Deloitte.

Case Study:

Building a private 5G network to support smart warehouse applications

April 2022

Introduction

Background

Forward-leaning organizations are exploring how 5G and edge computing technologies can impact their business. A 2021 Deloitte study spanning the Americas, Europe, and Asia Pacific showed 76% of the more than 400 surveyed enterprise executives believe 5G will become the most critical network technology within the next three years.[1] Similarly, an NTT study of roughly 200 senior leaders across Germany, Japan, the United Kingdom, and the United States found that 90% expect private 5G to become the standard network of choice in their industry within five years, with 80% planning to deploy private 5G networks within the next 24 months.

Such research reveals optimism across almost all verticals and geographies regarding the potential productivity gains private 5G and edge computing can drive for enterprises. Fiber-like speed and capacity combined with distributed compute and storage can enable low-latency applications to automate manual processes and drive cost efficiencies in ways not feasible with wired networks or previous generations of wireless technology.

The desire to stay at the forefront of technology evolution motivated a tech-savvy manufacturing company to ask how 5G and edge computing might improve productivity in its warehouse operations. Fortuitously, Deloitte was already pursuing a 5G opportunity for a public sector client with a similar objective. The collision of these two events presented a unique opportunity for Deloitte and the manufacturing company to collaborate in building a private 5G network. The duo would use the network to learn and experiment with cutting-edge applications while providing a proof of concept for the government client.

The collaboration focused on applications that could directly benefit from the speed and reliability of a private 5G network, including autonomous mobile robots and precision asset tracking. It also presented the opportunity to explore leading cybersecurity practices and yielded lessons regarding private network architecture and implementation for future projects.

Experimentation, implementation, and operational improvements

Deloitte and the manufacturing company teamed to determine high-value, smart applications for a 45,000-square-foot warehouse. Deloitte's role was to architect and deploy the network and identify and implement applications that could benefit from 5G—specifically, 5G's ability to support real-time communications, device density, and machine-to-machine communications with ultra-reliable, low-latency connectivity. After exploring many options, Deloitte and the manufacturing company narrowed their focus on using the 5G network to experiment with:

- A precision location tracking system
- Fully autonomous mobile robots (forklifts) with onboard decision-making capabilities
- A high-definition computer vision and environmental sensor system
- AR/VR visual screens (tablets)

The 5G and edge compute network provided the warehouse operator with a flexible and reliable platform to support each identified use case. While too early to quantify specific operational improvements, the warehouse operator has already observed anecdotal productivity benefits. For example, the integrated 5G-enabled sensor and asset tracking systems provide perpetually accurate inventory and real-time location data on hundreds of thousands of items, no matter where they are in the warehouse, improving pick accuracy and reducing human error and cycle times for inventory audits.

The benefits of a 5G cellular network have become apparent to the warehouse operators as they deploy an increasing number of autonomous mobile robots (AMRs). Previous networks struggled to accommodate more than 20 AMRs given the amount of data passed between the robots and the applications and between the robots themselves to communicate their location to each other. 5G networks enable more AMRs to move pallets safely and autonomously from receiving to their designated locations, allowing operators to focus on higher-value activities instead of spending time traversing the massive warehouse.

Weighted bins connected to the warehouse management system (WMS) allow for perpetual inventory counts using predictable weight attributes and the ability to generate automated discrepancy reports. Furthermore, the coverage achieved through a relatively low number of 5G antennas and radios has provided greater flexibility in the use and placement of high-definition cameras and environmental sensors improving the effectiveness of security access (facial recognition/biometrics) and quality control (light, temperature, humidity) systems.

