IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 November 2025, accepted 27 January 2026, date of publication 6 February 2026, date of current version 13 February 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3661888

RESEARCH ARTICLE

In-Depth Study and Analysis of OT and IT Traffic Separation in Refinery and Petrochemical Industries

VANLIN SATHYA, STEVE TOTEDA, AND RAJEEV SHAH
Celona Inc., Campbell, CA 95008, USA
Telecommunications and Industrial 5G
Corresponding author: Vanlin Sathya (vanlin@celona.io)

ABSTRACT The convergence of Operational Technology (OT) and Information Technology (IT) in industries such as refineries and petrochemical plants promises improved performance and better decision-making, but true enhancement of security comes from I5G capabilities — device-bound identity and location technology that provides secure, tamper-proof authentication, precise access control and logical and physical network segmentation. However, traditional networks struggle to meet the stringent connectivity demands of integrated OT/IT environments. This paper investigates the potential of Industrial 5G (I5G) networks to address these limitations, exploring existing OT/IT connectivity architectures based on WirelessHART, LoRa, and Public Cellular (MNOs). We propose I5G solutions that enable effective OT/IT separation through logical and physical network segmentation. Furthermore, we present a comparative analysis of latency performance for IT and OT devices in an I5G network, considering realistic load scenarios with and without logical and physical network segmentation (*i.e.,* micro-slicing), providing valuable insights for practical I5G deployments.

INDEX TERMS Industrial 5G, OT/IT convergence, network security, micro-slicing, latency analysis, industrial IoT, refineries, petrochemical.

I. INTRODUCTION

The convergence of Information Technology (IT) and Operational Technology (OT) is a significant trend in the industrial sectors [1], [2], including the refining and petrochemical industries. IT refers to the use of computers (Laptops), mobile devices (Tablets, iPads, Phones), and telecommunication equipment (as shown in Fig. 1) to store, retrieve, transmit and manipulate data, while OT involves hardware and software that detects or causes changes through direct monitoring and control of physical devices, processes, and events as shown in Fig. 2. The integration of these two domains can lead to improved operational efficiency, enhanced safety and security, and better decision making capabilities.

The advantage of implementing an industrial network, specifically Industrial 5G (I5G), in the context of OT/IT integration is driven by several factors, particularly in hazardous environments like refineries and petrochemical plants. Firstly, Industrial 5G (I5G) networks offer enhanced security features compared to traditional public cellular networks. The ability to control and manage the network internally ensures that sensitive data remains within the organization, reducing the risk of external threats and data breaches. This is particularly important in industries where the integrity and confidentiality of data is paramount.

Equally important, I5G networks provide critical safety capabilities for hazardous industrial environments. In refineries and petrochemical plants, real-time gas detection and monitoring systems are essential for preventing catastrophic incidents involving toxic gases like hydrogen sulfide (H2S), carbon monoxide (CO), and volatile organic compounds (VOCs). I5G networks enable reliable, low-latency connectivity for gas detection sensors, emergency shutdown systems (ESD), and safety instrumented systems (SIS) within the hazardous zone, ensuring immediate response to hazardous conditions. The network's reliability and dedicated infrastructure ensure that safety-critical communications are

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

© 2026 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

never compromised, even during peak network usage or cyber incidents.

Secondly, I5G networks provide superior performance in terms of latency, reliability, and bandwidth. Unlike traditional mobile network operators (MNOs), LoRa gateway and Wi-Fi networks, I5G networks can be tailored to meet the specific needs of industrial applications. For example, the low latency and high reliability of I5G networks are essential for real-time monitoring and control of industrial processes. This ensures that critical operations are not disrupted by network delays or failures.

In comparison, while MNOs offer connectivity solutions for industrial applications, their adoption for OT network remains limited. These networks often rely on public infrastructure, which may not be optimized for industrial applications. Furthermore, the shared nature of public networks can lead to congestion and poor performance during peak usage times. Lastly, in the MNO-based OT network, the enterprise data will not stay in the industry premises. On the other hand, Wi-Fi networks, although suitable for certain applications, lack the robustness and security features required for large-scale industrial deployments. Wi-Fi networks are also more susceptible to interference and have limited coverage range, making them less ideal for extensive industrial environments such as oil and gas and petrochemical industries.

In converged IT and OT environments, the implementation of Industrial 5G (I5G) networks addresses key performance and reliability challenges by providing a dedicated, high-performance foundation that can be tailored to mixed workloads. Micro-Slicing (logical and physical network segmentation) builds on this capability by assigning each device profile to its own performance lane—rather than relying on complex flow-based QoS—allowing enterprises to prioritize OT and IT traffic with precision. This approach ensures deterministic performance for latency-sensitive OT systems such as programmable logic controllers (PLCs), and sensors, while IT applications operate in flexible best-effort lanes. With end-to-end encryption, predictable performance isolation, and high reliability, Micro-Slicing makes I5G an attractive option for industries seeking to strengthen and modernize their digital infrastructure.

In summary, the motivation for adopting I5G networks in the context of OT/IT integration is driven by the need for enhanced security, superior performance, larger outdoor coverage foot-print and the ability to tailor the network to meet the specific needs of industrial applications. In this paper will explore the existing OT/IT architecture, proposed solutions for OT/IT separation, and the role of various OT connectivity technologies such as WirelessHART, MNO (Public Cellular), LoRa gateway and our proposals in achieving effective OT/IT integration. We conclude with an experimental study of integerating IT and OT device to analyze the performance interms of coverage, throughput and latency of the I5G network.

II. INDUSTRIAL HAZARDS, SAFETY SYSTEMS, AND OT CONNECTIVITY NEEDS

In this section, we discuss the products manufactured by these industries, why these environments are hazardous, what existing safety and monitoring devices are available for protection, and the need for OT networks in these environments.

A. GASES IN REFINERIES AND PETROCHEMICAL INDUSTRIES

Refineries and petrochemical plants handle various highly toxic and hazardous gases, creating significant risks. These include hydrogen sulfide (H2S), hydrogen cyanide (HCN), carbon monoxide (CO), chlorine (Cl2), and ammonia (NH3), all of which can cause severe health effects, including death, with even brief exposure. Other hazardous gases such as sulfur dioxide (SO2), nitrogen oxides (NOx), and volatile organic compounds (VOCs) like benzene, toluene, and xylene also contribute to the risk profile of these facilities. The release of these substances can occur during routine operations, process upsets, or accidents, particularly in confined spaces or during catalyst handling.

To mitigate the risks associated with poisonous gases, refineries and petrochemical plants implement rigorous safety protocols at multiple levels. These include engineering controls such as leak detection and ventilation systems, administrative controls like safe work procedures and training programs, and the use of personal protective equipment (PPE). Continuous air quality monitoring is also critical for detecting leaks and ensuring safe working conditions. The specific gases present and the level of risk vary depending on each facility's specific processes.

Ultimately, prevention hinges on regular risk assessments, proactive hazard management, and strict adherence to established safety protocols. A comprehensive approach, encompassing both technological safeguards and robust safety procedures, is vital for minimizing the potential for accidental releases and ensuring the safety of workers, the surrounding community, and the environment. Modern gas detection systems rely on networked sensors that must communicate continuously with emergency shutdown systems (ESD) and safety instrumented systems (SIS). These safety-critical communications require deterministic, ultra-reliable connectivity with guaranteed latency, capabilities that distinguish OT networks from traditional IT infrastructure. This hazardous environment underscores the critical need for reliable, real-time OT networks that can support continuous monitoring, rapid emergency response, and fail-safe operations even during extreme events.

B. MODERN GAS DETECTION INFRASTRUCTURE

Modern refineries employ a comprehensive, multi-layered approach to gas detection, integrating fixed, portable, and advanced analytical technologies to ensure worker safety and environmental protection. Fixed gas detection systems,

TABLE 1. Summary of IT OT device and sensor connectivity options.

