, as well as in remote locations where public networks are not available, for instance at mining locations and offshore oil rigs.

Security and encryption

Private networks, based on cellular technology, offer high security levels since 3GPP standards are closely adhered to across vendors and include some of the most stringent encryption standards, meaning that all sensitive data stays on the premises.

Ensured capacity

A private network removes contention with other network users to ensure the availability of capacity for the enterprise.This makes it possible to guarantee network performance, such as uplink and downlink bit rates and latency.

Retained control

Private networks let enterprises determine and control how resources are utilized and how traffic is prioritized, and the Radio Access Network can be customized to optimize reliability and latency. Enterprises can also control their security to ensure that sensitive information remains secured within their premises.

Critical reliability

A private network based on LTE and 5G technology offers performance and enables applications that cannot be accommodated by Wi-Fi, such as ultra-high definition video surveillance.

Predictable and ensured low latency

Private networks are predictable and ensure the low latency required for many IoT applications that rely on time-bound communications, where delays can result in a catastrophic failure, such as for critical control of remote devices like heavy machinery.

High data speeds for communication

A private network offers higher data speeds compared to narrowband Land Mobile Radio systems which suffer from capacity restraints. This is ideal for video and high-resolution imagery, which is highly desirable to our enterprise customers.

Ecosystem

The Ericsson Industry 4.0 ecosystem of devices, applications, system integrators and OEMs creates market demand and complements the portfolio, which allows the user to take advantage of innovative use cases.

Future-proof

Ensured compatibility and readiness for 5G will allow users to benefit from the enhancements and functionality that 5G can offer.

Our ecosystem partnerships

Devices and hardware

Machinery OEMs and companies providing chipsets, modules, gateways, sensors and IT infrastructure that enable or are enabled by cellular connectivity; suppliers of enabling SIM technologies.

Software and applications

Application developers, independent software vendors and hyperscale cloud providers developing and selling offerings that reside in any of the IT layers of the enterprise.

Professional services

System integrators, business advisors and test houses with offerings and services for installing and running the network, testing and certification, or end-to-end solutions and industry digitalization.

Ready to get started?
We can put you in touch with our mobile operator partners.

WEBSITE

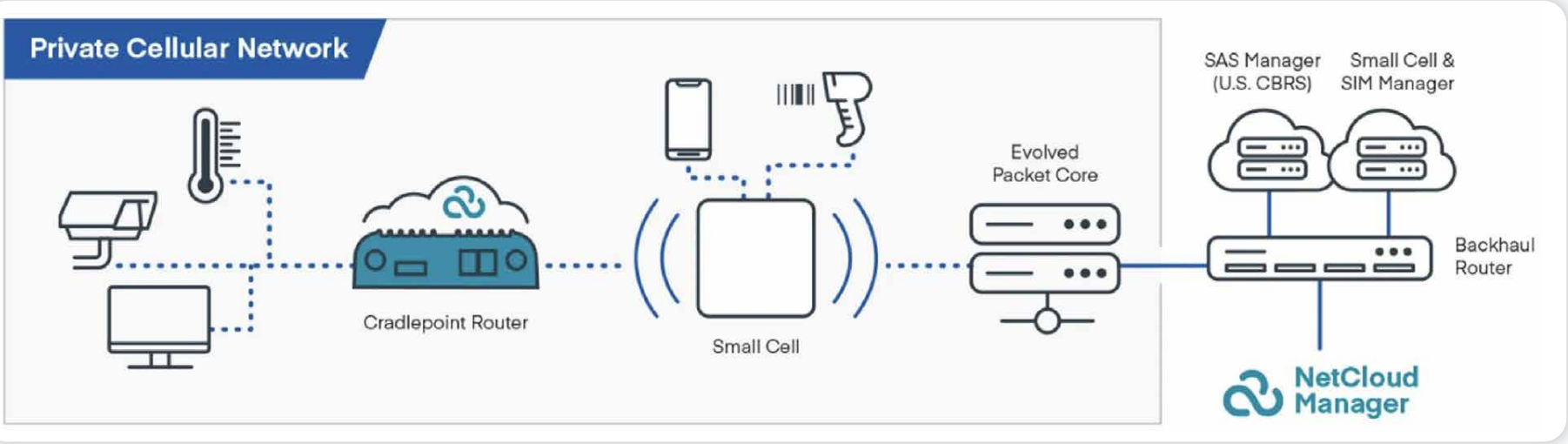
cradlepoint

Cradlepoint is an Original Equipment Manufacturer (OEM) of wireless edge solutions. These unlock the power of LTE and 5G cellular networks to connect fixed and temporary sites, vehicles, field forces, and IoT devices, anywhere. NetCloud Manager is at the heart of everything Cradlepoint does. It is a cloud-based subscription service that combines cloud management, software-defined networking, and unified edge security with industry-leading LTE and 5G cellular networking technology to power a portfolio of purpose-built wireless edge routers and adapters.

More than 15,000 enterprise and government organizations around the world — including 75 percent of the world's top retailers, 50 percent of the Fortune 100, and 25 of the largest U.S. cities — rely on Cradlepoint to keep critical sites, workforces, vehicles, and devices always connected and protected. Major service providers use Cradlepoint network solutions as the foundation for innovative managed service offerings.

Cradlepoint is now an Ericsson company, having been acquired in November, 2020. This acquisition united the global leader in 5G communications technology with the global leader in 4G LTE and 5G wireless edge solutions. Together Cradlepoint and Ericsson are uniquely positioned to unlock the full transformational value of 5G with end-to-end intelligence and control that spans from the carrier core to the enterprise edge.