Network elements: Overview, challenges, and lessons

Deloitte engaged eight different external organizations, each contributing their best-of-breed components and capabilities in delivering a complete network solution to support identified applications. As Deloitte architected the wireless network and integrated the solutions of its selected collaborators, several technological and operational challenges emerged. Specifically, the team encountered challenges around the following:

Network design:
Interoperability between vendors in an open radio access network (RAN) environment

User equipment (UE):
UE availability in certain spectrum bands

Spectrum selection:
Utilization of licensed and unlicensed spectrum

Backhaul:
Capacity to support 5G requirements

Cybersecurity:
Cybersecurity enhancements in a wireless environment

RAN intelligent controller (RIC):
Availability of an open RIC and RIC-based xApps

Network operations:
Ongoing network operations considerations

The paragraphs on the following pages describe these challenges and share lessons for future implementations.

Network design

The network design leveraged an open and virtualized radio access network (vRAN) running on commercially available servers demonstrating Open RAN. The radio access equipment is LTE and 5G enabled.

For this specific implementation, Deloitte utilized a third-party software vendor's Enhanced Packet Core (EPC) to interact with a JMA Wireless virtualized RAN, called XRAN. Four discrete radio units (RUs) were connected via fiber jumpers to a virtualized baseband unit running on a standard server. The RAN configuration was Multiple-Input Multiple-Output (MIMO), with each RU supporting two physical antennas. This configuration allows for future scaling of coverage and capacity with the easy addition of RUs as needed. The virtualized baseband unit, 4G/5G core network, and edge computing platform were all housed in one central powered, cooled rack unit, including the XRAN, UPS, EPC, and distribution switch, and provided a minimal form factor adapted for the industrial warehouse environment.

Figure 1. A single rack houses the virtualized baseband unit (CU/DU), the 4G/5G core, edge computing platform supporting smart warehouse applications, a distribution switch, and UPS. The rest of the infrastructure, including backhaul, used the warehouse operator's existing IP network.

While technology often captures the most attention, it is important not to forget about the network's physical construction, such as how and where to place and power the remote antennas and radio units and the need for construction oversight to ensure vendors install networks to specifications. Initially, the team designed the antennas to be located on the warehouse walls. However, because floor-to-ceiling shelving against the walls made access difficult, the installation vendor placed the antennas on the ceiling. The RUs are conveniently located next to the server rack unit. This design change highlights the need for construction oversight on the radio frequency (RF) design and the IT component location to make sure networks are built to specifications and function properly in the physical environment where they are deployed.