Parameters	Wired	Public Cellular (MNO)	WirelessHART	LoRa WAN	Industrial 5G
Focus	Reliable Communication	Wide Area Connectivity	Process Automation and Control	Long Range, Low Power IoT	Dedicated Control/Security
Coverage Range	Limited by Cable Length	Wide Area	Up to 200 m	5-15 Km	Configurable (e.g.: campus)
Data Rates	High (Gbps)	10s-100s Mbps	250 Kbps	0.3 bps - 50 Kbps	100s Mbps-Gbps
Battery Consumption	N/A Line Powered	Moderate to High	Moderate	Moderate to High	Moderate
Network Topology	Point-Point	Cellular	Mesh	Star	Cellular
Determinism	Very High	Low to Moderate	High	Low	High
Security	High	Strong	Strong	Moderate	Strong (> MNO security)
Complexity	High	Moderate	More Complex	Simpler	Moderate
Licensing	Typically Not Required	Licensed Spectrum	Unlicensed	Unlicensed	CBRS/Private Spectrum
Mobility	Low	High	Low	Low	High
Cost	High	High	Moderate	Low	Moderate

strategically positioned throughout the facility, provide continuous, real-time monitoring of critical gases such as hydrogen sulfide (H2S), carbon monoxide (CO), and volatile organic compounds (VOCs). These systems utilize a variety of sensor technologies, including electrochemical sensors for targeted gas detection, infrared sensors for broad-spectrum monitoring, and catalytic bead sensors for detecting flammable substances. Fixed systems are also equipped with alarms, data logging, and remote monitoring capabilities to enable prompt response to potential hazards.

In addition to fixed systems, refineries rely on portable gas detectors, handheld devices carried by personnel performing maintenance, confined space entry, or other high-risk tasks. These portable units provide workers with personal exposure monitoring, alerting them to immediate dangers through audible and visual alarms. They also feature data logging and GPS tracking to document worker location and gas concentrations, enabling detailed exposure analysis and hazard assessment. Advanced technologies like open-path gas detectors (OPGDs) offer wide-area monitoring by measuring average gas concentrations over distances of hundreds of meters, while flame detectors rapidly identify fires and explosions.

Finally, sophisticated analytical instruments, such as gas chromatography-mass spectrometry (GC-MS) and Fourier transform infrared spectroscopy (FTIR), are deployed in laboratories to analyze gas samples collected from process streams, identify potential leaks, and ensure regulatory compliance. Emerging technologies, including wireless sensor networks and drones equipped with gas sensors, offer opportunities to enhance monitoring coverage and accessibility, while artificial intelligence (AI) algorithms promise to enable predictive leak detection and optimize safety protocols. Technology selection depends on factors such as the specific gases to be monitored, cost considerations, and regulatory requirements. Proper implementation, along with regular calibration, maintenance, and comprehensive training, is key to ensuring effectiveness, which in turn safeguards workers and the environment.

C. NEED FOR OT NETWORKS IN REFINERIES AND PETROCHEMICAL INDUSTRIES

Refineries and petrochemical plants require continuous monitoring and control of thousands of interconnected process variables and safety systems. A dedicated OT network is essential to meet these stringent operational requirements. OT networks differ fundamentally from IT networks in their design priorities:

OT networks provide deterministic, guaranteed-latency communication for time-critical control and safety functions, whereas IT networks prioritize flexibility and high throughput for business applications. This distinction necessitates dedicated OT infrastructure:

1) REAL-TIME CONTROL AND MONITORING

- **Process Control:** Refineries and petrochemical plants rely on complex control systems to manage chemical reactions, distillation processes, and other operations. OT networks provide the communication infrastructure for these systems, enabling real-time monitoring of process variables (e.g., temperature, pressure, flow rates) and automated control actions.
- **Safety Systems:** Critical safety systems, such as emergency shutdown systems (ESD), fire and gas detection systems (F&G), and safety instrumented systems (SIS), depend on reliable OT networks for rapid response to hazardous conditions.
- **Operational Efficiency:** Timely access to accurate process data enables operators to optimize plant performance, reduce energy consumption, and minimize waste.

2) HIGH RELIABILITY AND AVAILABILITY

- **Continuous Operation:** Refineries and petrochemical plants operate 24/7, and any disruption to the OT network can lead to significant production losses or safety incidents. OT networks are designed with redundant components and robust protocols to ensure high availability and minimize downtime.
- **Deterministic Performance:** Real-time control applications require predictable communication latency and minimal jitter. OT networks are designed to provide deterministic performance, ensuring that control signals are delivered within strict time constraints.

3) ENHANCED SECURITY

While OT networks face increasing cyber threats [3], [4] that can disrupt operations, compromise safety systems, and steal sensitive data, a dedicated OT network enables the implementation of security measures tailored to the unique characteristics of industrial control systems.

- **Air Gapping:** Historically, OT networks have been physically separated (air-gapped) from IT networks to prevent unauthorized access. However, the operational need for data integration and remote monitoring is driving OT/IT convergence, creating new challenges that require advanced network solutions to maintain security while enabling connectivity.
- **Network Segmentation:** Security practices are put in place to segment the OT network into zones based on criticality and security requirements. This limits the impact of a successful cyberattack.
- **Access Control:** Robust access control mechanisms ensure that only authorized personnel can access critical control systems.
- **Device Security:** Modern OT devices support dynamic security configuration, allowing security parameters to be adjusted based on current threat levels and risk assessments.

4) SUPPORT FOR SPECIALIZED PROTOCOLS AND DEVICES

- **Industrial Protocols:** OT networks support a variety of specialized industrial protocols, such as Modbus, Profibus, and HART, which are used to communicate with sensors, actuators, and other control devices.
- **Legacy Equipment:** Many refineries and petrochemical plants have legacy equipment that is not compatible with modern IT networks. OT networks provide a platform for integrating these legacy devices into the overall control system.

5) REGULATORY COMPLIANCE

- **Safety Regulations:** Refineries and petrochemical plants are subject to stringent safety regulations, such as OSHA's Process Safety Management (PSM) standard, which require them to implement robust control systems and safety measures.
- **Environmental Regulations:** OT networks ensure regulatory compliance through 24/7 automated monitoring of emissions and waste streams, providing early warning of potential violations and maintaining continuous compliance records.

In summary, these requirements, e.g. deterministic performance, specialized protocols, and stringent security, historically necessitated complete separation between OT and IT networks. However, modern industrial operations increasingly require data integration between domains. This creates a critical challenge: how to converge OT and IT onto shared infrastructure while maintaining the isolation and performance guarantees each requires. Section III explores how Industrial 5G networks with advanced technology address this challenge.

III. IT OT CONNECTIVITY ARCHITECTURE

In this sub-section, we discuss different OT connectivity options. Table 1 shows the summary of wired, Public Cellular, WirelessHART, LoRa WAN and Industrial 5G (I5G). We discuss the advantages and disadvantages of traditional communications and in real-world deployments when the end user enable the mission-critical applications (eg: OT devices) on less than reliable networks or networks with coverage gaps, potentially leads to huge losses in the return on investment. For example: In the refinery (Oil & Gas) environment, sensors are used to monitor the flow of the oil when it moves from one division (A) to the other division (B) for processing the crude oil into a valuable product. In some cases, Division A and B belong to two different companies, and they will charge or value the revenue based on the flow of the oil. If the sensor data is not reliable in transmitting or if it fail to transmit on on-time due to coverage holes or no connectivity. Then its a huge problem in such scenarios. Hence, in this Section, clear differences with each technology, helps the end user to decide which use-case to enable on which network. Also, Fig. 4 shows the connectivity architecture with backhaul connection to the controller system.

A. WIRED NETWORK-BASED OT TRAFFIC CONNECTIVITY

Wired network-based OT traffic connectivity [5] is a crucial aspect of industrial communication systems, providing reliable and secure data transmission for monitoring and controlling industrial processes. In OT environments, wired networks are often preferred for their stability, high data rates, and low latency, making them suitable for critical applications that require real-time communication and precise control.

