WHITE PAPER

INTEGRATING ERICSSON PRIVATE 5G TO UWM CONNECTED SYSTEMS INSTITUTE CPWE NETWORK

Use-Case Example of Private 5G Integration in Industrial Automation

By Asif Al Zubayer Swapnil
Research and Technology Coordinator, UWM Connected Systems Institute
PhD Candidate, UWM College of Engineering and Applied Science

uscellular BUSINESS

UNIVERSITY of WISCONSIN UWMILWAUKEE | CSI CONNECTED SYSTEMS INSTITUTE

Executive Summary

This white paper offers a detailed overview of a recent project at the University of Wisconsin Milwaukee (UWM) Connected Systems Institute (CSI), centering on the integration of private 5G systems within a connected manufacturing environment. A joint venture between UScellular®, Ericsson, Rockwell Automation and the CSI team, this effort aimed to connect the CSI Advanced Manufacturing Testbed to the Converged Plantwide Ethernet (CPwE) network using Ericsson private 5G system. A significant milestone in deploying private 5G in Industry 4.0 scenarios, this document also introduces the current state of wireless technologies in industrial environments, addressing the viability of private cellular as an option to provide coverage, security, mobility, and reliability for wireless connectivity in industrial automation.

As manufacturers continue to mature in their digital transformation journey, the evolving environment has pushed the limits of conventional Operational Technology (OT) and Information Technology (IT) solutions. Private 5G provides manufacturers a secure wireless communication channel with the necessary coverage, security, mobility, and reliability - which are essential to meeting the demands of today's information and communication processing.

The project's scope involved a preliminary technical test of private 5G network infrastructure in an Industry 4.0 context. The phases covered the evaluation of the Ericsson private 5G system, its adaptation and design changes for CPwE network integration, implementation of these changes and thorough connectivity and operational testing. This process included initial assessments and necessary custom modifications to meet the CPwE network's specific needs, representing a true Industry 4.0 environment. This white paper documents these evaluations and the modifications made, providing insights into the technical process.

Initially, UScellular provided the Ericsson private 5G system, configured for standard enterprise network connectivity. Utilizing cloud-connected management and configuration services, this setup enabled a quick and efficient deployment. Yet, the concept of network zones within the CPwE network demanded further configurations, allowing the Ericsson private 5G system to serve both Enterprise and Industrial Zones through distinct 5G network segments. Supported by Ericsson, UScellular and Rockwell Automation, necessary adjustments were identified and implemented, resulting in the successful transfer of all automation and IoT services to the 5G network. This white paper details the design decisions emerging throughout the project.

However, the project faced challenges, notably in ensuring device compatibility with the state-of-the-art 5G NR Standalone network. To overcome this, UScellular provided compatible mobile gateway devices from Cradlepoint, an Ericsson subsidiary. Another major challenge was the Routing Behind Mobile Station (RBMS) feature, essential for network reachability. An implementation issue of 5G NR radio features in the Qualcomm modem chip's reference firmware hindered the use of RBMS functionality with most mobile gateway devices available during the project and required a workaround solution to be devised. The solution involved disabling RBMS and utilizing a Generic Routing Encapsulation (GRE) tunnel for data routing. The white paper delves into some technical details of these workarounds.

In conclusion, the project's successful completion offers invaluable insights into the complexities of deploying private 5G networks in industrial settings, highly relevant to industries considering 5G adoption. This initiative has broadened the understanding of private 5G applications and established a solid test environment at CSI and UWM Campus. It sets the stage for further research and optimization of private 5G networks for industrial use. Additionally, this white paper presents recommendations, highlights the future scope of projects and emphasizes the potential for collaboration with UWM CSI for anyone interested in adopting private 5G systems for industrial operations and automation.

Background

Industrial networking has evolved significantly from its rudimentary beginnings, when it relied heavily on relay and switch-based systems. The advent of Programmable Logic Controllers (PLCs) marked a shift towards more sophisticated data transfer and communication protocols. Early networking methods, including radio frequency (RF) technology, faced limitations such as security vulnerabilities. The development of RS232 and Modbus protocols in the mid-20th century introduced more advanced serialized data transmission and broader communication capabilities. The emergence of Ethernet in the 1980s further revolutionized industrial networking, offering higher data transmission rates and the ability to connect a larger number of nodes.

Converged Plantwide Ethernet (CPwE)

Developed collaboratively by Rockwell Automation and Cisco [1], CPwE represents an innovative approach to integrating industrial and traditional office networks. It facilitates the strategic convergence of Operational Technology (OT) and Information Technology (IT), essential for industrial environments. CPwE architecture, grounded in standard Ethernet technologies, incorporates industrial enhancements to satisfy stringent industrial requirements.

Key to CPwE is the segmentation of the OT network and the Enterprise IT network into distinct zones. The Enterprise IT network zone resembles a traditional office network, handling standard IT services, internet connectivity and data management. In contrast, the Industrial Zone (IZ) encompasses the plant floor network, managing machine control, supervisory automation and industrial IoT networks. IZ is the section of network where industrial automation requirements such as real-time communication and safety critical protocols are deployed. IZ holds many legacy OT devices, which, while typically simpler and lower-powered, may become vulnerable if directly exposed to the internet.

To safeguard the IZ, it is isolated from both the internet and the Enterprise IT network, ensuring no direct data flow between these areas. This isolation is crucial for protecting sensitive OT systems from potential cyber threats.

A pivotal component of CPwE is the Industrial Demilitarized Zone (IDMZ)[2], serving as a buffer zone between the OT and IT networks. IDMZ is integral to network security, mediating communications between these zones and adding an extra layer of security. Implementing IDMZ involves using gateways and replication of data and services from servers within the IZ. These tools act as intermediaries, allowing necessary data exchange while maintaining the segregation and security of the respective networks.

In the context of CPwE's architecture, its scalability, real-time communication, determinism and manageability are not just technical features; they are essential components that bridge the operational gap between the industrial and IT worlds. By distinctly segregating yet seamlessly connecting the OT network (IZ) and the Enterprise IT network, CPwE enables a harmonious flow of data and control. This unique balance ensures that while the IZ remains protected and isolated, it does not sacrifice the efficiency and responsiveness needed in dynamic industrial environments. CPwE's ability to support a diverse range of industrial protocols while maintaining stringent security measures exemplifies a forward-thinking approach to industrial networking. This empowers industries to not only safeguard their operations but also embrace technological advances for improved productivity, agility and innovation in a rapidly evolving digital landscape.

Photo courtesy University of Wisconsin-Milwaukee

Private Cellular Networks

Private Cellular Networks, especially 5G, are rapidly evolving to meet the demands of industrial communication. While they are not the pinnacle of industrial communications yet, their potential to adapt to these needs is significant[3]. Currently, these networks are in the nascent stages of being incorporated into industrial settings, reflecting the gradual alignment of 5G capabilities with the specific requirements of industrial environments[4].

Private 5G networks offer dedicated, reliable, secure connectivity. However, they are not inherently tailored for industrial applications but do hold the potential to be customized for such environments. This adaptability is particularly crucial considering the diverse nature of industrial communication needs. The potential of private 5G networks in industrial settings is substantial, though it is more about the promise they show rather than a guaranteed revolution in industrial systems communication.