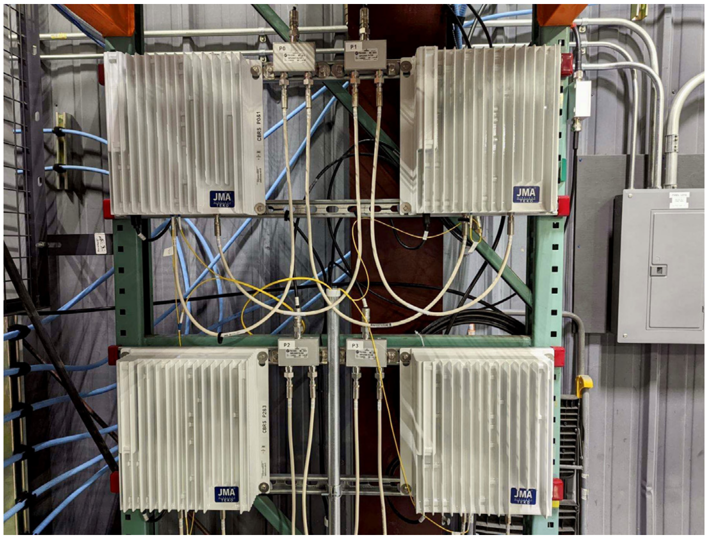
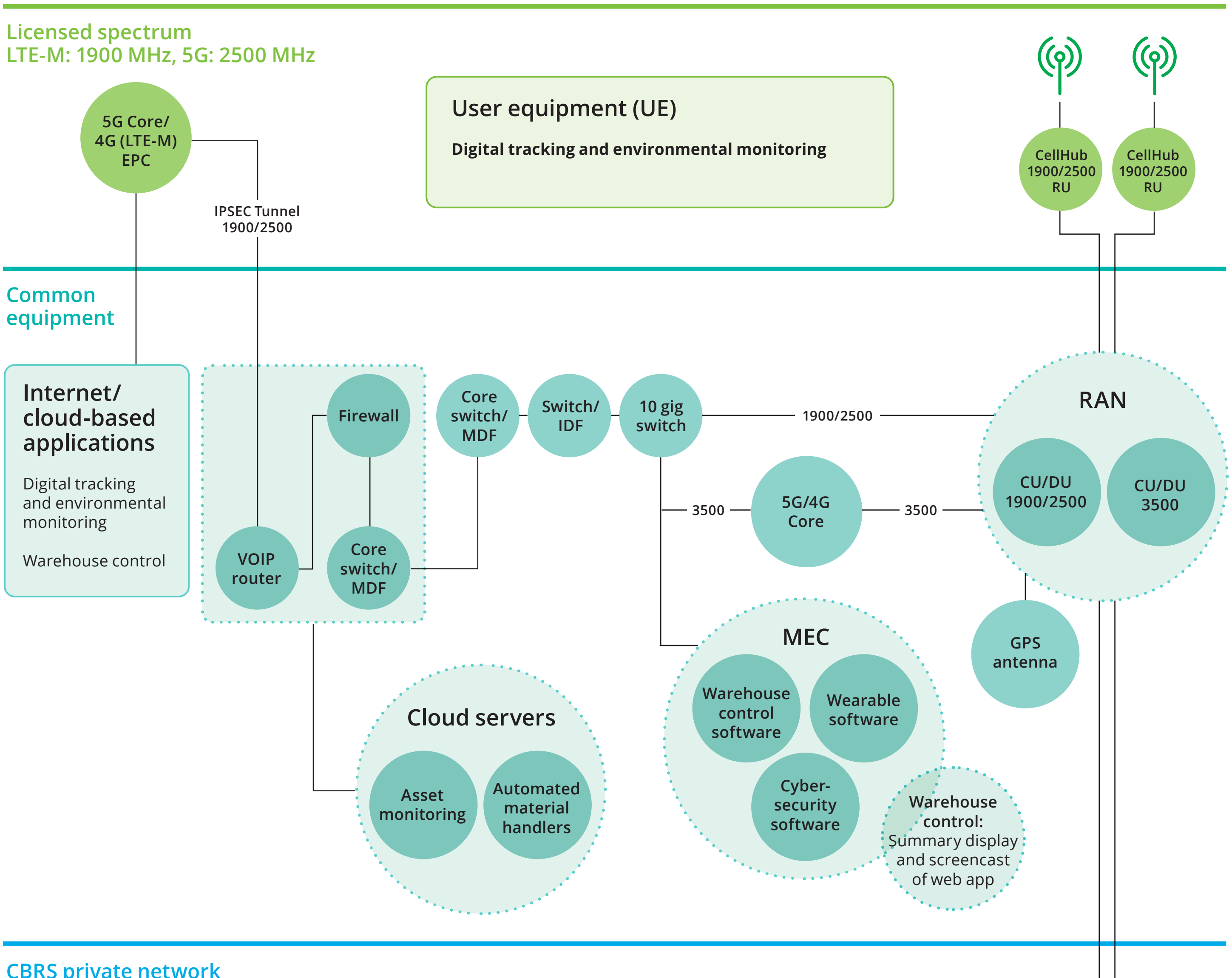


Figure 2. Radio unit (RU) placement in close proximity to the server rack allows easy access for troubleshooting and installation. The upgrade of these RUs to new 5G enhancements and improvements is accomplished via software upgrade—no need for HW component replacement.

Network design lessons:

- Vendor diversity and innovation require strong integration and program management capabilities to keep all the moving pieces in step. Access to a strong systems integrator with a rich set of trusted associates who can combine best-of-breed products, services, and capabilities is vital.
- Persistent supply chain issues highlight the value of open architectures that provide greater flexibility in selecting potential vendors. In this case, the team could easily swap in an alternative edge compute server when they found the original choice was unavailable.