- **Ethernet Technology:** Ethernet technology is widely used in wired OT networks, offering high-speed data transmission and robust performance. Industrial Ethernet implementations utilize CAT 5e, CAT 6, and CAT 6A cables to provide deterministic connectivity between OT devices, including sensors, actuators, PLCs, and SCADA systems. These implementations—such as PROFINET, EtherNet/IP, and Modbus TCP—ensure predictable latency and guaranteed delivery times essential for real-time control, while supporting data rates from 100 Mbps to 10 Gbps depending on cable category and distance.
- **Wired OT Network Infrastructure:** [6] In many industrial environments, wired OT networks are deployed to connect various devices and systems. For example, Most refineries uses a wired OT network with Industrialized Ethernet technologies, specifically Wired OT Network Infrastructure [6], with examples that include specialized industrial Ethernet networks such as Honeywell's Experion Local Control Network (ELCN), which provides redundant, deterministic communication between process controllers, I/O systems, and operator workstations. These networks ensure the reliable, low-latency data transmission essential for real-time process control and safety system integration. This setup allows for efficient communication between OT devices, ensuring that critical data is transmitted securely and reliably.

(a) Ruggedize Laptop. (b) Scanner (c) Iphone and IPad (d) Hazardous Zone Device

FIGURE 1. Different IT form factors (handheld and tablets) used in Refineries and Petrochemical Industries.

- **Integration with IT Networks:** Wired OT networks can be integrated with IT networks to enable seamless communication and data exchange between IT and OT systems. This integration is essential for achieving OT/IT convergence, allowing organizations to leverage the benefits of both domains. For instance, one single common architecture design is needed which includes a mix of LoRa, Wi-Fi, and I5G networks, with wired connections using Ethernet cables. This hybrid approach ensures that both IT and OT systems can communicate effectively, enhancing overall operational efficiency.
- **Security and Encryption:** Security is a paramount concern in OT environments, and wired networks offer several advantages in this regard. Wired connections are inherently less susceptible to interference and eavesdropping compared to wireless networks, providing a more secure physical communication channel for transmitting sensitive data. For additional protection, encryption protocols such as IPsec can be implemented to secure OT traffic end-to-end across the network. In industrial environments, however, TLS/SSL is more commonly used for IT traffic, while OT networks often employ industrial-specific security protocols like OPC UA security or rely on network segmentation and air-gapping rather than encryption due to latency constraints. This ensures that data remains confidential and protected from unauthorized access.
- **Reliability and Stability:** Wired networks are known for their reliability and stability, making them ideal for critical OT applications. Unlike wireless networks, which can be affected by interference and signal degradation, wired connections provide consistent performance and minimal downtime. This reliability is crucial for maintaining the integrity of industrial processes and ensuring that operations run smoothly.

1) CHALLENGES AND LIMITATIONS

Despite their advantages, wired networks also present certain challenges and limitations. The deployment of wired infrastructure can be costly and time-consuming, especially in large industrial and hazard environments. Additionally, wired connections may lack the flexibility and scalability of wireless networks, making it difficult to reconfigure the network as needed. Ensuring compatibility and interoperability between different network components can also be complex, requiring careful planning and implementation.

B. PUBLIC CELLULAR-BASED CONNECTIVITY FOR OT APPLICATIONS

Public cellular (MNO) connectivity [7], [8], [9], [10], [11], [12] can play a role in OT networks, but its applicability is limited to scenarios where private network deployment is either impractical, cost-prohibitive, or operationally unnecessary. These situations are generally non-critical in nature, or where moderate performance variability is acceptable. Examples include: connecting widely separated sites, linking mobile assets that frequently change location, or enabling temporary connectivity during construction or short-term projects.

In most industrial facilities, especially in process industries like oil & gas, refining, and petrochemicals, public cellular is not a primary network for plant-floor operations. Life-safety and mission-critical control systems—such as Emergency Shutdown Systems (ESD) or Safety Instrumented Systems (SIS)—require deterministic performance with quantifiable and proven reliability metrics. Since public cellular networks do not offer the Service Level Agreements (SLAs) or transparency required for reliability calculations (e.g., Probability of Failure on Demand, PFD, per IEC 61508), they are excluded from these roles.

- **Remote Connections:** One of the key advantages of MNO-based (Public Cellular) connectivity is its ability to facilitate connections between geographically separated OT networks where private infrastructure is not feasible. For example, chemical processing facilities often use MNO connections to link OT networks separated by approximately 35 miles. At Location A, they deploy a multi-carrier cellular gateway capable of operating on three different MNOs for redundancy, while Location B uses a single-carrier connection through Public Cellular Wireless. This setup provides communication between remote locations for supervisory monitoring and non-critical control functions,

though it remains unsuitable for real-time control applications due to latency variability.

- **Flexibility and Scalability:** MNO-based connectivity offers wide-area coverage [13], [14], [15], [16] and the ability to quickly deploy devices using physical SIMs or eSIMs, which can be advantageous for connecting remote or mobile OT assets without building dedicated infrastructure. However, large-scale deployments can create SIM management complexity, and public network congestion during peak periods may reduce scalability in practice.
- **Security and Encryption:** [17] Public cellular networks provide SIM-based authentication and over-the-air encryption, helping protect data in transit from unauthorized access. In OT environments, however, the shared nature of public networks increases the attack surface, and additional endpoint and application-layer security measures are needed to mitigate risks beyond what the MNO inherently provides.
- **Reliability and Performance:** MNO infrastructure can deliver stable performance for non-critical telemetry and monitoring, with reasonable latency under normal load conditions. The performance lies in latency variability—especially at cell edges or under heavy load (''cell breathing'')—which makes public cellular unsuitable for deterministic, time-sensitive OT control or safety systems.
- **Integration with Existing Infrastructure:** Public cellular can be part of a hybrid network design that also includes LoRaWAN, Wi-Fi, and private LTE/5G, enabling OT systems in remote locations to connect with central monitoring platforms. Yet integration can require protocol translation, additional gateways, or VPN solutions to overcome NAT restrictions, which adds cost and complexity.
- **Use Cases in OT Networks:** Appropriate applications include remote tank level monitoring in rural areas, temporary environmental sensing during plant turnarounds, and fleet tracking for cranes or heavy transport during mobilization. It is generally not used for gas monitoring in life-safety systems, as these require dedicated, standards-compliant safety networks with proven reliability metrics not offered by MNO services.

1) CHALLENGES AND LIMITATIONS OF MNO-BASED OT TRAFFIC CONNECTIVITY

While public cellular offers certain deployment advantages, it presents inherent limitations for OT applications—particularly those requiring deterministic, guaranteed performance or regulatory compliance.