One of the ideal use cases for private 5G is in supporting the Industrial Internet of Things (IIoT) and smart manufacturing[4]. The high availability and reliability of private 5G[5] make it a suitable candidate for these applications, particularly in scenarios of dynamic industrial environments where these are combined with the inherent mobility benefits of the private cellular networks. Examples include advanced predictive maintenance, autonomous mobile robots (AMRs) and real-time monitoring using Augmented Reality and Digital Twins[4], where private 5G can significantly enhance operational efficiency and safety.

However, the integration of private 5G into industrial settings presents several challenges. The uncertainty surrounding which industrial applications can effectively be supported by private 5G necessitates extensive testing and exploration of use cases. Issues such as device readiness, spectrum access, necessary skill sets within enterprises, and the development of a viable business case highlight the complexity of adopting private 5G in manufacturing and other industrial operations. These challenges underscore the current state of private 5G as an emerging technology still being tested and evaluated for its full range of applications in industrial settings. Significant progress has been made across the industry in overcoming many of these challenges. With the introduction of CBRS spectrum in the US devices are catching up with native 5G NR support over CBRS along with alternatives that can bridge non-cellular native devices over to cellular. These advancements, coupled with the development of necessary skill sets within enterprises and the formulation of viable business cases, signify the evolving landscape of private 5G adoption in manufacturing and other industrial operations.

Within this evolving landscape, the enhanced mobility, speed and security offered by private 5G networks make them a compelling proposition for the future of industrial automation. This section sets the stage for a deeper exploration of CPwE and Private Cellular Networks, highlighting their respective stages of adoption and maturity. While they are at different points in their development, both technologies are integral in shaping the future of industrial networking. The subsequent sections will delve into the technical aspects and applications of CPwE and Private Cellular Networks, underscoring their role in advancing the next generation of industrial automation. This narrative transition aims to bridge the understanding between the established framework of CPwE and the emerging potential of Private Cellular Networks.

Problem Description

The evolution of industrial automation, key to the advancement of industrial operations, is increasingly leaning toward wireless networking solutions, despite the proven efficacy of wired networks. This shift is driven by the unique benefits that wireless networks offer in the context of modern industrial environments. Unlike wired networks, wireless solutions provide unparalleled flexibility and mobility, essential in rapidly changing industrial layouts and processes. When needing or wanting to change operations on a manufacturing floor, cables can limit the opportunity for flexibility. Wireless solutions enable easier and more cost-effective scalability, allowing the integration of a growing number of devices and sensors while reducing the need for extensive physical cabling. This contributes to meeting sustainability goals by minimizing material usage and energy consumption. Additionally, modern wireless networks facilitate live data transmission and monitoring, which are critical for the efficiency and responsiveness of automated systems. However, this transition also introduces new challenges.

The limitations of traditional wireless networks, in terms of bandwidth, reliability and security, are becoming apparent. This is where advanced technologies like private 5G come into play, offering the potential to overcome these hurdles with improved connectivity and robust security measures while providing the flexibility benefits of wireless. Our preceding discussions on Converged Plantwide Ethernet (CPwE) and Private Cellular Networks have set the stage for understanding this transition, highlighting the evolving networking needs in industrial automation and the role of emerging technologies in meeting these demands. For instance, certain applications, like motion control and safety operations, require ultra-low latency to ensure immediate responsiveness. On the other hand, there are scenarios where high bandwidth is more crucial, such as in real-time monitoring, image processing and in recent time AI-driven operations. The bandwidth limitations of traditional wireless networks often fall short in these demanding situations, especially in environments rife with interference. This insufficiency is further complicated by the need for reliability metrics such as bounded latency, tolerance to packet loss and precise time synchronization. For example, specific control services in industrial automation may require bounded latency as low as a few milliseconds, with zero tolerance for packet loss[4], a standard that conventional wireless solutions struggle to meet.

Wireless Networking Challenges in Industrial Automation

In the realm of industrial automation, traditional wireless technologies such as Wi-Fi, Bluetooth, with advanced standards like Wi-Fi 6E or BLE, along with proprietary RF protocols, are most common. Yet, these technologies often struggle to meet the stringent requirements of industrial environments. Their shortcomings become particularly apparent when considering the high-density device deployment, the necessity for consistent and reliable connectivity and the harsh conditions typical of industrial settings.

These technologies face a fundamental limitation: the trade-off between latency and bandwidth. In industrial automation, where precise, split-second decisions are critical, latency is a vital concern. High jitter, often resulting from interference or network congestion, can significantly compromise the performance of these technologies, leading to inconsistent and unreliable network behavior. This issue becomes even more complex when considering the diverse demands across various industrial applications.

For instance, certain applications, like motion control and safety operations, require ultra-low latency to ensure immediate responsiveness. On the other hand, there are scenarios where high bandwidth is more crucial, such as in real-time monitoring, image processing

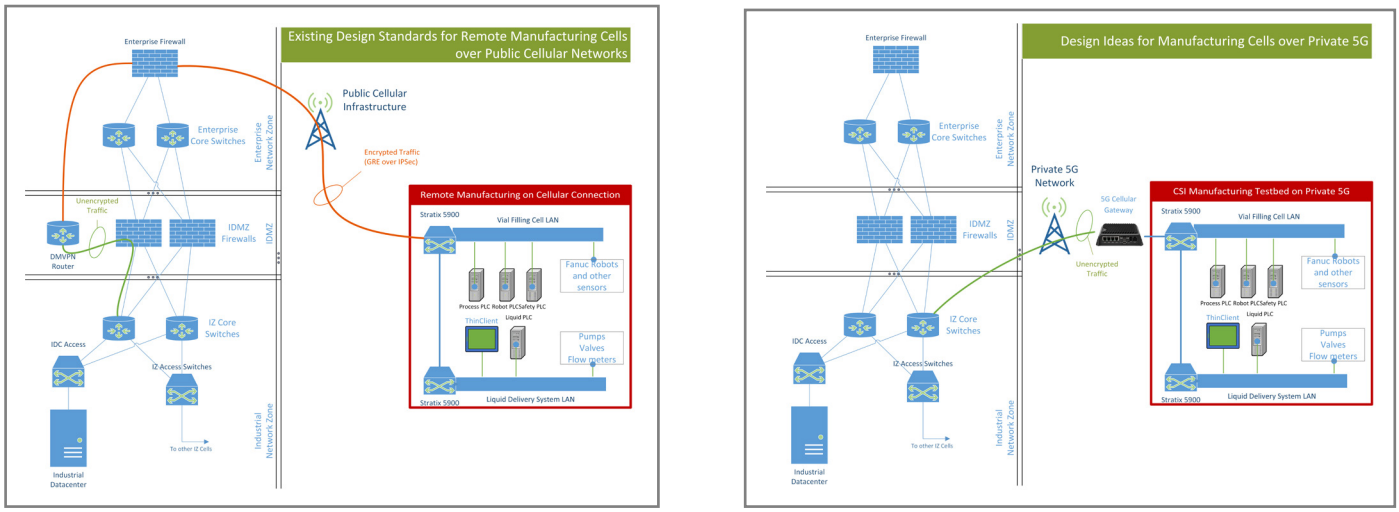

Figure 1: CPwE guidelines provide options for using Public Cellular networks for remote site connectivity to the IZ, but with Private Cellular network, new simplified designs are possible.

and in recent time AI-driven operations. The bandwidth limitations of traditional wireless networks often fall short in these demanding situations, especially in environments rife with interference. This insufficiency is further complicated by the need for reliability metrics such as bounded latency, tolerance to packet loss and precise time synchronization. For example, specific control services in industrial automation may require bounded latency as low as a few milliseconds, with zero tolerance for packet loss[4], a standard that conventional wireless solutions struggle to meet.