The figure below shows how Cradlepoint supports an overall PCN solution. Cradlepoint devices coupled with the Cradlepoint NetCloud Manager (NCM) service offer very high flexibility when operating within a 4G or 5G network. Because the devices are standards based, they can operate on any 3GPP-compliant network and communicate on any Internet Protocol (IP) network. To add further integration, the Cradlepoint application programming interface (API) and software development kit (SDK) can be leveraged to create and share information between software programs from 3rd Party Management systems, unmanned/automated business systems, AR/VR, artificial intelligence (AI), or Internet of Things (IoT) endpoints.



WEBSITE

NetCloud Manager

The NetCloud Manager Service, combined with a purpose-built cellular-enabled wireless edge router, is delivered as a subscription aligned to meet business needs for branch connectivity, branch continuity, in-vehicle, and IoT networks. NetCloud offers a Full-Stack of analytics (Layer 7) allowing IT teams to gain insight into applications, network health, and security data through intuitive dashboards and actionable alerts that provide a full picture of their Wireless WAN, applications, and network usage.

NetCloud simplifies network management by making it easy to understand and apply licenses, identify and push out software updates, upgrade software feature sets, amass education tools, and connect with other customers. Another rich feature of the NetCloud Service and Cradlepoint endpoints is the ability to access network data that third-party applications need to provide higher levels of insights and control. NetCloud Service extensibility makes this rich data available in a variety of ways to meet user requirements. Whether a turn-key solution, a differentiated general connection/application, or a custom connection is required, NetCloud offers flexibility in making the connections.

Cradlepoint's solution can be leveraged for intelligent traffic steering through SD- WAN functionality. With minimal data usage, Cradlepoint services such as Smart WAN intelligently assesses the health of WAN link such as MPLS, Satellite, radio and LTE/5G and its ability to run applications. Follow this link for more on NetCloud in Section 4.

PCN Endpoints

NetCloud™ by cradlepoint

IDEAL PRODUCT POSITIONING	R500	900 w/dock	IBR1700	E300	E3000	R1900
	IoT CBRS only Cat 7	**Mobile** CBRS & Public Cat 18	**Mobile** CBRS & Public Cat 18	**Branch** CBRS & Public Cat 18	**Branch** CBRS & Public Cat 18/5G	**Mobile/IoT** CBRS & Public 5G/Cat 20
Students in home	X					
Video surveillance	X					
Sensors without integrated cellular	X					
Digital signage	X					
Kiosks	X					
CBRS network vehicles	X					
CBRS & public cellular small vehicle		X				
CBRS & public cellular large vehicle			X			
Small medium office/classroom				X		
Medium to large office/classroom					X	
5G CBRS & public cellular network					X	X

Cradlepoint routers for PCN

The Cradlepoint IBR, R and E series routers are all-in-one platforms that offer Cellular, Ethernet, Wi-Fi and Serial connectivity for all mobile, in-vehicle, branch and IoT needs. The figure shows the routers most suited to PCN and IoT applications. From a design standpoint, the Cradlepoint router will provide cellular connectivity over an LTE or 5G Modem and can accept dual SIM cards. For high availability needs, there is the added option of running a secondary modem to provide dual active networking capabilities. With respect to Antennas, Cradlepoint can work with internal and 3rd party suppliers for Outdoor Cellular + Wi-Fi antennas for external mobile connectivity. We leverage a standard SMA connection to allow for most supplier antenna connectivity.

WEBSITE

Key Features:

- Stylized indoor, in-vehicle and hardened outdoor models
- Mobile wizard-based installation application
- "Captive modem mode" with Cradlepoint router
- 5G+4G dual connectivity (ENDC)
- Support for SA (Standalone) 5G NR
- 5G tools & value confirmation in NetCloud
- Adaptive to any SD-WAN or router environment
- Zero-touch deployment & Day-1 wireless
- Advanced remote management suite
- Deep wireless analytics assisted by machine learning
- 5G tools & value confirmation built into the NetCloud platform
- Cloud-managed for ease of deployment, remote management & reporting
- Carrier-class connectivity with multiple levels of test & recovery

Bridging generations of cellular networks

Dual connectivity, otherwise known as ENDC (E-UTRAN New Radio – Dual Connectivity), is the technology that enables a 4G and 5G connection to occur at the same time. In the past, a change in network demand or availability typically resulted in a clunky transition between 3G and 4G. The device was forced to choose between one or the other. ENDC allows streams of LTE and 5G to flow simultaneously, ultimately increasing bandwidth and reducing service interruptions.

Through dual connectivity, the 4G LTE network acts as an anchor band that is supplemented by 5G providing a seamless handoff between the two. When connected to a 5G modem, ENDC allows traffic requirements to determine whether an LTE connection is sufficient to transmit data or if the traffic should be passed to an available stream of 5G.

WEBSITE

Expeto's NeXtworking™ solution is the world's leading cloud-based platform purpose built to enable mission critical hybrid 5G Private Mobile Networks (PMNs) for enterprise customers, allowing them to consume these networks according to their mission critical business needs. Seamlessly integrated into their existing IT systems, Expeto's NeXtworking platform allows enterprises to connect to any combination of private or public mobile networks – and manage their network of networks from a single point of control with complete visibility and control of their data. For the first time in the history of enterprise connectivity, enterprises can harness the full scale and security of cellular networks with a solution as easy to deploy and manage as Wi-Fi.