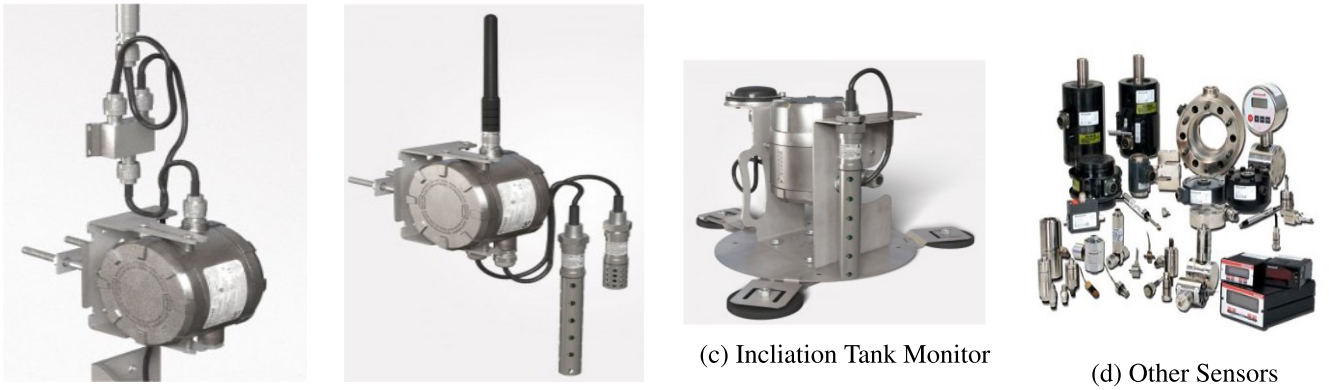
- **Lack of Performance Guarantees:** MNO networks typically do not offer SLAs with quantifiable metrics like PFD (Probability of Failure on Demand) required by standards such as IEC 61508. This makes them unsuitable for life-safety or high-reliability control applications.
- **Variable Latency and ''Cell Breathing'':** Latency can fluctuate significantly, especially during peak load when coverage cells ''breathe'' and fringe sites lose signal strength. This unpredictability can affect control loop performance or time-sensitive monitoring.
- **Limited Control and Visibility:** Public networks provide little to no control over routing, QoS policies, or network configuration. OT operators have minimal visibility into underlying network performance or fault conditions.
- **Connectivity Challenges at the Edge:** Devices at cell edges or in remote locations may experience unstable connectivity, especially where fewer towers or limited spectrum bands are available.
- **NAT and Protocol Restrictions:** Carrier-grade NAT can block certain inbound connections or industrial protocols, requiring workarounds that add complexity.
- **SIM and Device Management Overhead:** Managing large fleets of SIMs, data plans, and subscription renewals adds operational complexity, especially when devices are widely distributed geographically.
- **Cost Considerations:** Ongoing subscription fees, SIM costs, and potential overage charges can add up, especially for high-data or large-scale deployments.
- **Regulatory and Technical Constraints:** Regulatory and Technical Constraints: Industrial integration may require gateways or protocol converters to interface industrial protocols with cellular connectivity, adding deployment complexity.

C. WIRELESSHART OT BASED ARCHITECTURE

The WirelessHART protocol [18] is a widely adopted standard for wireless communication in industrial environments. Both WirelessHART and ISA100.11a build upon the IEEE 802.15.4-2006 physical layer, operating in the 2.4 GHz ISM band (2400-2483.5 MHz), but implement proprietary MAC layers optimized for industrial applications. The protocol supports maximum data rates of up to 250 Kbits/sec, making it suitable for various industrial applications.

One of the key features of WirelessHART [19] is its mesh network architecture. In a mesh network, devices communicate with each other and act as repeaters, ensuring reliable and resilient data communication. This architecture enhances the network's robustness, as data can be routed through multiple paths, reducing the likelihood of communication failures.

The WirelessHART protocol employs direct sequence spread spectrum (DSSS) technology and channel hopping for communication. DSSS spreads the signal over a wider frequency band, making it more resistant to interference and eavesdropping. Channel hopping further enhances reliability by periodically changing the communication channel, reducing the impact of interference and improving overall network performance.



(a) Monitor Gas. (b) Hydrocarbon Sensor (c) Incliation Tank Monitor (d) Other Sensors

FIGURE 2. OT Sensor used in refineries and petrochemical industries.

(a) Methane Emission. (b) Gas Heat Map (c) Drone Inspection (d) AI based Robots

FIGURE 3. Advanced OT devices with AI/ML data traffics on industry network.

Time Division Multiple Access (TDMA) is another critical feature of WirelessHART. TDMA ensures reliable latency and controlled communication among devices on the network. By dividing the communication channel into time slots, TDMA allows multiple devices to share the same channel without causing collisions, ensuring timely and predictable data transmission.

In the context of OT networks, WirelessHART is used to connect various sensors and actuators, enabling real-time monitoring and control of industrial processes. Refinery companies have deployed OT networks using WirelessHART devices at some locations, while in other places, they have opted for wired networks.

The use of WirelessHART in OT networks offers several advantages [20]:

- **Flexibility:** WirelessHART eliminates the need for extensive cabling, making it easier to deploy and reconfigure the network as needed. This is particularly beneficial in dynamic industrial environments where equipment and processes may change frequently.
- **Scalability:** The mesh network architecture allows for easy expansion of the network by simply adding more devices. Each new device can communicate with its neighbors, extending the network's coverage and capacity.
- **Reliability:** The combination of mesh networking, DSSS, and channel hopping ensures that the network remains reliable even in the presence of interference and other challenging conditions. The TDMA mechanism further enhances reliability by preventing data collisions and ensuring timely communication.
- **Power Consumption:** WirelessHART devices rely on battery power, with a typical lifespan of 5–7 years. Managing power consumption is a key challenge, especially in industrial environments where devices are often installed in remote or hard-to-access locations. A primary advantage of WirelessHART is its time synchronization feature, which allows sensors to remain in a low-power "sleep" mode for extended periods, waking only to transmit data. This significantly extends battery life and reduces the need for frequent replacements or recharging, which can be costly and impractical.
- **Security:** WirelessHART incorporates robust security features, including encryption and authentication, to protect data from unauthorized access and tampering. This is crucial in industrial environments where the integrity and confidentiality of data are paramount.

1) LIMITATIONS ON WIRELESSHART

While WirelessHART offers several advantages for OT networks, it also presents certain challenges and limitations that need to be addressed for optimal performance and reliability.

- **Interference and Signal Quality:** WirelessHART operates on the 2400-2483.5 MHz license-free ISM bands [21], [22], which are also used by various other wireless technologies such as Wi-Fi and Bluetooth. This can lead to interference, affecting signal quality and reliability. In industrial environments, where numerous wireless devices may be operating simultaneously, managing interference becomes a critical challenge.
- **Limited Data Rates:** The maximum data rate supported by WirelessHART is up to 250 Kbits/sec [23]. While this is sufficient for many industrial applications, it may not be adequate for high-bandwidth applications such as video streaming or large-scale data analytics or drone and robots in the future (as shown in Fig. 3). The limited data rate can constrain the types of applications that can be effectively deployed on WirelessHART networks.
- **Scalability Issues:** Scalability Constraints: TDMA architecture limits practical deployments to 100-250 devices per gateway with typical 4-8 second update rates. While sufficient for dedicated sensor networks, large facilities with thousands of monitoring points require multiple gateway deployments. However, WirelessHART remains well-suited for its intended purpose of low-power, periodic process monitoring where these constraints are acceptable.
- **Security Concerns:** While WirelessHART incorporates robust security features such as encryption and authentication, it is not immune to security threats. Industrial environments are often targeted by cyber-attacks, and ensuring the security of wireless communication is paramount. Continuous monitoring and updating of security protocols are necessary to mitigate potential vulnerabilities.
- **Integration with Existing Infrastructure:** Integrating WirelessHART with existing wired infrastructure and other wireless technologies can be complex. Ensuring seamless communication and interoperability between different network components requires careful planning and implementation. Compatibility issues and the need for specialized equipment can add to the complexity of integration.
- Latency and Real-Time Communication While WirelessHART employs TDMA to ensure reliable latency, real-time communication can still be challenging in certain applications. Industrial processes often require immediate and precise control, and any delay in communication can impact operational efficiency and safety. Ensuring low latency and real-time responsiveness is critical for effective OT network performance.

D. LoRa BASED OT ARCHITECTURE

LoRa (Long Range [24], [25]) is a wireless communication technology that is designed for long-range, low-power, and low-data-rate applications. It is particularly well-suited for industrial environments where devices need to communicate over long distances with minimal power consumption. The LoRa architecture [26] is based on a star-of-stars topology, where end devices communicate with gateways using the LoRa physical layer, and the gateways forward the data to a central network server.