The Imperative for Practical Implementation Trials of Private 5G

The introduction of private 5G networks offers a promising solution to the challenges faced in industrial automation, particularly addressing the limitations of traditional wireless technologies like Wi-Fi and Bluetooth. These technologies, while essential in current industrial setups, often struggle with issues such as network interference, congestion and the stringent demands in dynamic industrial environments. The availability of the Citizens Broadband Radio Service (CBRS) spectrum for private 5G networks[6] presents an opportunity to develop a robust alternative to wireless technologies currently deployed in the Industrial, Scientific and Medical (ISM) bands.

Private 5G networks are adept at balancing high bandwidth and low latency requirements, essential for diverse industrial applications. 5G's advanced Quality of Service (QoS) mechanisms, as per the latest 3GPP standards, allow for precise control over traffic prioritization and network performance. This control is achieved through dynamic QoS management, enabling packet-level traffic differentiation and efficient handling of network congestion and interference. Unlike Wi-Fi, where latency varies with interference and congestion, private 5G networks employ controlled bandwidth allocation using Time Division Duplex (TDD) and Frequency Division Duplex (FDD) methods, to ensure consistent and reliable network performance.

However, the true test of private 5G's capabilities lies in its practical implementation within industrial settings. Deploying private 5G networks in real-world industrial operations environment is crucial for evaluating their effectiveness in addressing traditional wireless network problems. This involves overcoming complexities related to integrating these networks with existing industrial systems and ensuring reliable support for a diverse range of communication requirements in modern factories.

A significant challenge in this practical implementation is ensuring compatibility with existing industrial equipment and protocols. Industrial systems often operate on specific communication standards and integrating private 5G networks requires careful alignment with these technical requirements to ensure smooth and seamless integration.

Moreover, the deployment and management of private 5G in an industrial context demands a different level of technical expertise. This includes not only an understanding of 5G technology, but also deep knowledge of the operational and security aspects specific to the industrial environment. Ensuring robust security in private 5G networks is especially critical, given the risks of cyber threats in industrial settings. The nature of private 5G networks, being inherently private, allows for integration into technologies like CPwE. While public cellular networks were discussed as a solution for remote connectivity with CPwE architecture, the requirement for encrypted tunnels are necessary (Figure 1) and new simplified design principles can be developed.

In the upcoming sections, this white paper will examine practical strategies for integrating private 5G in industrial automation, using a real-world implementation project as a case study. This approach will showcase how to navigate challenges and maximize the benefits of private 5G, enhancing connectivity, efficiency and safety in industrial settings.

Solution

In addressing the complexities of integrating private 5G into industrial automation, the University of Wisconsin-Milwaukee's Connected Systems Institute (UWM CSI) embarked on a pioneering project. This endeavor, a real-world application of private 5G in an industrial setting, serves as a tangible testament to the practical benefits and challenges of such an integration. Leveraging the CPwE architecture, UWM CSI's initiative underscores the crucial role of collaborative, hands-on projects in bridging theoretical knowledge

with practical application. This section delves into the specifics of the private 5G implementation at UWM CSI, highlighting the synergistic roles of key partners – Rockwell Automation, UScellular and Ericsson – in navigating and aligning the complexities of this cutting-edge technological fusion.

0UWM CSI's Implementation of Private 5G with Rockwell Automation and UScellular®

The University of Wisconsin-Milwaukee Connected Systems Institute (CSI) exemplifies collaboration between industry professionals and academics, driving forward the integration of advanced digital technologies in manufacturing. CSI's focus extends beyond its state-of-the-art facilities to fostering a synergy of knowledge and expertise in the field of Industry 4.0.

In a project to integrate private 5G into the CPwE network, CSI collaborated with Rockwell Automation and UScellular. Rockwell Automation as a founding member of UWM CSI played a crucial role in setting up the CPwE network, ensuring seamless communication and enhanced efficiency in industrial operations. Meanwhile, UScellular was instrumental in introducing private 5G into the industrial operations environment, deploying the Ericsson private 5G network. This network wasn't just a connectivity solution; it was a transformative factor within the testbed, bringing high-speed, low-latency wireless networking solution for industrial automation .

The project's primary goal was to provide a practical demonstration of private 5G's capabilities in managing and operating factory lines with both traditional and modern industry needs. The project revolved around three main components: the CSI advanced manufacturing testbed, the CSI industrial datacenter and the Ericsson private 5G solution.

The CSI advanced manufacturing testbed is a state-of-the-art advanced industrial operations testbed that simulates a fully integrated and automated manufacturing line. The testbed consists of industrial robots, intelligent conveyor systems, control and automation systems and liquid and process control equipment.

In the CSI industrial datacenter, virtualized services are hosted across three different network security zones—Enterprise, IDMZ and Industrial Zone—adhering to CPwE principles. The PlantPAx supervisory control running the Liquid Delivery System in the CSI Advanced Manufacturing Testbed is situated in the Industrial Zone, while the PLEX MES system controlling the production ordering and supervision of the Vial Filling Cell in the Testbed is in the IDMZ. An FactoryTalk Edge Gateway instance in the Industrial Zone interfaces with the testbed controllers (PLCs), passing through a firewall zone to connect to the internet and stream data to Azure IoT Hub. All three of these systems use EtherNet/IP protocol to communicate directly to the Allen-Bradley ControlLogix PLCs in the testbed and collect tag data. PlantPAx and Edge Gateway uses FactoryTalk Linx, PLEX MES system uses Kepware KepserverEX with Allen-Bradley suit.

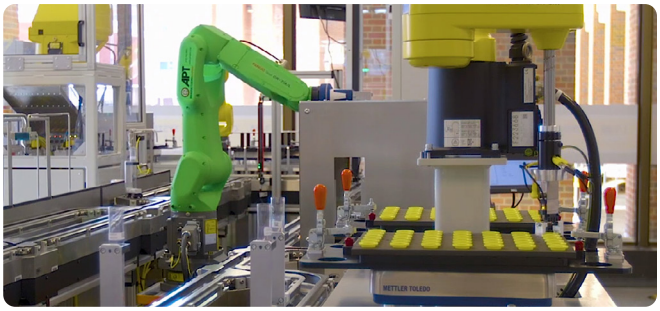

Photo courtesy University of Wisconsin-Milwaukee

The Ericsson private 5G system features a RAN operating on 5G NR SA over CBRS spectrum, and an integrated 5G core with a pair of network controllers. The network controllers connect to Ericsson's cloud-based Network Management Portal (NMP) over a secure tunnel over the internet, while having separate network interface to connect to on-site/enterprise network. The system supports multiple 5G network segments on the radio network and can route them to different VLANs on the enterprise network interface. The segment-to-VLAN mapping allows diverse devices on the 5G network to connect to the industrial and enterprise zones in the datacenter maintaining segmentation of network traffic.