Figure 3. Smart warehouse network architecture



User equipment (UE)

Asset monitoring: Camera - bullet (x2), Camera - dome (x2), LTE dongle (x4)

Automated material handlers: Autonomous pallet robot (x2), Autonomous forklift (x1), LTE dongle (x3)

Warehouse control: Tablet (x2), Weighted bins with controller (x2 bins, x1 controller), LTE dongle (x1)

Wearables: Tablet (x1), Augmented reality glasses (x1), Ring scanner (x1), Wi-Fi modem (x1)

User equipment (UE)

A primary obstacle encountered by the team in deploying smart warehouse applications on a private 5G network related to the immaturity of the 5G ecosystem, specifically the availability of 5G-native user equipment (UE) that can work across all available spectrum bands. Fortunately, this is an issue that should naturally resolve with time.

Due to the lack of available user equipment, the project team needed to develop workarounds to get existing user equipment to work on the network. Specifically, the team retrofitted existing devices and sensors associated with different applications (e.g., security cameras, autonomous mobile robots, and autonomous forklifts) with dongles that converted USB to 5G wireless connections to get them to work on the network. While this strategy was successful, it also introduced new points of potential failure that took time to troubleshoot. For example, some applications worked when using the UE's embedded Wi-Fi (an ethernet connection) but only worked intermittently when switched over to the cellular network.

User equipment lessons:

- Lack of 5G-native user equipment impedes application deployments on private 5G networks. However, the ease of implementation should improve as 5G-native user equipment becomes more readily available.
- As we await 5G ecosystem maturity, much of the available user equipment (sensors, tags, etc.) supporting various enterprise applications will require workarounds to operate on 5G networks.
- The dongle solution described above will not be necessary as OEMs produce more 5G-native UE. Deloitte expects that 5G-native UE for these use cases will be more widely available starting in the second half of 2022.

Spectrum selection

Many factors influence the choice of spectrum utilized by the network. Once again, the availability of user equipment that can operate on a specific spectrum type (i.e., unlicensed CBRS spectrum or licensed spectrum) and spectrum band (i.e., low-band, mid-band, and mmWave) can influence spectrum selection. Moreover, use case requirements may further narrow spectrum selection. For example, the need to limit interference or enhance security may dictate the use of licensed versus unlicensed spectrum.

In this case, the team initially contemplated using only unlicensed CBRS spectrum. However, target project timelines coupled with the timing for available UE prompted the team to build a network capable of utilizing both CBRS unlicensed spectrum and licensed carrier spectrum. Licensed spectrum procured from a wireless carrier was required to support UE associated with an asset tracking solution. Specifically, the team was challenged to get the digital tags used by the asset tracking solution to work on the network. These tags operated on a specialized narrowband LTE technology called CAT-M, requiring licensed mid-band spectrum. The team could not retrofit these tags to work on the unlicensed CBRS 3500 network, and a Wi-Fi-based workaround did not allow the tags to triangulate location accurately. With experimentation and learning as part of their mandate, the project team decided to see if it could engage a carrier to provide the licensed mid-band spectrum needed to solve this problem.

Procuring licensed spectrum from a carrier presented an unusual challenge. Making licensed spectrum available to serve third-party networks is an emerging yet still uncommon business practice for many carriers. While carriers understand the opportunity that private networks provide in monetizing their spectrum and driving more traffic (IoT and MM2M devices) onto their networks, this is still in its early stage. Nevertheless, a national carrier provided Deloitte the opportunity to procure its licensed spectrum and put it into immediate operation toward enabling innovative applications on the private network. This was key to standing up the 5G network and opening access to a broader set of use cases.