- **LoRa Physical Layer:** [27] The LoRa physical layer uses a modulation technique called Chirp Spread Spectrum (CSS), which allows for long-range communication with low power consumption. CSS spreads the signal over a wide frequency band, making it resistant to interference and capable of operating in noisy environments. The LoRa physical layer operates in the license-free ISM bands, such as 868 MHz in Europe and 915 MHz in North America.
- **LoRaWAN Architecture and Protocol:** [28] LoRaWAN (Long Range Wide Area Network) is the communication protocol and system architecture for managing the communication between end devices and gateways. It defines the MAC (Medium Access Control) layer and the network layer, providing features such as secure communication, adaptive data rate, and network scalability. LoRaWAN supports three classes of end devices:
  1) Class A: End devices have the lowest power consumption and communicate with the network server only when they have data to send. After sending data, they open two short receive windows for downlink communication.
  2) Class B: End devices open additional receive windows at scheduled times, allowing for more frequent downlink communication.
  3) Class C: End devices have continuous receive windows, except when transmitting, allowing for low-latency downlink communication.
- **Gateways:** Gateways [29] act as intermediaries between end devices and the network server. They receive data from end devices and forward it to the network server using a backhaul connection, such as Ethernet, cellular (MNO or I5G), or Wi-Fi. Gateways can handle communication from multiple end devices simultaneously, making them scalable and efficient for large deployments.
- **Network Server:** The network server is the central component of the LoRa architecture. It manages the communication between end devices and gateways, handles data routing, and ensures secure communication. The network server also manages device authentication, data encryption, and adaptive data rate adjustments to optimize network performance.
- **Application Server:** The application server processes the data received from end devices and provides the necessary application logic. It can be integrated with various industrial applications, such as monitoring and control systems, data analytics platforms, and enterprise resource planning (ERP) systems.

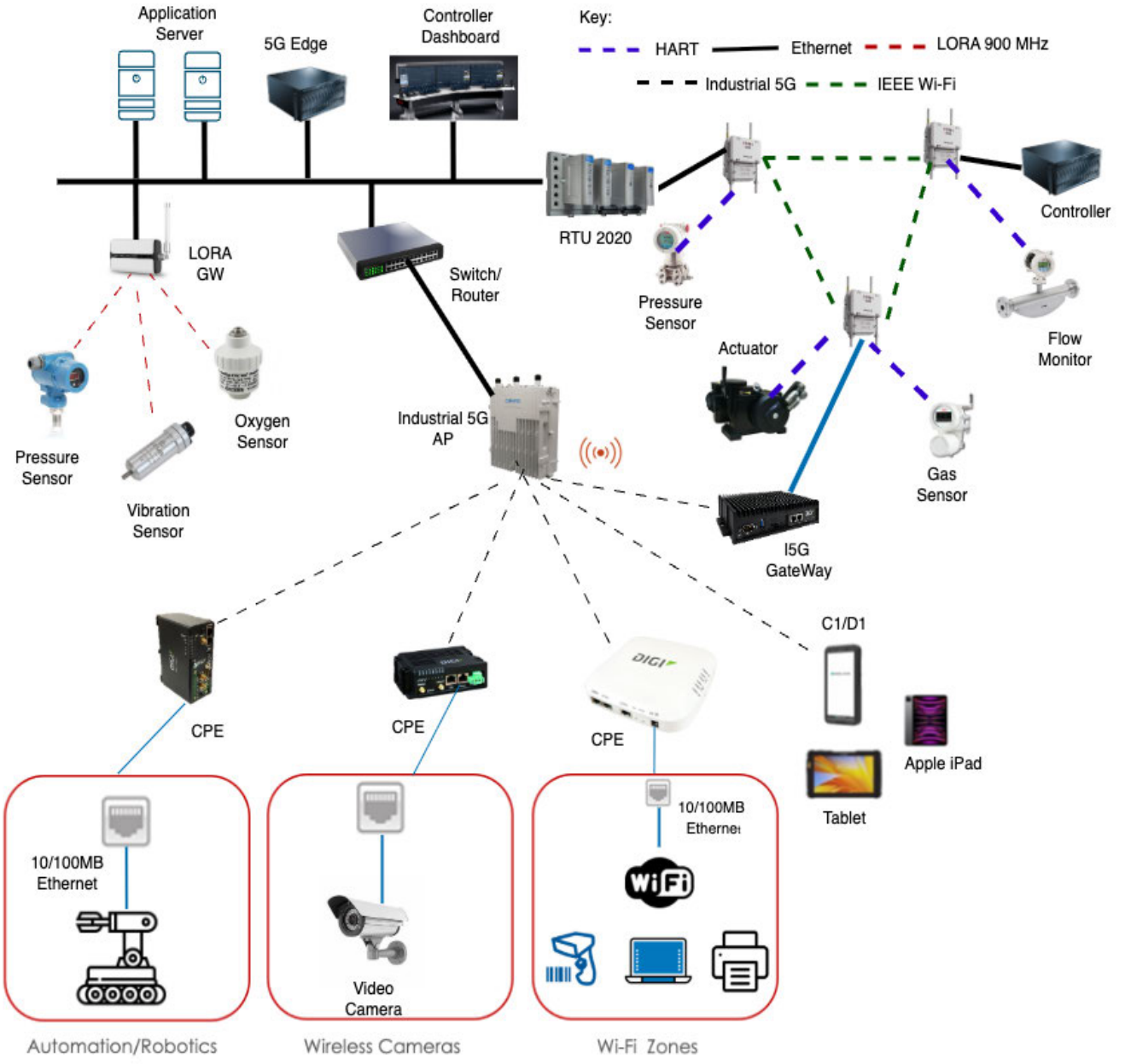


FIGURE 4. IT OT connectivity architecture - wired, LoRa, WirelessHART, and I5G.

- **Integration with OT Networks:** In OT networks, LoRa can be used to connect various sensors used for condition monitoring to aid in the monitoring and control of industrial processes.

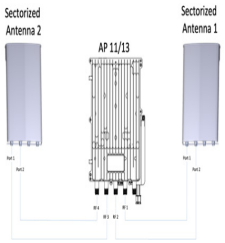
Use Cases in OT Networks

1) Gas Monitoring: LoRa can be used to connect gas detectors in industrial environments, providing real-time data on gas levels and ensuring safety compliance.
2) Tank Monitoring: LoRa-enabled sensors can monitor fluid levels in storage tanks, providing data for inventory management and process optimization.
3) Mobile Cranes: LoRa can be used to monitor the position and status of mobile cranes, ensuring safe and efficient operation.
4) Heat Maps: LoRa-enabled sensors can provide data for creating heat maps of industrial environments, helping to identify areas of high activity or potential hazards. The possible type of OT network Heat Maps are:

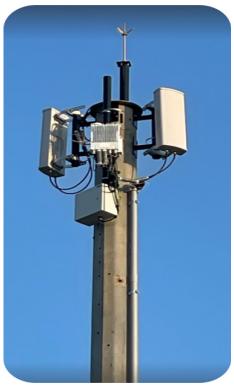
   - **Thermal heat maps** - showing temperature variations across the facility.
   - **Activity heat maps** - showing areas of high operational activity.

(a) Outdoor AP

(b) Sector Antenna



(c) AP with Sector Connections

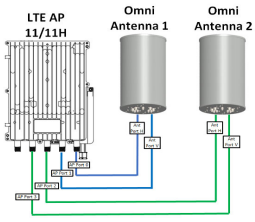


(c) Sector Deployment

FIGURE 5. Sector antenna installations - I5G outdoor AP.

(a) Outdoor AP

(b) Omni Antenna



(c) AP with Omni

(c) Omni Deployment

FIGURE 6. Omni antenna installations - I5G outdoor AP.

- **Gas concentration maps** - visualizing hazardous gas distributions.

1) CHALLENGES AND LIMITATIONS OF LoRa IN OT ENVIRONMENTS

While LoRa technology offers several advantages for OT networks, such as long-range communication and low power consumption, it also presents certain challenges and limitations that need to be addressed for optimal performance and reliability.