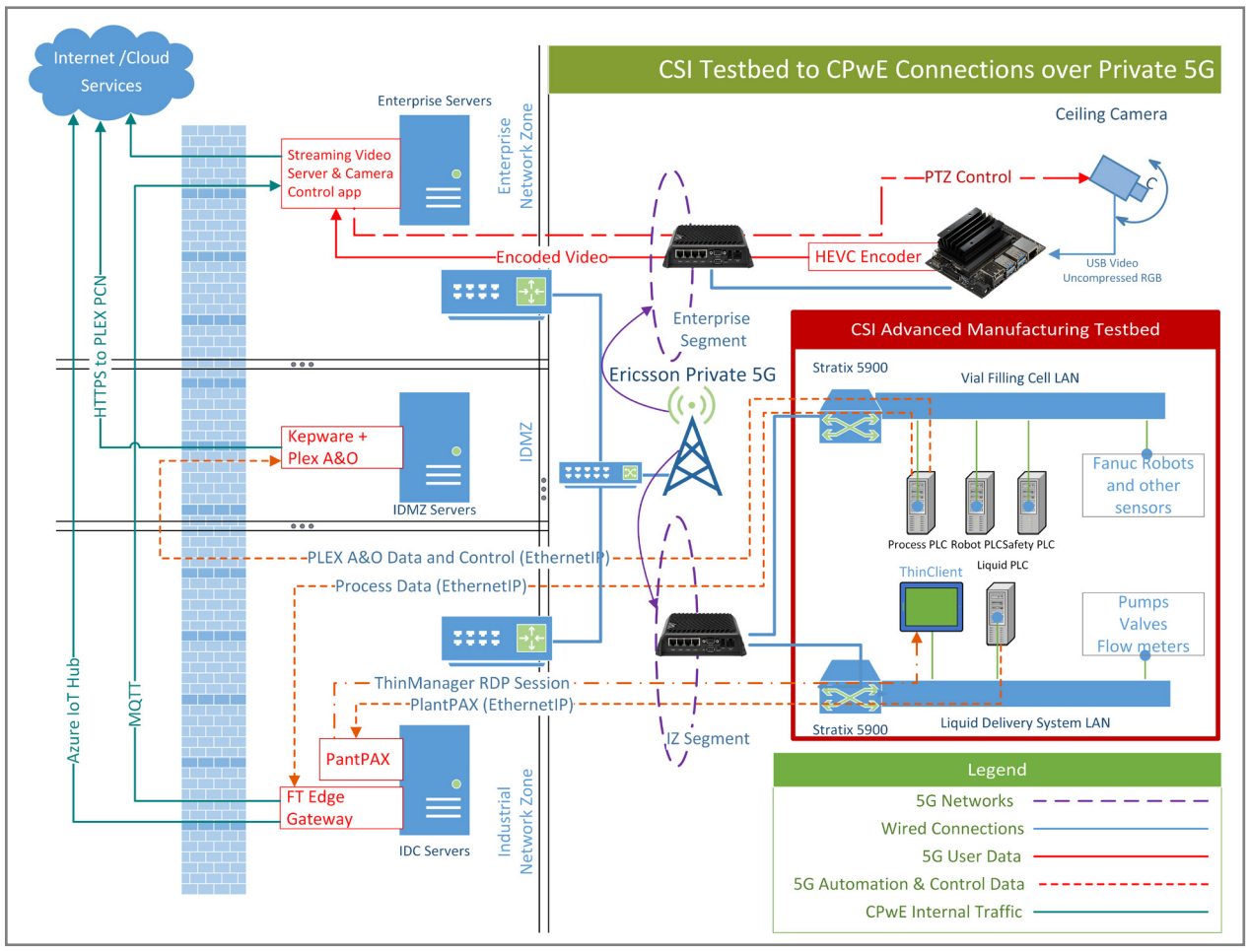

Figure 2: Project outcome of integrating EP5G system to CSI CPwE network.

The project's primary objective was to demonstrate the practical application of private 5G in managing and operating factory lines, catering to modern industry needs. This involved testing various applications like supervisory control and video streaming over the 5G network. A significant innovation included using IoT data to control camera movements based on supervisory control inputs, showcasing private 5G's potential in enhancing automated monitoring systems.

Specific tests conducted to verify the functionality and performance of the private 5G system included:

- Supervisory Control Test: Testing if the supervisory control using EtherNet/IP protocol, PlantPAx distributed supervisory control system running on virtualized servers in the Industrial Zone, and the PLEX MES System's cloud connectivity through the IDMZ , continues seamlessly as it did on Wired Ethernet connections.
- Video Streaming Test: Assessing whether the camera can stream High-Definition video 24/7 using High Efficiency Video Coding (HEVC), also known as H.265 compression, without quality loss or impacting other applications.
- IoT Camera Control Test: Evaluating an application where supervisory control data from the Edge Gateway is sent to a python application using the MQTT protocol, controlling the camera's movement and tracking different operations of the production run using its Pan-Tilt-Zoom feature.

This project serves as a landmark case study, demonstrating the implementation of private 5G in industrial automation, highlighting its critical role in transforming connectivity, efficiency and safety in smart manufacturing environments. The integration of these systems underlines how private 5G can bridge the gap between conventional industrial setups and advanced digital infrastructures, proving itself as a robust wireless solution.

Details of the Implementation Project

The following narrative outlines the strategic integration of private 5G into the established CPwE framework at UWM CSI, detailing the synergistic convergence of existing network components and new 5G technology.

Architecture of UWM CSI's CPwE Network: The CPwE network at UWM CSI, engineered by Rockwell Automation, integrates a comprehensive IDMZ alongside an Industrial Datacenter (IDC) featuring a virtualized environment. This setup supports on-premises services essential for industrial operations. The network architecture includes dual Fortinet Firewalls, segmenting the system into Enterprise, IZ and IDMZ zones. In the Enterprise zone, two Cisco Catalyst 9300 switches are stacked, forming a combined core-access configuration. Conversely, the IZ hosts a pair of stacked Catalyst 9500 switches, responsible for routing Layer 3 (L3) traffic. Additionally, stacked pairs of Catalyst 9300 switches are deployed as Layer 2 (L2) access switches within the plant. These switches facilitate both wired and Wi-Fi networks and connect the IDC and IDMZ servers. Figure 3 illustrates various services operational within the IDC, the enterprise network and on the plant floor, all while maintaining clear zone separations.