Expeto's platform presents a compelling opportunity for enterprises as well as Mobile Network Operators and Mobile Service Providers (MxOs collectively). For MxOs, NeXtworking can enable new and meaningful segment growth by providing enterprise customers with a versatile and valuable enterprise-first solution for Private Mobile Networking, using both public and private spectrum. MxOs can now offer enterprise IT/OT teams what they are demanding – the ability to manage their PMN on their own terms – while MxOs maintain their already established infrastructure. This effectively monetizes MxO network investments across new and valuable enterprise frontiers, while giving enterprise customers the IT/OT capabilities they require.

With the power of control over their own network of networks, enterprises are fully equipped to manage crucial network operations from the comfort of their own IT department. Networks can be established in a manner of minutes, not the usual months, thus empowering enterprise customers to move further and faster through their Industry 4.0 journeys.

At the core of Expeto's NeXtworking platform is the understanding that every enterprise is unique. That is why NeXtworking is inherently scalable to satisfy a wide range of use cases – no matter the device density or low latency required. So, whether you are an MxO searching for an adaptable 5G-powered PMN to deliver to enterprise customers, or you are the enterprise itself, unwilling to compromise on your connectivity requirements – NeXtworking is well suited to meet your needs and launch you into the next generation of business.

Put simply, Expeto's platform is the only enterprise-first PMN solution that offers the functionality of carrier grade connectivity with the ease of use of Wi-Fi and the power of control for the enterprise. And with the advent of 5G, Expeto is positioned to create meaningful industry disruption. NeXtworking gives enterprises the opportunity to harness the revolutionary capabilities of 5G for their own benefit while MxOs can see returns on their substantial 5G investments, while opening new compute and application revenue streams to meet ever-expanding enterprise needs.

Expeto's *Enterprise First*™ value proposition can be traced back to the inception of the company. The Expeto team includes seasoned experts with origins in both MxOs and enterprise software organizations, providing the team with the relevant experience and intimate understanding of enterprise requirements. Expeto has unique insight into how enterprise customers want to consume 5G and how MxOs can generate meaningful enterprise growth in supporting the enterprise IT/OT operating model. Ultimately, what enterprises seek are partners who can enable a 5G connectivity foundation for the digital initiatives which are essential to their growth plans and competitive differentiation. Incumbent hum-drum options are no longer adequate for enterprise outcomes - Expeto's NeXtworking platform is a bridge bringing MxOs, SI and application providers together to generate opportunities across the ecosystem and to deliver enterprise customers with solutions that meet their needs and exceed their expectations.

To learn more about Expeto and our and our innovative ecosystem of partners – including Hitachi, AWS, Rogers, Avanade and more – please visit our website at www.expeto.io.

WEBSITE

Pod Group is the world's first Enterprise Network Operator (ENO). An ENO puts the ownership of the IoT network into the hands of the enterprise, by providing managed services including global IoT connectivity, eUICC (eSIM), Private Cellular Networks and innovative in-house designed SIM applets via one centralized platform in a Network as a Service (NaaS) model. The main benefit of an ENO is that it combines the control and visibility of its own core network with the flexibility, customized services and global reach of a specialist in IoT connectivity.

With over 20 years of experience working in partnership with IoT enterprises across a wide variety of sectors, including telematics, transport and logistics, energy and environment, healthcare, retail, consumer applications, banking and finance, utilities, emergency services and security, Pod Group offers specialist consultancy and support services, as well as access to a wider ecosystem of partners to enable enterprises to create and deploy global IoT applications at scale.

We have offices across the globe and access to 600+ networks in 185 countries. As a result, Pod Group provides global multi-network, multi-IMSI and eUICC connectivity solutions combined with end to end security, centralized connectivity management and a hierarchical billing platform. Pod Group's dedicated IoT support team, including in-house developers and systems engineers, is available 24/7 to offer technical support and troubleshooting.

What does an ENO offer?

For too long enterprises have had to 'make do' with cellular networks that were designed more for consumer applications than for IoT connectivity. With a fragmented marketplace of MNOs and MVNOs, siloed networks with complex roaming agreements, increasing IoT security threats and a lack of centralized control, enterprises need tailored network services now more than ever.

A number of technical and market-driven factors have enabled Pod Group to become the world's first ENO. Spectrum is now available for enterprise use, which means that private LTE and 5G networks as well as roaming between public and private networks is now a possibility. The maturity of the eUICC standard has also opened up far more possibilities for enterprises, enabling remote provisioning of SIMs, access to multiple networks with a 'bootstrap' profile, and a 'future-proof' connectivity standard.

For enterprises to take advantage of these technological advancements, however, the market had to be ready. While MNOs tend to prioritize higher ARPU consumer applications and are not necessarily set up to serve long-tail enterprise applications, MVNOs are often unable to give enterprises full control of the core network, leaving Enterprise Network Operators to fill the gap and commit to fully serving enterprise needs.

There are three elements of enterprise network ownership that have been revolutionized by the ENO model. These are the core network, the SIM card and the platform.

WEBSITE

ENO core network:

Pod Group has its own network core including its own mobile codes that are not tied to any one market (901 MCC). This enables Pod to establish direct roaming agreements and to operate cross border services using a single SIM and a single price for data connectivity. In addition, Pod has its own mobile core to provide autonomy from mobile operators and a private LTE mobile core, for enterprise customers requiring autonomy and security whether they are utilizing public or private spectrum. Pod's partnership with Expeto, a provider of disruptive cloud and edge IoT Connectivity technology, enables Pod to offer seamless integration of industrial-grade public and private LTE/5G networks to its customers' enterprise IT networks, giving them the agility, speed and security to launch IoT applications globally as extensions of their existing networks. For the enterprise, this can all be managed via a centralized platform in a Network as a Service (NaaS) model, giving enterprises network visibility, control and the additional, ENO-exclusive benefit of seamless public and private networking.