Spectrum selection lessons:

- Deploying on multiple spectrum bands may be necessary to support certain use cases. In this case, the team required both unlicensed and licensed spectrum and tri-band radios with 5G and backward LTE compatibility to accommodate legacy network elements and available user equipment. An upfront assessment of UE connectivity requirements can help inform network configuration and spectrum selection.
- When using licensed spectrum, allow time to negotiate retransmission agreements with the carrier to ensure all parties adhere to the FCC's license requirements.

Backhaul

5G networks are capable of data rates up to 20 Gbps. To realize the full potential of a 5G network, however, all elements in the network should be capable of handling these higher speeds. For this reason, weak links in the legacy infrastructure can become bottlenecks and require an upgrade.

The project team found that the warehouse's existing internet cable connection was the most cost-efficient backhaul option to the wireless carrier's core network. However, since this internet connection was shared across an organization, and its performance could vary with demand, the team upgraded the internet cable from 100 Mbps to 1 Gbps to reduce potential congestion. But even as it upgraded the internet connection, it discovered that a VoIP router that sat outside of the firewall was choking speeds down to 100 Mbps and needed replacement.

Backhaul lessons:

- When designing private networks, it is crucial to examine and plan the link budget of the network when taken as a whole, not simply the RAN or within the four walls of the facility being served. The entire chain is only as strong as its weakest link, which in some instances may be equipment or links not directly associated with the private network.
- Leveraging existing infrastructure may require material modifications to LAN network elements such as intermediate distribution frames and main distribution frames.
- It is important to understand the importance of day-to-day operational connectivity over facilities that may be shared to help ensure no disruption to critical applications as a result of placing new traffic on a shared network element.

Cybersecurity

While the adoption of wireless networks (either LTE or 5G) can offer many benefits, it can also create new security concerns and challenges relative to traditional wired LAN and may require organizations to reassess their security management programs.

Deloitte implemented a zero trust architecture (ZTA) in accordance with an emerging leading practice. ZTA assumes networks are already compromised and thus focuses on continuous logging and monitoring to lock down further intrusion. Accordingly, the network continually authenticates everyone and everything—users, servers, and machines—across all communication channels.

The team deployed several additional fail-safes to account for the wireless versus wired nature of the network. For example, given the use of radio waves, the team put in stronger FIPS 104-2 (104-3) encryption across all communications and a SIM failover mechanism that would keep the network operational in case of a signal-jamming event. Given the mobile nature of many end devices, the team also limited SIM usage to specific hardware using mobile equipment identifiers (MEIDs) and IP addresses to prevent transporting their use to other devices.

An overall concern was balancing security with the mission and operational needs for high network performance. For example, continuous authentication and other security measures can add data overhead, slow networks, and undermine the speed, reliability, and latency benefits of a 5G private network. The team deployed a hybrid on-premise MEC/offsite cloud system in response. The system processes non-critical operations in the cloud while retaining critical time-sensitive operations on the on-premise MEC. The virtual nature of the network also allows for over-the-air configuration management to monitor, balance, and maintain baseline operations and security.

Cybersecurity lessons:

- Adding wireless to enterprise networks introduces new security concerns and challenges relative to traditional wired LAN and may require organizations to reassess their security management programs.
- Private networks create an opportunity to deploy zero trust architectures that continually monitor networks and authenticate users to detect and mitigate unauthorized intrusion.
- Hybrid cloud/MEC systems—where some vendor applications reside in the cloud while others stay on-premise on the MEC—can help balance security with network performance requirements, but they also expand the network's security boundary.

RAN intelligent controller (RIC)

The RIC helps control and optimize RAN operations and supports applications and use cases that need to interact with the RAN, like location tracking, mobility management, network slicing, authentication, and interference management. Applications that require access to the RIC are collectively referred to as xApps. Additional development work is needed for radio manufacturers to be able to interface with the RIC. RIC interface involves radio manufacturers making their APIs available to outside developers who can then write new xApps, like those mentioned above, to interact with the RAN directly. In the spirit of experimentation and learning, the team trialed both solutions. Experimentation with xApps gave the team confidence that an open RIC will become a significant differentiator for 5G networks in the next 24 months.