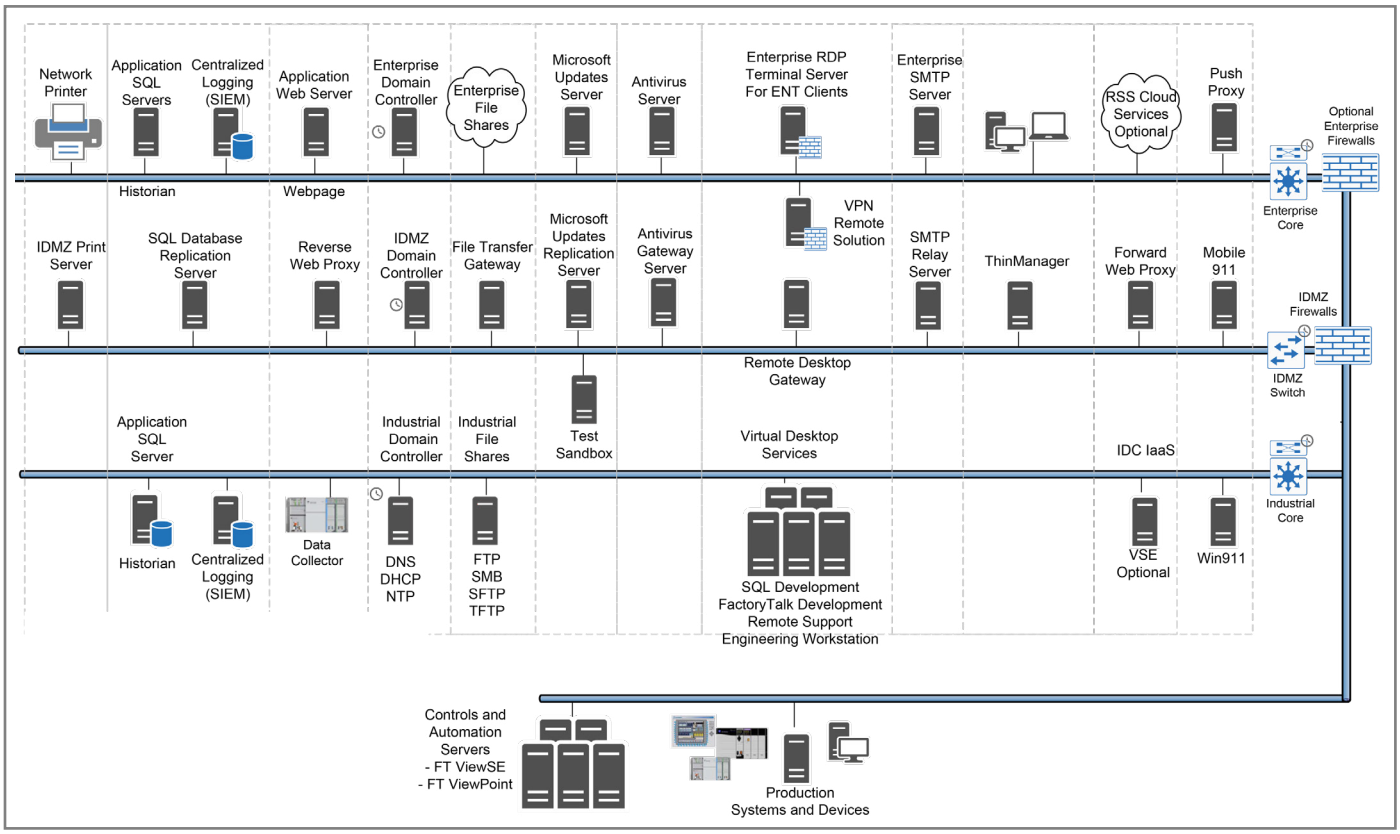

Figure 3: Example deployment of different CPwE services in different Zones at CSI network.

It is pertinent to note that, although CPwE guidelines have been followed as closely as possible in the CSI's industrial network design, a few deviations from the guidelines have been necessary to meet application demands arising from the modern need for cloud-connected IIoT systems and dashboards. Notable deviations appearing in this white paper include the use of direct cloud connectivity to Azure IoT Hub from applications running in the IZ segment, as well as the convergence of physical Wi-Fi infrastructure for Enterprise and IZ networks while maintaining separation in network traffic. These deviations were developed with help from CSI's industry partners, such as Fortinet and Heartland Business Systems, who play major roles in industrial network deployment and cybersecurity. Some of these modifications are validated using Fortinet's Enhanced Purdue Model[7], utilizing a Next Generation Firewall (NGFW) with Next Generation Intrusion Prevention (NGIPS) and deep packet inspection (DPI) capabilities for industrial protocols.

Components of the Ericsson Private 5G System: The private 5G system, supplied by UScellular and sourced from Ericsson for the project, is referred to as the Ericsson private 5G system. This compact system comprises a few key components that can either be accommodated in a standalone small rack or integrated seamlessly into existing enterprise datacenter racks, occupying a minimal space of just 5 rack units. The Ericsson private 5G system comprises a Baseband and a Radio Dot System. The Radio Dot System comprises one or more Indoor Radio Units (IRUs)[8] situated at the central location, along with multiple Radio Dots[9] spread across the facility. These Radio Dots connect to the IRU using CAT6A twisted pair cables and RJ45 connectors. However, these cables do not carry Ethernet signals; instead, they transmit direct radio signals, benefiting from shielded twisted pair conductors. The Radio Dots function as radio antennas, power amplifiers, and frequency band filters, while the IRUs control and supply power to the Radio Dots, connecting them to the baseband. Additionally, the Ericsson private 5G system features two network controllers configured in an active-passive setup, ensuring high availability. These controllers run the 5G Core and manage connections to the cloud-based management portal. Furthermore, they facilitate the link from the 5G Core to the customer network for on-premises data handling. The design, inspired by the Control and User Plane Separation (CUPS) concept, ensures efficient routing of customer data. Data from the radio network devices is directed to the on-prem network, distinct from the management portal data. This latter data is encrypted and sent to Ericsson's secure, cloud-based Network Management Portal (NMP).

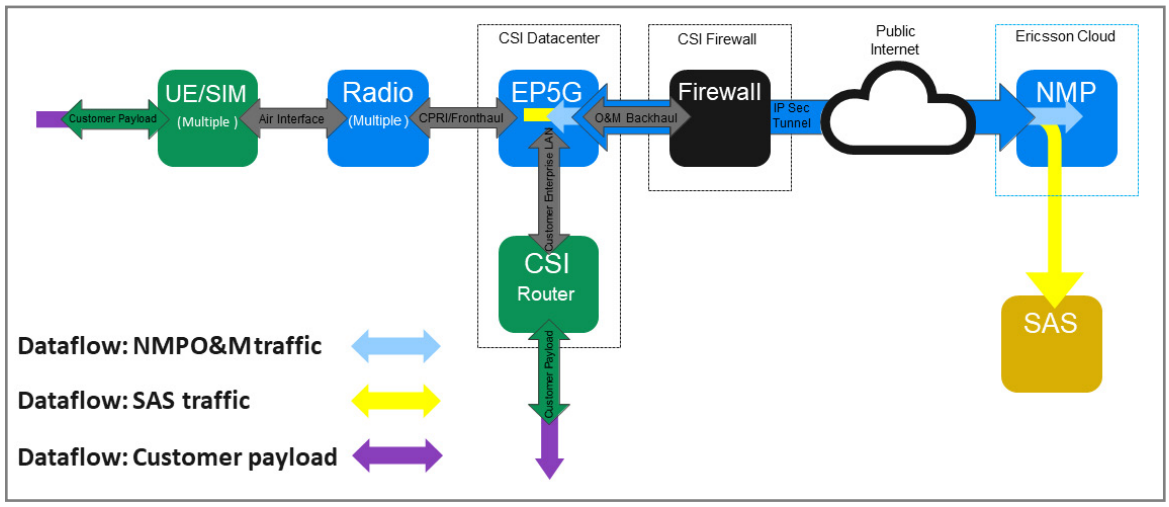

Figure 4: Management and user dataflow of EP5G system at CSI.