ENO SIM card:

ENO SIMs use eUICC as standard. This can store multiple SIM profiles in the same chip. Other eUICC solutions only offer one standard SIM profile for each roaming partner. Pod Group features an operational Priority Roaming SIM Profile (with Multi-IMSI capabilities) plus a failsafe multi-network SIM profile. In addition, innovation in the development of SIM applets such as Zero Touch Provisioning or SIM2Cloud Encryption has converted the SIM card into an active element in the device, meaning that computing resources can be freed up and manufacturing costs reduced. Other SIM applet examples developed by Pod Group include a data monitor embedded on the SIM card. This app will swap network carriers on poor signal strength or when local data outages happen.

ENO Platform:

The key to the ENO offering is the provision of managed services via one centralized platform, giving the enterprise full visibility and control over its IoT network, whether public, private or a combination of the two, without the need to employ a team of network specialists in-house. Pod Group's IoT Suite is a modular platform, allowing enterprises to manage global IoT connectivity, security and billing from one interface. However, if the enterprise simply needs to use one element of the platform the modular nature of the portal makes this possible. For example, they may want to use only the hierarchical billing and subscription management module, and bring their own connectivity agreements. This agnostic platform, combined with Pod's consultancy services, including Pod Verify device testing, 24/7 technical support and access to Pod's wider ecosystem of hardware, software and Systems Integrator partners for the deployment of private networks gives enterprises the long term support they need to deploy and scale customized IoT solutions.

TAOGLAS®

WEBSITE

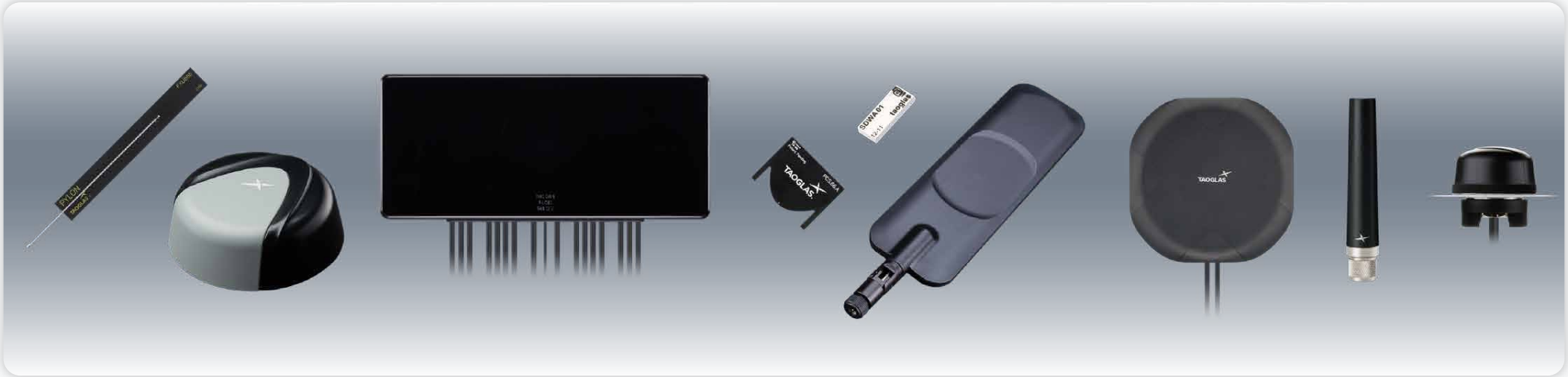
Private Cellular: Top Considerations for Organizations and Their Device OEMs

Smart cities, manufacturers, utility companies and other organizations have no shortage of wireless options for connecting their Internet of Things (IoT) sensors, streetlights, employee smartphones, autonomous industrial robots and other devices. But navigating all of those options and choosing the right one can be daunting.

Take cellular. With few exceptions — particularly utility companies – most organizations traditionally got cellular service from a public operator. But over the past few years, the U.S. and other countries have steadily changed their regulations to allow businesses to own and operate private mobile networks.

This means their data doesn't compete with other customers for network bandwidth, which is particularly valuable for mission-critical and latency-sensitive applications. For instance, with private 4G or 5G, businesses have the end-to-end control necessary to provide deterministic latency for applications that need it, such as time-sensitive networking (TSN) for Industry 4.0 manufacturing. Ownership also gives them total control over data privacy and greater protection against malware because network access is limited to their devices.

Owning and operating a network is a major investment, but it also can be cheaper than paying a mobile operator for service. These savings can be significant even when the organization doesn't have a lot of bandwidth-intensive applications. For example, the 3GPP 5G standards include a set of features and capabilities known as Massive Machine-Type Communications (mMTC), which enable 5G networks to support up to 1 million devices per square kilometer. So



WEBSITE

even if a private network supports only a fraction of that amount — such as 10,000 low-bandwidth IoT sensors and controllers — the monthly data volume can quickly add up to terabytes. With a public network, that could add up to a bill so large that many of those applications might become cost-prohibitive, undermining that organization's digital transformation.