- **Interference and Signal Quality:** LoRa operates in the license-free ISM bands, such as 868 MHz in Europe and 915 MHz in North America. These bands are also used by various other wireless technologies, which can lead to interference and affect signal quality. In industrial environments, where numerous wireless devices may be operating simultaneously, managing interference becomes a critical challenge. The presence of physical obstacles, such as walls and machinery, can also degrade signal quality and reduce communication range.
- **Limited Data Rates:** LoRa is designed for low-data-rate applications, with maximum data rates typically ranging from 0.3 kbps to 50 kbps. While this is sufficient for many industrial applications, such as sensor data transmission, it may not be adequate for high-bandwidth applications, such as video streaming or large-scale data analytics or drones and robots in future. The limited data rate can constrain the types of applications that can be effectively deployed on LoRa networks.
- **Scalability Issues:** Although LoRa's star-of-stars topology allows for easy expansion, scalability can become an issue in large-scale deployments. As the number of end devices increases, the network may experience congestion, leading to reduced performance and reliability. Ensuring efficient network management and optimization is crucial to address scalability challenges. The duty cycle limitations imposed by regulatory bodies also restrict the amount of time a device can transmit, further impacting scalability.
- **Security Concerns:** While LoRaWAN incorporates security features such as encryption and authentication, it is not immune to security threats. Industrial environments are often targeted by cyber-attacks, and ensuring the security of wireless communication is paramount. Continuous monitoring and updating of security protocols are necessary to mitigate potential

vulnerabilities. The use of shared frequency bands also increases the risk of eavesdropping and jamming attacks.

- **Power Consumption:** LoRa devices are designed for low power consumption, making them suitable for battery-powered applications. However, managing power consumption is still a significant challenge, especially in industrial environments where devices may be deployed in remote or inaccessible locations. Ensuring long battery life and efficient power management is crucial. Frequent battery replacements or recharging can be impractical and costly, particularly in large-scale deployments.
- **Integration with Existing Infrastructure:** Integrating LoRa with existing wired infrastructure and other wireless technologies can be complex. Ensuring seamless communication and interoperability between different network components requires careful planning and implementation. Compatibility issues and the need for specialized equipment can add to the complexity of integration. The lack of standardized protocols for interoperability with other industrial communication systems can further complicate integration efforts.
- **Latency and Real-Time Communication:** LoRa is designed for low-power, long-range communication, which can result in higher latency compared to other wireless technologies. Industrial processes often require immediate and precise control, and any delay in communication can impact operational efficiency and safety. Ensuring low latency and real-time responsiveness is critical for effective OT network performance. The duty cycle limitations and the use of ALOHA-based channel access mechanisms can contribute to increased latency.
- **Regulatory Constraints:** LoRa operates in the license-free ISM bands, which are subject to regulatory constraints such as duty cycle limitations and power output restrictions. These constraints can impact the performance and scalability of LoRa networks. Compliance with regulatory requirements is essential to ensure legal operation and avoid interference with other wireless systems.

Existing wireless connectivity solutions such as WirelessHART and LoRa effectively serve their intended purposes for low-power sensor networks, but they cannot support high-bandwidth mobile IT devices (tablets, laptops, video systems) or enable OT/IT convergence. To address this gap, I5G networks provide the high-bandwidth, low-latency connectivity required for mobile workers, enterprise applications, and converged OT/IT infrastructure, operating alongside rather than replacing dedicated sensor networks.

IV. IT OT I5G CONNECTIVITY

A. WHAT IS INDUSTRIAL 5G?

Industrial 5G in the United States, and more generally in Industry globally, represents a paradigm shift in wireless networking, offering organizations a dedicated, localized 5G network tailored to their specific needs. Unlike traditional public cellular networks operated by MNOs, a Industrial 5G network is deployed within a defined area, such as a factory, warehouse, or campus, and is either owned and operated by the organization itself or managed by a third-party provider. The example of I5G outdoor AP with sector and omni antenna are shown in Fig. 5 and Fig. 6. This approach allows for unprecedented control over network performance, security, and data localization, empowering businesses and institutions to unlock a wide range of advanced applications and use cases. The cornerstone of many industrial 5G deployments in the U.S. is the Citizens Broadband Radio Service (CBRS) spectrum, operating in the 3.5 GHz band, which offers a flexible licensing model with both shared and licensed access, making it an attractive option for various deployment scenarios.

The benefits of industrial 5G extend across a variety of industries and applications. For industrial and outdoor refinery environments, industrial 5G enables advanced automation, robotics, and remote monitoring, providing the high reliability and low latency communication essential for critical control systems. In refineries and petrochemical settings, it delivers secure and high-performance wireless connectivity for devices on corporate campuses, supporting bandwidth-intensive applications like video conferencing and data sharing. Fig. 7, shows the detail I5G end to end connectivity architecture from UE to AP and then to 5G edge.

Fundamentally, industrial 5G in the U.S. empowers organizations to move beyond the limitations of traditional wireless networks and create customized connectivity solutions that meet their unique requirements. By deploying dedicated 5G networks using CBRS spectrum, businesses and institutions—particularly in safety-critical industries like oil and gas—can achieve greater control over their data, enhance security, improve reliability, and enable secure OT/IT convergence. This self-contained network approach, using organization-controlled hardware, unlocks new opportunities for innovation and growth while maintaining the stringent safety and performance standards required in industrial environments.

B. CURRENT USAGE OF INDUSTRIAL 5G

For years, the oil and gas industry has grappled with significant obstacles in its pursuit of digital transformation, primarily stemming from traditional network limitations. Wi-Fi, while ubiquitous in office settings, falters within sprawling, metal-rich environments like refineries. Its signal struggles to penetrate dense steel structures, demanding a high density of access points that becomes both economically prohibitive and logistically unmanageable—at one Gulf Coast refinery, using Wi-Fi would have required over 300 access points just to cover the distillation unit. Meanwhile, public cellular networks introduce different challenges: inconsistent signal reliability in remote locations, critical data security concerns, and limited control over network performance—where any downtime can translate into millions in lost revenue. The

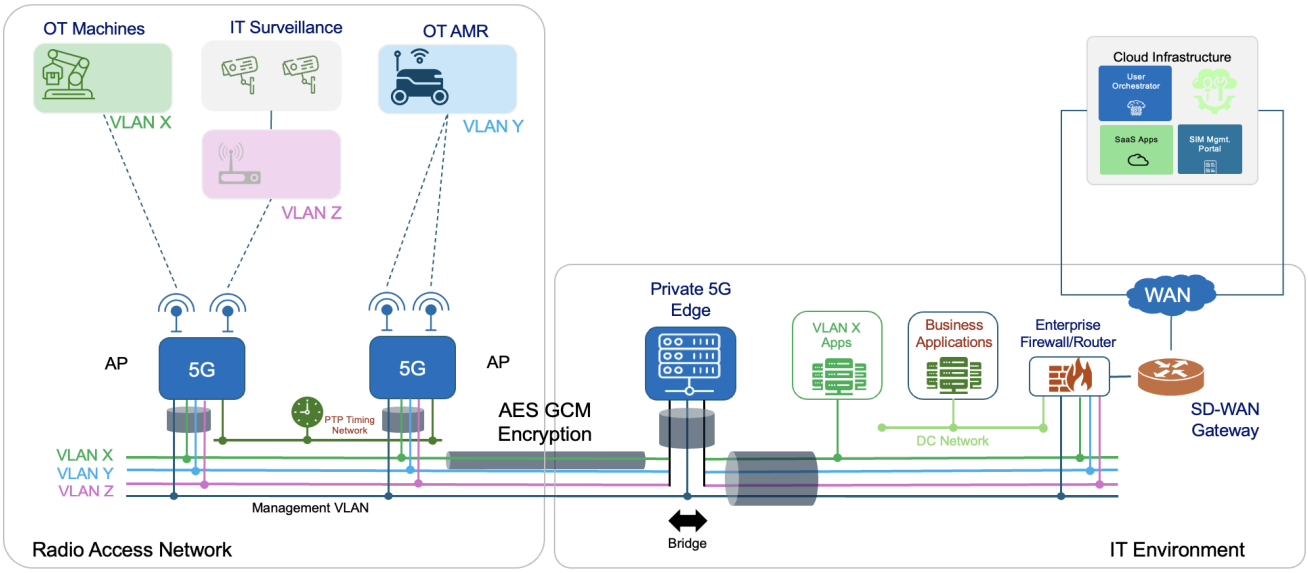


FIGURE 7. Secure encryption for OT/IT traffic - End-to-End I5G architecture.

need to air-gap OT devices also makes many operators wary of deploying wireless solutions, relying heavily instead on costly wired deployments.