Installation and Configuration of the Ericsson Private 5G Infrastructure: The deployment and setup of the Ericsson private 5G system are directly managed by the UScellular team, with expert help from Ericsson. The package, comprising the Baseband, Indoor Radio Unit (IRU) and Network Controllers, is delivered ready for installation. In scenarios where re-racking isn't necessary, the system can be operational simply by connecting it to power and providing internet access for the Network Management Portal (NMP). Ericsson professionals also assist in the strategic installation of radio dots across the facility. Additionally, a GPS signal, sourced from an external antenna, is essential for the time synchronization of the 5G New Radio (NR) system. Visual aids include a diagram detailing the radio dot placement and the datacenter's location, housing the network controllers, baseband and IRU. Another diagram illustrates the external antenna's connection, providing the GPS feed.

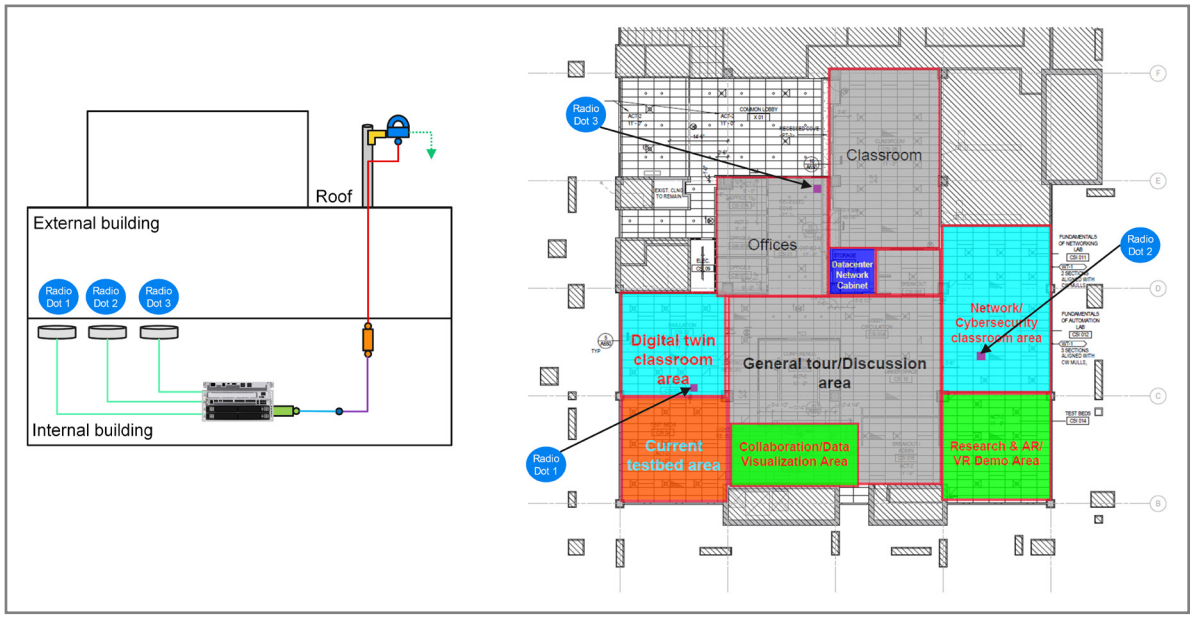

Figure 5: Location of the Radio Dot units and the Outdoor GPS antenna

An important aspect of the setup is the GPS signal, vital for the time synchronization of the 5G New Radio (NR) system. This signal is obtained from an outdoor antenna; the antenna is supplied by Ericsson but was installed by UWM due to the need for outdoor space. Figure 5 illustrates the placement of the radio dots within the facility and the location of the datacenter, where the network controllers, baseband and IRU are situated. The figure also shows the placement and connection of the outdoor antenna, providing the GPS feed.

Network Integration and Configuration for Dual-Zone Connectivity in the Ericsson Private 5G System: The system, supplied to UWM CSI, was initially designed for a singular connection point to the customer's network, utilizing an active-passive configuration via two network controllers. This setup provided a single 10Gbps SFP port on each network controller for connection to the Customer's Enterprise LAN. These controllers establish a Multicast VRRP (Virtual Router Redundancy Protocol) pair, sharing one virtual IP address. The system supports multiple VLANs from the Enterprise LAN, each with distinct VRRP pairs and VIPs, allowing routing to various segments in the Radio Network.

During the CSI integration project, a requirement emerged for the Ericsson private 5G system to serve both the Enterprise and IZ zones of the CPwE network. This necessitated physical connections from both the Enterprise Core and IZ Core switches to the network controller. This design was modeled after CSI's existing Wi-Fi infrastructure, which, while not conforming to CPwE guidelines for deploying WLAN technology,[10] had been thoroughly designed and validated by CSI's networking and cybersecurity industry partners. The Ericsson private 5G system's integration mirrored these validated configurations to ensure a seamless transition.

To achieve similar connectivity for the Ericsson private 5G system, an additional pair of Dell EMC switches was employed. These switches consolidate the physical connections from both the Enterprise Core and the IZ Core into a single physical link for each network controller, accommodating multiple VLANs. These VLANs are then mapped to distinct network segments within the radio network.

Furthermore, the network controllers' management network ports are connected to the enterprise network using a separate VLAN. This VLAN provides internet connectivity and DHCP, enabling the network controllers to connect to Ericsson's cloud services for self-configuration. Figure 6 shows a simplified layout of the logical connection from the Ericsson private 5G network system to different parts of the CSI CPwE network.

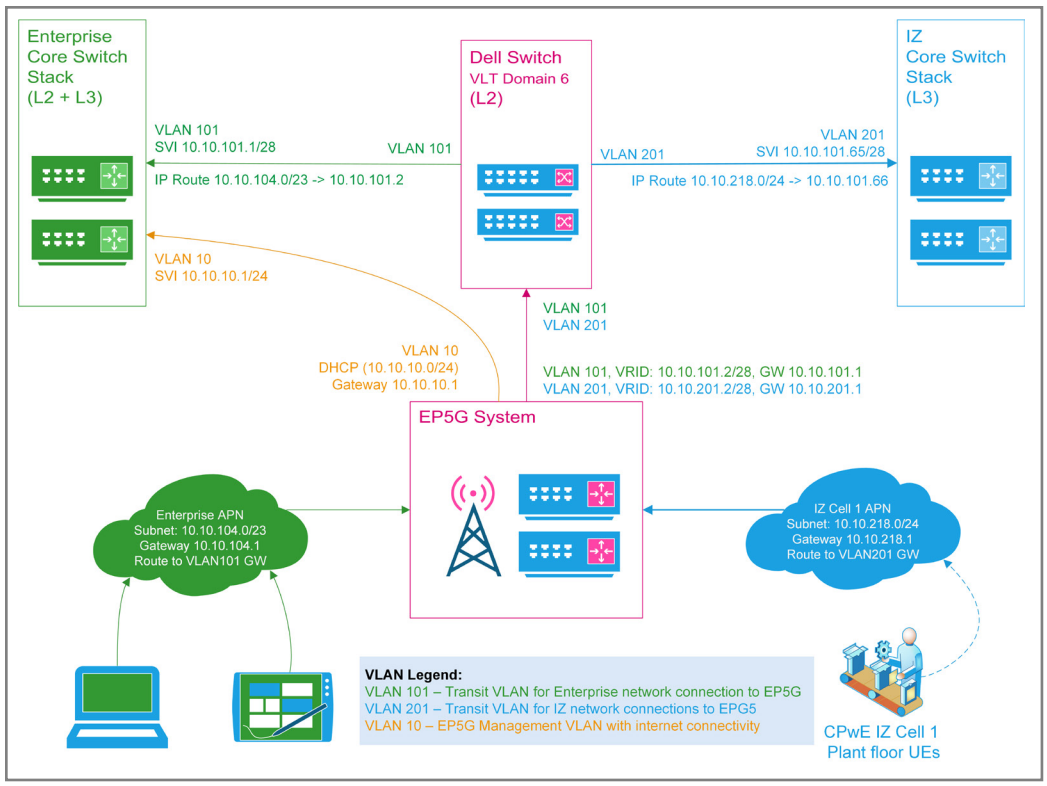

Figure 6: Simplified logical diagram showing the connectivity of different EP5G segments to the different zones of the CSI CPwE network.