Some organizations recognize the benefits of owning a network because they already do. Examples include utility CDMA networks at 450 MHz, and the Terrestrial Trunked Radio (TETRA) networks owned by first responder agencies and railroads. But those legacy technologies are approaching the end of their useful lives, which is why many of those organizations are upgrading to 4G or 5G. For example, many utilities are replacing their CDMA 450 networks with LTE 450.

Wi-Fi arguably is the most common private network technology. Virtually every type and size of organization has a wireless LAN. However, Wi-Fi isn't designed to support large-scale deployments such as a smart city spanning 500 square miles or a 1,500-acre oil refinery. Devices also can lose their connection when they're being handed off between Wi-Fi access points. This problem is rare with 4G and 5G because they were designed from the ground up to provide seamless connectivity for mobile devices over large geographic areas.

To serve the burgeoning private 4G/5G network market, device vendors and systems designers should focus on solutions that can support a wide variety of bands. This flexibility enables them to develop products that can be sold to a wide variety of organizations in a wide variety of countries. Many private network applications involve IoT, where compact size and low cost are two more key considerations for device vendors and systems designers. This is also important considerations for IoT device manufacturers when identifying which bands to support. The devices should be optimized from an RF and antenna perspective to support a variety of bands.

One example is the Taoglas PCS.66.A, which is ideal for embedded applications where low cost is a top customer requirement. It supports 600 MHz to 6 GHz, with high efficiency (up to 80%) to enable maximum throughput for any 4G and 5G application.

The Taoglas TGX.45 is a 2×2 MIMO dipole antenna designed to provide reliable service even in harsh outdoor installations. Featuring support for all sub-6 GHz 4G and 5G bands — including Band 31 (450 MHz) and Band 71 (617 MHz) — the cross-polarized antennas' layout also enhances performance capabilities, thus improving signal quality and maximizing throughput.

Another solid choice is the Taoglas Apex IV TG.46.8113, a wideband 5G/4G dipole antenna that covers all sub-6 GHz bands, including 450 MHz. Ideal for routers and terminals, it has the highest wideband efficiency of any terminal antenna on the market today and is optimized for the 5G NR C-bands between 3.3 GHz and 4.2 GHz.

Private cellular also is an example of how one choice leads to several more, starting with whether to use licensed or unlicensed spectrum. Cellular bands traditionally were the exclusive domain of mobile operators, but that's steadily changing in many countries. For example, Germany set aside parts of 5G bands for private networks, including 3.7-3.8 GHz, in October 2019. Just one year later, 82 organizations had been awarded spectrum licenses. (https://omdia.tech.informa.com/OM014642/In-Europe-we-will-see-a-growing-trend-toward-allocating-spectrum-to-private-networks)

One benefit of choosing licensed spectrum is that public networks use it, too. As a result, private operators benefit from the mass market's economies of scale and equipment selection. Another benefit is greater protection against interference because those frequencies aren't shared with other operators — public or private.

Another consideration applies to both licensed and unlicensed spectrum: frequency range. Depending on the country, this decision is made partly by regulators. For example, many European utilities traditionally used the 450 MHz band because it has lower capex: Signals

WEBSITE

travel farther at low frequencies, so fewer base stations are required.

Utility applications frequently are low bandwidth, such as automated meter reading and outage sensors. That's another reason why low bands such as 450 MHz are a good fit: The lower the frequency, the less data it can support. Higher spectrum is a better fit for organizations with bandwidth-intensive applications, such as HD or 4K video for surveillance and machine vision for autonomous material handlers. The tradeoff is higher capex because the private network will need a higher density of base stations. Higher frequencies also have more difficulty penetrating physical obstructions such as walls. Lower spectrum, such as traditional cellular bands at 850 MHz and 1900 MHz, requires fewer base stations and provides better in-building penetration, with the tradeoff of lower data rates.

Many private operators are choosing a middle ground: the 6 GHz band, which starts at 5.9 GHz and runs to 6.4 GHz or 7.1 GHz, depending on the country. It's high enough to support bandwidth-intensive applications but without the capex and opex of a high-density network in, say, millimeter wave (mmWave) spectrum.

"The 6 GHz range is a mid-band frequency and sits at a balancing point between coverage and capacity, providing the perfect environment for citywide 5G connectivity," the GSMA says.

Another key benefit is the amount of spectrum available at 6 GHz. In the U.S., for example, 1200 MHz is available for unlicensed 5G use. "The 2023 World Radiocommunication Conference (WRC-23) will play a decisive role in determining future access to the upper 6 GHz range (6425-7125 MHz)," the GSMA says. "Balanced decisions on the use of this range can allow license-exempt technologies, when needed, to make use of the lower part of the band where required while reserving the upper portion at 6425-7125 MHz for licensed 5G."

Taoglas has released and upgraded many of its existing products to support the newly established bandwidth between 6 and 7.125 GHz. Taoglas offers various mounting options including embedded SMD, embedded flex PCB, and terminal mount antennas. For applications requiring external permanent mount antennas, its 11-in1 Synergy MA1511 is perfect for MIMO requirements and where single, small form factors are required, its WS.03 or TU.60 are ideal. Taoglas' Guardian X MA9917, with up to 17-in-1 combinations has also been designed to cover the increased bandwidth and to cater for the multi network routers we see entering the market today. It comes in a slim panel design and is available with adhesive or wall mounting options.

For embedded applications, the super small Taoglas Pylon, FXUB85 is Taoglas' widest bandwidth embedded adhesive flex antenna covering 600MHz to 8GHz with incredible efficiency. The Venti FXP52X series offer embedded MIMO options for the increased spectrum and our SDWA.01 ceramic SMD antenna offers a high efficiency, high peak gain solution for device PCBs.