RIC lessons:

- OEMs that decide to interface with a RAN Intelligent Controller will accelerate application and ecosystem development. This involves developing and making their APIs available to third-party developers who can then write new applications that can interact with the RAN (xApps).
- Interfacing with a RIC will involve significant development work to create standard protocols (APIs). Until then, getting applications to work on the networks will entail workarounds.

Network operations

Private networks will require ongoing resources to run and manage the network. Network operations can be run in-house by an organization that owns the network or by external vendors. However, except for the largest organizations, many enterprises will likely outsource network management to a carrier or another third-party provider.

Managing wireless networks requires a different knowledge base than that held by traditional enterprise networking executives. Most in-house IT teams are inexperienced with wireless networking, and getting up to speed may require significant training and hands-on experience.

Another concern is that licensed carrier spectrum comes with FCC mandates and other legal and regulatory requirements like 911 compatibility, testing, uptime, and carrier visibility. It is unclear if these obligations will extend to organizations running private networks on licensed carrier spectrum. As a result, we expect a market for managed services to develop to manage, monitor, and maintain private wireless networks for these and other reasons.

Whoever manages the network should be strategically aligned with the network mission. For example, many private 5G networks will be built to support time-sensitive, mission-critical applications. Ensuring high-level network performance will require operational rigor (i.e., knowledgeable personnel, real-time monitoring capabilities, break/fix maintenance with onsite spare inventories, etc.).

Finally, the team found it helpful to have dedicated onsite resources from installation to onboarding the first use cases. Having someone on the ground when adding new devices or applications to the network was also helpful.

Network operations lessons:

- For networks built for nonproduction, testing, or proof-of-concept purposes, it is important to note that the use of public spectrum owned by carriers may include operational requirements to which the network must adhere. Examples are 911 capabilities, testing, uptime, and carrier visibility, in addition to FCC or other legal and regulatory mandates. Therefore, the operational plan should factor in the level of effort associated with adhering to these requirements daily.
- The degree of operational rigor should align with the strategic imperatives of the network. For example, suppose the network will support mission-critical applications. In that case, a high degree of operational rigor may be necessary (i.e., real-time monitoring, spares onsite, available break/fix personnel, etc.) to support high performance levels. On the other hand, an experimental network may not justify the costs associated with maintaining a high degree of operational support.

Conclusion

While many vendors in the network ecosystem have been touting the benefits of 5G private networks for several years, actual implementation experience is still in the early stages. Deloitte acquired significant insights through its involvement in delivering a complete end-to-end 5G edge computing solution—from building the underlying 5G network to enabling the user equipment and applications that allow enterprises to achieve desired business outcomes.

Each 5G deployment will depend on the customer's requirements, the portfolio of use cases it will support, what spectrum bands are available, and other factors. There's no one-size-fits-all approach, and each implementation will differ. In this case, the team involved many different players to implement a given use case and deliver an end-to-end solution. Having access to a rich set of trusted collaborators who can provide industry-leading products, services, and capabilities for different parts of the solution is vital. Strong integration and program management capabilities are required to keep all the moving pieces in step.

Authors and acknowledgments

Brad Hunt
Senior Manager, Telecommunications Lead, Infrastructure & Capital Projects
Deloitte Transactions and Business Analytics LLP
bradhunt@deloitte.com

Christine Bennett
Manager, 5G and Advanced Connectivity Leader
Deloitte Consulting LLP
cbennett@deloitte.com

The authors would like to thank Chris Bates, Jack Fritz, Dan Littmann, and Naima Hoque Essing for their contributions to this article.

Endnotes

1. Jack Fritz et al., "Accelerating enterprise innovation and transformation with 5G and Wi-Fi 6," Deloitte Insights, March 22, 2021.

Deloitte.