Network Management and Performance Metrics of the Ericsson Private 5G System: The NMP offers comprehensive capabilities for managing network segments. These include assigning IP subnets to specific segments, mapping the routing from segments to CPwE VLANs and controlling network Quality of Service (QoS), along with priority settings for each segment. Additionally, the NMP features a user-friendly User Equipment (UE) management system. The UE in this case can be any device that can connect to the Ericsson private 5G network a sim card, ranging from 5G-ethernet gateways and routers to devices with native 5G connectivity. This system supports SIM card management, encompassing tasks such as writing and editing SIM card data. Key functions include assigning IP addresses to SIM cards, allocating SIM cards to different segments, and providing monitoring and performance statistics for each SIM card. This suite of features ensures efficient and tailored management of network resources and user equipment.

The Ericsson private 5G system at CSI was deployed on 5G NR Standalone within the CBRS band n48. Spectrum allocation is managed automatically by Ericsson's Network Management Portal (NMP), facilitated by spectrum requests from a SAS (Spectrum Access System)[11] provider selected jointly by UScellular and Ericsson. The CSI setup received a spectrum grant from SAS under the General Authorized Access (GAA) tier. Utilizing the available n48 band spectrum at the UWM campus, two 20 MHz spectrum cells have been established indoors at the CSI facility, serviced by three radio dots .

An Industrial Watchdog device, constantly powered and connected to the radio network with a sim card, monitors and reports key metrics like roundtrip latency and bandwidth to the NMP. This data is accessible through the NMP dashboard. Performance metrics gathered during the project indicate that the UWM CSI setup achieved bandwidths up to 480 Mbps, with latency figures ranging from 10-14ms. This performance level, characterized by high reliability and low jitter, has been sufficient to support all supervisory industrial automation functions, IIoT demonstrations and video streaming demos highlighted in this project, without any notable loss in system performance or operability.

Challenges and Workarounds

As we transition from detailing the implementation project, it is essential to consider the technical complexities that arose. The subsequent section will unpack these challenges, examining the obstacles and innovative solutions that the team encountered while integrating private 5G into the CPwE architecture at UWM CSI. This exploration will not only highlight the technical hurdles but also the collaborative efforts and strategic problem-solving that contributed to the project's success.

Technical Hurdles Encountered

A primary challenge encountered in the project was sourcing devices compatible with the 5G NR Standalone (SA) network. Despite the Ericsson private 5G system's capability to operate with LTE or 5G NR Non-standalone networks, the project's focus on harnessing the latest technology and the inherent complexities of using cutting-edge solutions, led to the decision to initiate with NR SA. However, while LTE Cat 18 devices are widespread in Industrial Automation and IIoT applications, devices compatible with 5G NR SA networks over CBRS as defined in 3GPP Release 16 are still emerging from development phases. This limitation necessitated the use of currently compatible and certified mobile gateways (UE), such as the Cradlepoint R1900 and E3000. These devices, functioning as Layer 3 routers, constrained the scope of testing for inter-device communication within various segments of a single industrial operations system over the private 5G network. This limitation highlights an area for further exploration in future projects, particularly in enhancing the capabilities of inter-device communication over private 5G networks.

A significant challenge identified during the project pertained to the bi-directional routing of packets to and from Industrial Automation devices through the mobile gateways. Typically, cellular networks are designed primarily to provide internet access to User Equipment (UE) devices, making bi-directional routing often unnecessary. In conventional industrial automation setups, the ability to freely route southbound packets from higher network levels to lower ones is crucial. Some example uses of this topology could be a monitoring server in the IDMZ polling sensor data from plant floor equipment, or an engineer accessing a Programmable Logic Controller (PLC) from a workstation to modify its program. To support such scenarios, particularly when a segment of the plant floor network is situated behind private 5G UEs acting as mobile gateways, Ericsson introduced the Routing Behind Mobile Station (RBMS) feature into the Ericsson private 5G systems during this project.

However, the implementation of RBMS revealed inconsistencies; while some packets routed correctly in both directions, others, both from different Industrial protocols and traditional networking protocols like TLS and HTTP, were dropped. Collaboration with Ericsson and Rockwell Automation identified that the RBMS feature functions seamlessly in LTE and NR NSA deployments. Yet, in NR SA deployments, bugs in certain Qualcomm modem firmware led to these issues, rendering RBMS currently impractical for NR SA deployments. This necessitates exploring alternative methods for routing southbound traffic to networks behind the mobile gateway. Such challenges emphasize the critical need for practical tests in the implementation of these systems within industrial automation contexts.

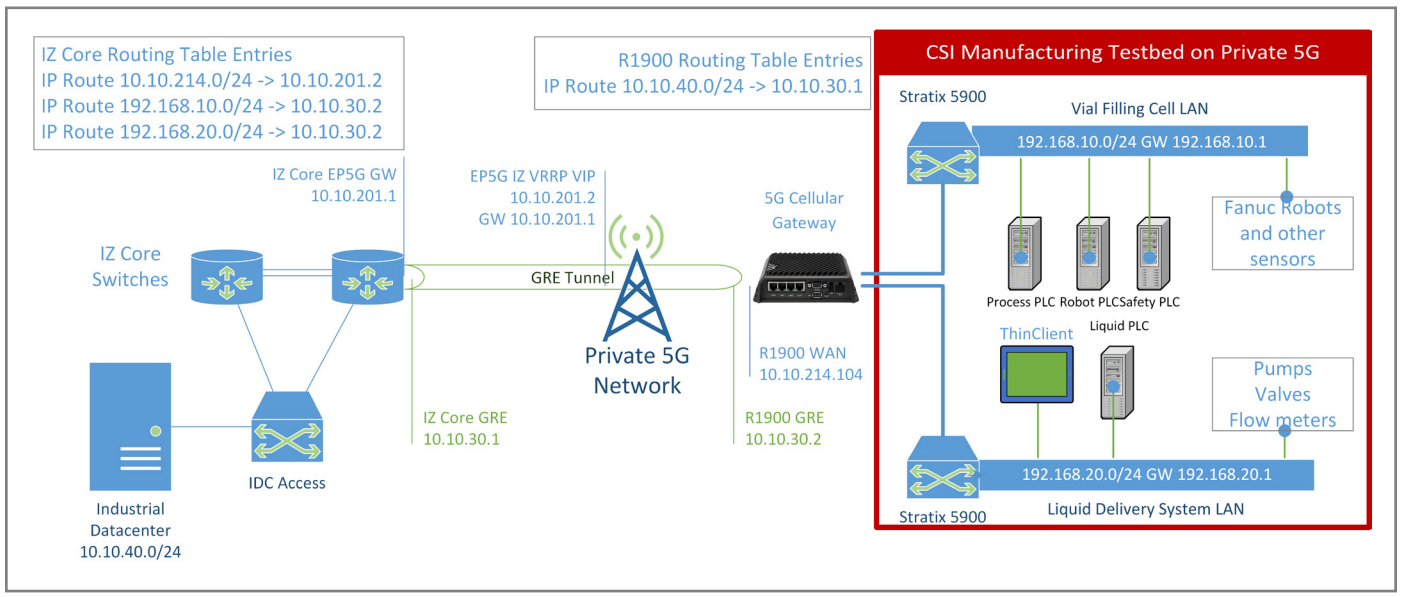

Figure 7: Example of routing configuration through GRE tunnels in CSI EP5G network