In order to help you with your antenna selection and device design, Taoglas offers a number of Design and Test Services. Whether to augment our existing off-the-shelf antennas or to work with you for a complete custom RF and antenna design and/or testing project, Taoglas' global engineering teams utilize their expertise on thousands of successful IoT projects. Taoglas can help you with pre-certification testing and get you to market fast and cost-effectively.

WEBSITE

THALES

Private Networks, Mobile Communication Services

Because eSIMs/SIMs hold private network and cellular data security credentials as well as connectivity subscriptions, they combine access and connectivity service continuity with the optimum user experience. Thales' connectivity services get the most out the eSIM/SIM fleet to guarantee the best user experience with the optimum level of security.

1 CONNECTIVITY ENABLEMENT AND MANAGEMENT

Instant Connect

Simplify Private Network eSIM/SIM on-boarding.

For the initial connectivity on-boarding, connect your Private Network users with an out-of-the box experience bootstrap connectivity service, without any need for initial connectivity capability such as Wi-Fi/Bluetooth or a preloaded mobile subscription.

ORDER CONNECT USE

THALES INSTANT CONNECT

Private Connect

Bring service continuity to your Private Network users across Private and Public Network.

For employees or things who need extended connectivity, combine public network coverage to private network's coverage with automatic switching (and still a priority to Private) without having to use specific or multiple devices or impacting the user experience with manual operations.

Evolutive Connect

Adapt your Private Network over regulation, technology and business conditions.

Depending on the evolution of the Private Network (standard, coverage), the mobility of the devices and users, you can adapt, add or delete remotely your initial subscription within the eSIM.

2 SECURE YOUR DIGITAL ASSETS AND DATA

Long Term Key Update

Get a future-proof and adaptive cyber protection.

Strengthen your cyber protection updating dynamically all over subscription life cycle eSIM/SIM credentials and algorithm upon Private Network request, at no renewal extra-cost or consequences for your users.

IoT Safe

Protect your sensitive data when your connected devices exchange with "the rest f the world".

From Private Network to cloud infrastructures ensure that data are sent to the right server, kept confidential and not altered with mutual authentication between the device and its cloud. Get a security by design with a touchless, out of the box, provisioning process.

3 TAYLOR AND ORDER YOUR PRIVATE NETWORK SIM/eSIM

On-line Ordering Platform

As a Private Network leader benefit from all eSIM/SIM use cases.

SELECT
eSIM/SIM capabilities:
☑ Credentials and parameters,
☑ Applets (IoT safe, multi IMSI)

ORDER
exact eSIM/SIM quantities you need.

CONNECT
people or devices instantaneously.

https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/enterprise-private-network

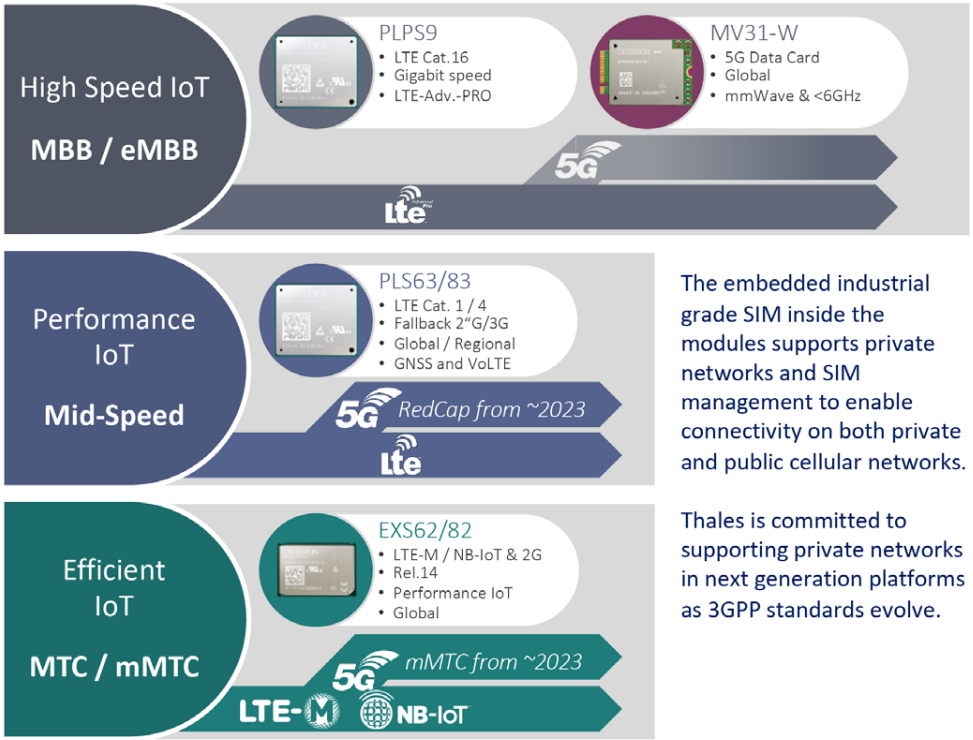
THALES

WEBSITE

Private Networks, Internet of Things

Thales's broad portfolio of Cinterion® IoT Modules, Gateways and Modem Cards enable always-on cellular communications for virtually any IoT or M2M application. Their rugged design, outstanding engineering and manufacturing standards make them ultra-reliable in the most extreme environments and over the long life of an M2M solution.IoT technology is built for long lasting solutions where devices require product, network, and security updates during their lifetime. The Cinterion IoT Suite provides services that help to manage the long lifecycle of IoT solutions and remotely update, control, secure, and manage devices and subscriptions.