The consequences of these connectivity limitations have been far-reaching, slowing down the adoption of advanced technologies and hindering the realization of significant operational efficiencies. Plant operators often remain tethered to inefficient, paper-based workflows, limiting their ability to access real-time data and make informed decisions. Connected worker initiatives, designed to equip personnel with mobile devices for enhanced communication and access to critical information, are much less effective when network coverage is unreliable. Remote monitoring capabilities, essential for ensuring safety and optimizing operations in hazardous environments, are compromised by the inability to deploy sensors and cameras in strategic locations. The potential for fully integrating IoT devices for applications like predictive maintenance, digital twins, and advanced analytics remains largely untapped, preventing facilities from proactively identifying and addressing potential equipment failures or process inefficiencies.

Industrial 5G networks have emerged as a transformative technology [30], poised to resolve many of these long-standing challenges and usher in a new era of digital connectivity for the oil and gas industry. Offering a compelling combination of control and security akin to Wi-Fi with the expansive range and reliability of cellular networks, industrial 5G grants oil and gas facilities unprecedented oversight and management of their connectivity infrastructure. Enterprises gain the ability to dictate Quality of Service (QoS) parameters, ensuring stringent data security protocols, and maintaining seamless connectivity across vast operational areas, all while requiring significantly fewer access points compared to traditional Wi-Fi deployments. This consolidated infrastructure not only reduces costs but also simplifies network management, empowering organizations to prioritize critical communications, tailor security policies to their specific needs, and adapt dynamically to operational demands. Crucially I5G maintains the security isolation that OT networks require through techniques that deliver the benefits of air-gapping without the limitations of physical separation.

The impact of industrial 5G extends far beyond simply improving network coverage and performance; it represents a fundamental shift in how oil and gas operations are conducted. By enabling reliable, high-bandwidth, and secure wireless connectivity, industrial 5G empowers connected workers with access to real-time data, digital work orders, and remote expert support, driving significant reductions in turnaround times and operational costs. It facilitates the deployment of remote monitoring systems in previously inaccessible areas, enhancing safety and security by providing real-time visibility into hazardous environments. Finally, industrial 5G accelerates the integration of IoT devices, enabling advanced applications like predictive maintenance, remote diagnostics, and robotics and automation, transforming operations from reactive to proactive, and enabling a new level of efficiency, safety, and productivity.

C. IT AND OT SEPARATION USING I5G MICRO-SLICING

Micro-Slicing[1] is a remarkable technique used in 5G NR network infrastructure, similar to network slicing [31]. However, it allows more granular and fine-tuned network slices tailored to the needs of specific applications, devices, or users. In sectors such as refineries, manufacturing, energy,

[1]The Micro-slicing technique has been implemented in I5G commercial platform to guarantee the QoS for the end OT and IT user.

warehouses, and logistics, a one-size-fits-all approach is insufficient. Therefore, Micro-Slicing enables each machine, application, or function to receive the exact network service it requires.

In an I5G LAN, Micro-Slicing is a method to create isolated traffic lanes. These lanes are highly customizable and enforce specific network performance guarantees known as Service Level Agreement (SLA) for different applications and user groups. To ensure QoS, each Micro-Slice is assigned a Flow Priority, Packet Delay Budget (PDB), and Packet Error Rate (PER). The end-to-end SLA mapping works by maintaining the network starting from the 5G RAN and through the enterprise's existing Layer 2/Layer 3 infrastructure (switches, routers, firewalls).

Each Micro-Slice is logically isolated and does not interfere with or access other traffic, increasing security. In case of congestion, the system dynamically prioritizes important traffic, ensuring reliable performance without any manual intervention. To enhance security, each traffic flow is individually data-encrypted. Furthermore, as traffic transitions from the 5G RAN to the enterprise LAN, it can be redirected to a secure network segment, such as a DMZ. The micro-slices are implemented as QoS flows within the PDU session of 5G NR 3GPP protocol stack. Its implemented both at the 5G core and the AP. QoS flows and traffic filters are configured on the Edge (5G core), UE, and AP.

1) MICRO-SLICING BEARER CHANNELS

Micro-Slicing uses the concept of bearer channels, which are logical paths in a network that are responsible for transporting data with specific QoS characteristics. There are three types of Micro-Slice bearer channels in I5G:

- Guaranteed bit rate (GBR) – Ensures a minimum bandwidth for apps that need consistent throughput. We can add extra bandwidth if available, and can set the GBR channel type for Video surveillance, voice calls, and sensor feeds.
- Non-guaranteed bit rate (Non-GBR) - No minimum rate guarantee. Enterprises use it for less sensitive or best-effort traffic. For File transfers and background updates, set Non-GBR channel type.
- Delay-Critical Guaranteed bit rate (GBR) – Critical GBR Combines GBR with ultra-low latency (as low as 5 ms), where timing is critical and set the delay critical GBR type for Real-time IIoT systems and robotic control.

2) PRIORITIZING AND ENFORCING MICRO-SLICES

While choosing a bearer type sets the framework for the Micro-Slice, the next step is to choose the QoS Class Identifiers (QCI) and 5G QoS Identifiers (5QI) which define how that slice behaves under congestion. These are predefined QoS templates (from 3GPP TS 23.203 standards). Each QCI and 5QI defines:

- Priority level: Lower Number = Higher Priority, for example, 1 has higher priority than 4.
- Packet Delay Budget (PDB): Defines the maximum acceptable delay for delivering packets. For instance, if traffic is assigned a QCI with a 100 ms PDB, the system must deliver each packet within that time frame. If it cannot, it may begin discarding lower-priority packets to meet the SLA.
- Packet Error Rate (PER): Specifies the acceptable packet loss rate. The ratio of failed to deliver packets and the total number of packets sent is represented using PER. For example, a PER of 10^2 allows for 1 packet to be lost for every 100 transmitted.

With 5G NR, additional QoS Identifiers (5QIs) are defined which can support much lower latency values, but similar mechanism is utilised by the QoS scheduler. Based on the IT and OT device, the private 5G LAN gives administrators the opportunity to create virtual Micro-Slices at a highly-granular level when compared to carrier 5G network slicing options. From a per-application perspective, Micro-Slicing is one of the only ways to provide strict, SLA-backed traffic flow guarantees across a wireless medium that can be directly integrated with the existing enterprise QoS framework already in place. The I5G solution creates a more granular approach by allowing administrators to organize their RAN by application and device group:

- *Device groups* – Administrators can place 5G endpoints that connect to the RAN via SIM card or eSIM into groups to logically segment them by device type. In many cases, the type of device often dictates what apps/services are being operated on a regular basis. This helps to coordinate which devices are assigned to a specific Micro-Slice.
- *Applications* – Applications can be configured within the I5G platform so that the control plane can identify the data flow being transmitted across the RAN. Once the application is identified by the I5G platform, the flow can be assigned to the appropriate Micro-Slice and associated network performance SLAs.

The QCI values, as shown in Table 2, indicate several 3GPP standardized settings for classes 1-9 for I5G operation. For most Industrial 5G (I5G) use cases, administrators primarily work with QCI values 1 through 9, which cover a wide range of common IT and OT traffic flows. QCI 1 to 4 serves for GBR bearers, typically used for latency-sensitive or mission-critical applications like real-time control or VoIP. In contrast, QCI 5 to 9 serves for Non-GBR bearers, supporting best-effort or background applications like file transfers and email.

These parameters enable precise enforcement of Micro-Slice behavior, ensuring that critical industrial applications maintain performance even under network congestion. While 5G NR introduces additional 5QI options for more advanced use cases, the fundamental approach to QoS enforcement remains similar. In most I5G LAN scenarios, the existing

TABLE 2. QCI parameters proposed by 3GPP.