Devising Solutions

To develop a workaround for the RBMS issue, we utilized strategies from the CPwE Design and Implementation Guide[12] for implementing a Site-to-Site VPN for connecting a remote manufacturing cell to a CPwE network via a public WAN. The guide suggests using Generic Routing Encapsulation (GRE) tunnels for establishing connectivity between the remote LAN and the IZ LAN in CPwE. However, as the guide primarily addresses the transportation of secure data over public WAN, it emphasizes creating these tunnels within an encrypted IPSec VPN tunnel. This necessitates additional configurations, including multi-point VPN termination routers and additional VRFs to segregate public and private networks.

In our scenario, since the traffic navigates through the secure Ericsson private 5G infrastructure without exiting the CSI network, we can bypass the security protocols outlined in the guide. We implemented a straightforward GRE tunnel from the IZ Core to each Mobile Gateway device. This allows us to route the subnets behind the mobile gateway through the GRE tunnel. The tunnel is configured between the IZ Core gateway IP address for the Ericsson private 5G network and the Cellular WAN interface IP address of the Cradlepoint R1900 mobile gateway. Consequently, within the Ericsson private 5G infrastructure, the Cellular WAN interface of the mobile gateway appears as a single endpoint IP, communicating with the gateway IP of the IZ core router. This arrangement circumvents the Qualcomm modem firmware bug, as GRE encapsulated traffic remains unaffected. Thus, routed traffic can flow smoothly within the tunnel. Figure 7 shows the GRE tunnel configuration between the IZ Core and the Cradlepoint R1900 gateway connecting the CSI Advanced Manufacturing Testbed to the CPwE network.

However, this introduction of the GRE tunnel has one implication: it reduces the available Maximum Transmission Unit (MTU) for connections from the testbed network to the rest of the CPwE network, from the standard network MTU of 1500 to 1420. This change necessitates reconfigurations in certain applications utilizing UDP traffic. A notable example of such an application requiring adjustments is the ThinManager service deployed in the CSI IDMZ. However, with the minor MTU change, all services communicating between the other parts of the IZ and IDMZ to the PLCs and devices in the CSI Advanced Manufacturing Testbed were fully functional and was indistinguishable from their operation over wired ethernet connections.

Recommendations

Reflecting on the UWM CSI private 5G integration project, hands-on experience and addressing unforeseen technical challenges during the project were invaluable. Here are some strategic recommendations for organizations looking to undertake similar technological integrations:

1. **Thorough Pre-Planning**: For comprehensive pre-planning, it is critical to consider the spatial and technical demands of installing 5G components. Ensuring the physical infrastructure, such as radio dot placement and GPS antenna installation, is essential.
2. **Vendor Collaboration**: Partner with experienced vendors who can offer end-to-end support. Collaboration with institutions like CSI offers unique access to top-tier technology partners, enriching the implementation with expert support and advanced insights. This alliance enables organizations to leverage CSI's established relationships and expertise.
3. **System Compatibility**: In terms of system compatibility, the integration highlighted the necessity for versatile network connections that cater to diverse zone requirements within industrial settings. Adapting the 5G system to interface with both the plant floor and enterprise network was crucial, demonstrating the need for a flexible approach to network architecture.
4. **Testing and Validation**: Establishing a suite of tests to benchmark network performance before and after 5G integration provides clear insight into the improvements and any areas that require optimization. This was exemplified by the project's demonstration with different services over private 5G network, which was instrumental in validating the network's low latency and high bandwidth capabilities.
5. **Training and Knowledge Transfer**: Training and knowledge transfer are essential and collaboration with CSI offers a unique opportunity to utilize their systems and resources for in-depth learning before committing to a full system acquisition. The project at CSI serves as a testament to the effectiveness of such collaborative training.

By engaging in a process that involves rigorous planning, partnership and comprehensive testing, organizations can ensure that the integration of private 5G into their industrial settings not only meets technical expectations but also aligns with long-term operational goals. This document, enriched by the detailed experiences of the CSI project, stands as a testament to the importance of a meticulous and informed approach to adopting 5G technologies.

Photo courtesy University of Wisconsin-Milwaukee

Conclusion

The UWM CSI private 5G project stands as a pivotal exploration into the strategic integration of advanced wireless technologies in industrial automation. This white paper has navigated through the comprehensive implementation process, emphasizing the transformative potential and strategic value of private 5G networks.

Looking ahead: The project's anticipations points to a dual path of expansion. On one hand, integrating Mixed-mode LTE technology with the existing Ericsson private 5G system offers an opportunity to harness current capabilities while accommodating prevalent devices. This step back is pivotal in understanding the full spectrum of possibilities within existing technological frameworks. On the other hand, UWM CSI would closely follow how the industry evolves forward, and would wish to see more features from future 3GPP releases become integrated into the capabilities of private cellular systems. Such advancements promise to unlock even greater potential in industrial automation, particularly in applications requiring stringent safety and precise motion control.

In conclusion, the UWM CSI private 5G project not only exemplifies a successful integration of current technology but also sets a forward-looking roadmap. It underscores the ongoing evolution in industrial connectivity, driving towards a future where industrial automation reaches new heights of efficiency, safety and innovation.

References

[1] Rockwell Automation, "Converged Plantwide Ethernet (CPwE) Design and Implementation Guide." Accessed: Jan. 28, 2024.

[2] Rockwell Automation, "Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense." Accessed: Jan. 28, 2024.

[3] D. D. Brandt and S. T. Griffiths, "5G - Not Just for Cell Phones Anymore," in ODVA 2020 Industry Conference & 20th Annual Meeting, Palm Harbor, Florida, USA: ODVA, Mar. 2020.

[4] G. Koschnick, "5G for Connected Industries and Automation (Second Editon)," White Paper. Accessed: Jan. 28, 2024.

[5] Ericsson, "Critical capabilities for private 5G networks," White Paper. Accessed: Jan. 28, 2024.

[6] "CBRS spectrum - Citizen's Broadcast Radio Service." Accessed: Mar. 08, 2024.

[7] Fortinet, "Securing OT in the Face of IIoT and 5G," White Paper. Accessed: Mar. 10, 2024.

[8] "Indoor Radio Unit." Accessed: Mar. 08, 2024.

[9] "Radio Dots." Accessed: Mar. 08, 2024.

[10] Rockwell Automation, "Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide." Accessed: Jan. 28, 2024.

[11] "CBRS SAS: Simple Explanation of the Spectrum Access System." Accessed: Mar. 08, 2024.

[12] Rockwell Automation, "Site-to-Site VPN to a Converged Plantwide Ethernet Architecture." Accessed: Jan. 28, 2024.

Cover photo and illustrations courtesy University of Wisconsin-Milwaukee