Cinterion Private Network Devices

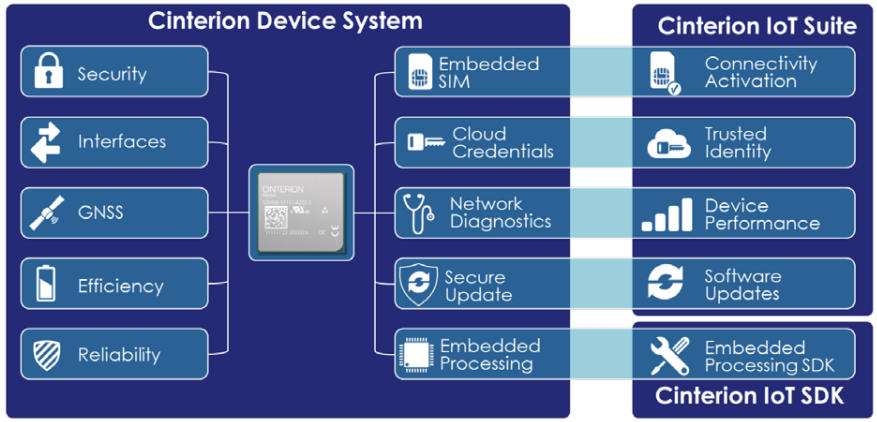


The embedded industrial grade SIM inside the modules supports private networks and SIM management to enable connectivity on both private and public cellular networks.

Thales is committed to supporting private networks in next generation platforms as 3GPP standards evolve.

Cinterion IoT Suite

The Thales IoT Suite simplifies the provisioning of connectivity profiles to the eSIM/SIM, reduces the need for on premise infrastructure to onboard devices, and facilitates the hand-over between private and public networks.
Thales Cinterion IoT Modules securely store diversified digital IDs and encryption keys in state-of-the-art hardware security containers. This ensures secure authentication in the private network to guarantee data confidentiality and integrity through encryption-based mechanisms. The IoT Suite supports large-scale, secure credential management for the lifecycle of connected devices on the private network.
The IoT Suite provides device management, software update and diagnostic services to ensure that devices remain reliably connected, secure and up to date throughout their lifecycles.



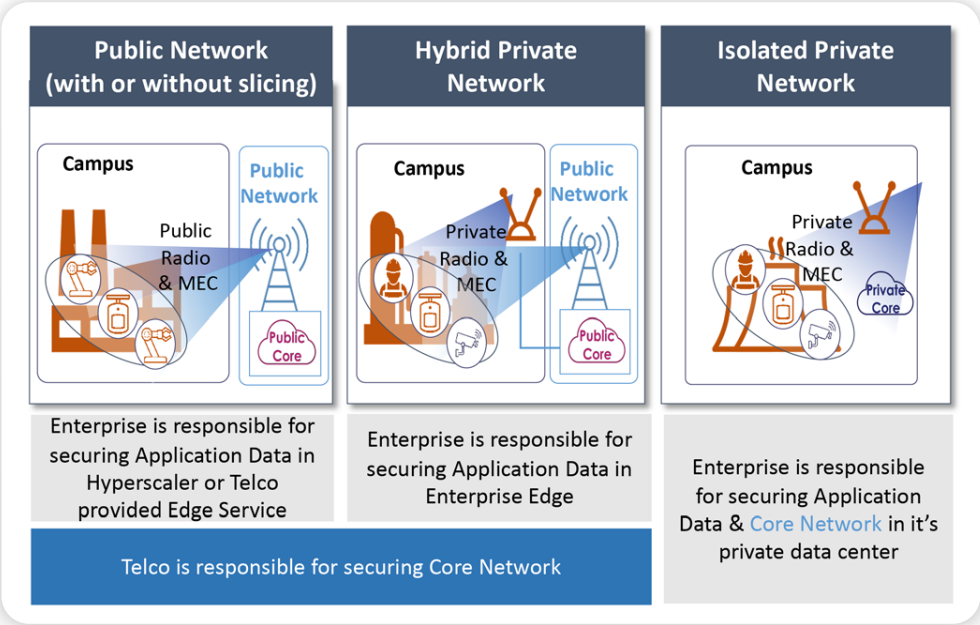
THALES

WEBSITE

Private Network Cyber Security Solutions

Shared Responsibility for Data Security between Enterprise & Telco

As enterprises continue to evaluate and adopt mobile private networks, there is growing awareness around the need for securing data and the infrastructure from cyber-attacks. Data Sovereignty and Privacy regulations are the other key drivers. Multiple options are available to enterprises for deployment of private networks with varying degrees of convenience and control on the deployment of core network, radio and edge computing assets. This results in the responsibility for securing sensitive data in the edge computing infra and core network to vary significantly as shown in the Figure opposite.



Thales Solutions for edge to core

Thales provides solutions to secure data & infra at the edge, mobile core network and xhaul. These solutions range from software-based Encryption and Key Management Solution (KMS) to hardware- based FIPS 140-2 level 3 certified HSM and High-Speed Encryptors (HSE). Telcos or Enterprises can leverage these solutions to address their security requirements.

Telcos Providing Secure Network As A Service

One of the critical operations performed by the Mobile Core is authenticating cellular subscribers/devices giving access to the mobile network. As enterprises leverage Mobile Private Networks, restricting connectivity to only their users/devices with utmost security becomes important. In addition, 5G has introduced SUPI/SUCI mechanism to protect subscriber's privacy. To prevent attacks/network compromise, the cryptographic parameters for these mechanisms should be stored and generated securely. Thales Luna HSMs support 3G/4G/5G Authentication Vector generation and high-performance ECIES algorithms for SUPI/SUCI mechanism.

Furthermore, as the mobile core manages sensitive data like subscribers/devices info, network usage info etc., enterprises look for assurance that access to these assets is restricted only to authorized personnel. Thales CipherTrust Data Security Platform (CDSP) & HSMs as RoT for PKI infra can help Telcos achieve this.

Enterprises Deploying Mobile Private Networks

As indicated in the diagram, the enterprise is always responsible for securing application data, irrespective of whether it's on a public cloud edge service (AWS Wavelength) or on-prem. For public cloud, BYOK (Bring Your Own Key) and higher security BYOE (Bring Your Own Encryption) solutions are available to help enterprises secure their data as per the cloud shared responsibility model. Moreover, for on-prem, depending on the level of security needed various options are available to secure data at the application layer or transparently at file/DB layer or at the storage layer. CipherTrust Data Security Platform (CDSP) reduces operational complexity by supporting multi-cloud & hybrid deployments.

In addition, enterprises deploying isolated core network can leverage CDSP to secure sensitive data like subscribers/devices information, network usage information etc. in the control-plane. Enterprises can also use HSMs to securely process 4G/5G network authentication requests, SUPI/SUCI crypto processing along with securing PKI-based infra elements like kubernetes, service mesh, certificate life-cycle managers etc. can be employed to prevent breaches.

THALES

WEBSITE

Private NetworkProject integration

Thales is a leader in designing, deploying and managing highly resilient and secured communications and infrastructure systems for critical governmental organizations and critical sites. The company has a long track record in projects for Defense, Security as well as for organizations that run critical infrastructures.

From Specialised Private Networks to Unified 4G/5G Private Networks

Previous generation of private networks consist in a collection of different siloed specialized eventually complemented by innovative technologies to offer services to the different end-user of an organization. For example, critical tasks related to safety and to operational coordination of personnel usually relied on narrow-band PMR (Private Mobile Radio) specialized systems like TETRA. Although those PMR technologies provide the required level of security and resilience, they are limited to basic services such as voice (private or PTT group calls) or text messages. To access to broadband services, alternative solutions based on Wi-Fi for campus coverage or based on complementary data cellular access for nationwide service is sometimes used. But these alternative solutions do not have the required level of resilience and security by mission and business critical operation. They also require an additional network to deploy and/or terminals to manage which increases complexity in deploying and managing the services and increases the costs.
Private 4G/5G network augmented with their mission critical services (aka MCS) is the way to unify all services over a single infrastructure, simplifying the solutions for private network owners and enhancing the services offered to their end-users in their daily tasks and during crisis. With this approach, organizations and their end-users benefit from a large and fully standard ecosystem that evolves gradually other each standard version bring new features and capabilities?
Besides, private 4G/5G networks pave the way to additional flexibility in the business model from 100% owned solution to hybrid models where the radio access can be provided by a commercial operator.

The Challenge to Deliver a Unified 4G/5G Private Network That Can Be Trusted

Private 4G/5G network is the way for mission and business critical organizations to improve the efficiency of the safety of their operations. However, whatever the deployment model, there are a number of challenges when it comes to deploy and operate an end-to-end solution that matches with the mission and business critical grade requirements. Indeed, such a critical system must be: Available anytime and anywhere in the service area; Be cyber-protected against the malicious attacks (4G/5G private network have a surface of attacks that is wider than legacy PMR systems) and provide higher level of privacy;

Simple to use and adapted to the specific jobs for the end-users; Easy to manage and supervise for an operator including the agility to provision and control the access of users to the system. And, although most of the component of the solution are based on standard, realizing a private network that works with such objective is not just a matter of plugging the pieces together. And, this is where Thales comes into paly!

Thales, The Trusted Partner To Build Mission Critical Private Network

Thales focuses on delivering and operating mission critical systems. For private 4G/5G network, Thales works with best-of-breed partners that provide building blocks of the private network in line with the deployment model (100% owned or hybrid). These building block include the COTS terminals, radio base station (if required), virtual core network and Managed Connectivity Services (MCS) software. Then, in line with the customer requirements, Thales designs based on the building block a system that can comply with the highest level of services availability (better than 99.999%), hardens the security of the system to certifiable level (360° security from the terminal, to the E2E communication to the network, including SOC if required), customize the MCS services to the end-user jobs, design and deliver the operation and maintenance system adapted to the missions, and can eventually operate the system and transfer it to the customer after a phase of transition.

Beecham Research is a leading technology market research, analysis and consulting firm established in 1991. We have specialized in the development of the rapidly-growing Connected Devices market, often referred to as M2M and IoT, worldwide since 2001. We are internationally recognised as thought leaders in this market and have deep knowledge of the market dynamics at every level in the value chain.

Our clients include component and hardware vendors, major network/connectivity suppliers, system integrators, application developers, distributors and enterprise users in both B2B and B2C markets. We are experts in M2M/IoT services and platforms and also in IoT solution security, where we have extensive technical knowledge.

info@beechamresearch.com

beechamresearch.com

@beechamresearch

facebook.com/BeechamResearch

linkedin.com/company/beecham-research

beecham research

Shaping the IoT future