QCI	Bearer Type	Priority Level	Packet Delay Budget (PDB)	Packet Error Rate (PER)	Example Services
1	GBR	2	100ms	10^{-2}	Conversational Voice
2	GBR	4	150ms	10^{-3}	Conversational Video (Live Streaming)
3	GBR	3	50ms	10^{-3}	Real Time Gaming
4	GBR	5	300ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
5	Non-GBR	1	100ms	10^{-6}	IMS Signalling
6	Non-GBR	6	300ms	10^{-6}	Video (Buffered Streaming)
7	Non-GBR	7	100ms	10^{-3}	Voice, video, gaming
8	Non-GBR	8	300ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing)
9	Non-GBR	9	300ms	10^{-6}	File sharing, progressive video, etc.

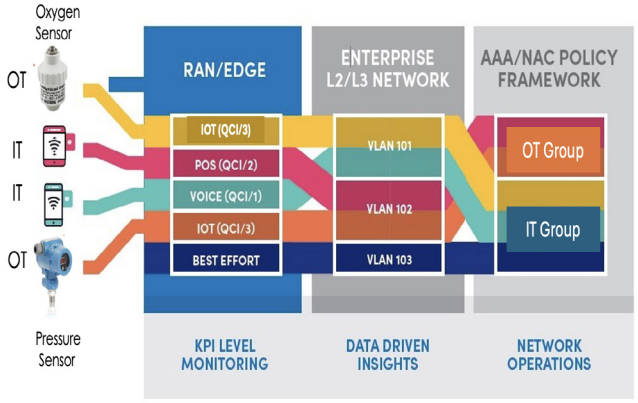


FIGURE 8. Micro-slicing for I5G -OT/IT.

QCI-based framework is sufficient to support the majority of enterprise and industrial traffic flows.

The diagram in Fig. 8 illustrates the operation of an I5G LAN configured with three distinct Micro-Slices, each aligned with a specific service category: 1) Oxygen Sensor (OT), 2) Pressure Sensor (OT), and 3) general IT Devices. Each Micro-Slice has a priority level, which tells the network which traffic is most important. If the network becomes too busy—causing delays or packet loss—the Micro-Slice with the lowest priority gets affected first. In this case, the IT Micro-Slice would be delayed before the OT Micro-Slices, so that critical sensor data can keep flowing without interruption.

This setup is very different from the typical 5G network slicing used by mobile carriers. Mobile operators use network slicing to offer different ''virtual'' networks to their business customers, each with different levels of speed, reliability, or security. However, those slices treat all traffic from that customer the same—regardless of whether it is a video call, a database update, or a sensor alert. That approach is not suitable enough for factories or other enterprise environments, where some applications (like safety monitoring) need much more reliable and fast communication than others (like email or file transfers). In most cases, 5G operators create and manage network slices on a use case basis [32], e.g. Fixed Wireless or Ultra-Reliable Low Latency use cases. This means that all customer traffic traversing a public 5G network slice will receive identical QoS service levels regardless of the type of application or service that is being transmitted across the RAN. The detail difference between Micro-slicing and network slicing is described in Table 3.

Also, managing all those slices across a nationwide network would be very complicated for carriers. While network slicing at a customer-level may be sufficient for certain wireless use cases, most enterprise organizations are seeking ways to better optimize and guarantee traffic flows and specific rates for mission critical business applications and services. In the 3GPP standards support up to 256 different S-NSSAI (Single Network Slice Selection Assistance Information) combinations per Mobile Network. But the practical reality is much lower. Most public 5G operators deploy 3-4 slices in a given market. It's typically limited RAN resource constraints since slices share the same physical spectrum and each slice consumes RAN capacity (resource blocks) and network functions (UPF, SMF, AMF, etc.) so more slices is equal to more overhead, less efficiency, while orchestration complexity grows exponentially. Hence, the network slicing simply cannot achieve as it would become too complex and cumbersome to manage this number of slices across a nationwide 5G infrastructure. That is where I5G Micro-Slicing stands out. It gives the business full control over how to handle the traffic inside its private 5G network. Instead of slicing traffic by customer, Micro-Slicing slices traffic by application or device type. It allows administrators to group devices (like sensors or laptops) and assign them specific traffic rules. So that the network can recognize the kind of sent data, apply the right Micro-Slice, and enforce performance guarantees like speed, delay limits, or reliability. The result is a smart, flexible network where important traffic is always prioritized—even during congestion—while less critical traffic waits its turn. The above advantages of micro-slicing and proposed 3GPP of 5QIs allows the I5G system to acheive reliably and consistently the latency metrics across IT and OT devices.

D. HOW OT AND IT SEPARATION USING I5G WORKS WITH IN SINGLE AP

Achieving OT/IT separation on shared radio infrastructure requires end-to-end encryption from UE through the AP to the Edge. In our solution, each device is designated as either

TABLE 3. Comparison between micro-slicing and 3GPP network slicing.

Aspect	Micro-Slicing	3GPP Network Slicing
Definition	A properatory-specific feature that enables per-application or per-device traffic policy enforcement within a single private 4G/5G network.	A 3GPP-defined mechanism for creating multiple logical networks (slices) on a shared public or private 5G infrastructure.
Scope	Operates at the enterprise/private network level within the edge platform.	Operates across the entire 5G system (core, transport, and RAN), often managed by a mobile network operator (MNO).
Implementation Layer	Implemented in the private 5G Edge and Orchestrator using QoS, policy control, and traffic steering.	Implemented at the 5G system architecture level (AMF, SMF, UPF, etc.) following 3GPP specifications.
Granularity	Fine-grained — can apply unique QoS, priority, and rate limits to specific applications, devices, or traffic flows.	Coarse-grained — typically defines broad service categories like eMBB, URLLC, or mMTC.
Configuration Complexity	Simple and automated through I5G Orchestrator UI or API.	Complex and requires coordination between network domains and operators.
Use Case Focus	Enterprise use cases such as video surveillance, AGV control, and voice prioritization in private LTE/5G networks.	Operator-grade use cases such as differentiating consumer, enterprise, or IoT services across wide-area 5G networks.
End-to-End Isolation	Logical traffic separation and QoS enforcement within the enterprise network; shares the same physical network.	Full logical and sometimes physical separation across core, transport, and RAN resources.
Standardization	Proprietary to Celona, built on top of 3GPP QoS mechanisms.	Defined by 3GPP (TS 23.501, 23.502, 28.530, etc.).
Deployment Environment	Private/enterprise 4G and 5G LANs managed by I5G Edge.	Public 5G networks or large-scale private 5G deployments managed by MNOs.
Goal	Optimize enterprise application performance and reliability with minimal configuration.	Enable multiple virtual networks with different service characteristics over a shared 5G infrastructure.

IT or OT, with traffic encrypted using unique eNB/gNB keys derived per UE.

To prevent IT and OT devices from sharing IPSec tunnels—a critical security vulnerability, each GTP tunnel is individually encrypted. This approach works as follows: When a PDU session is created, the I5G edge generates a random symmetric key, encrypts it with a pre-shared key known to the AP, and forwards it within the cNGAP UE Context Setup Request. The same key is simultaneously shared with the User Plane Function (UPF) via the PFCP Session Modification message.

The AP uses this unique key to encrypt GTP payloads, while the UPF performs the corresponding decryption (or vice versa). AES-GCM encryption (as shown in Fig. 7) is used with per-packet sequence numbers to prevent replay attacks and MAC/hash validation to detect tampering. Key rotation occurs automatically during handovers and service requests, leveraging existing NGAP and PFCP message flows for seamless security updates without additional overhead.

In OT/IT deployments, devices connecting through Customer Premises Equipment (CPEs) via Wi-Fi or Ethernet require network segmentation using separate subnets—typically one for IT and another for OT. However, a critical limitation exists: wired traffic behind the CPE remains unencrypted, potentially exposing sensitive data. For enhanced separation, organizations can deploy multiple UPF instances[2] dedicated to IT and OT traffic respectively. While this approach provides stronger conceptual isolation, it requires additional IP address allocation, which may impact customers with limited address space. Alternatively, a single UPF instance can still maintain effective separation by implementing distinct route tables per VLAN and per port, offering a more address-efficient solution while preserving security boundaries.

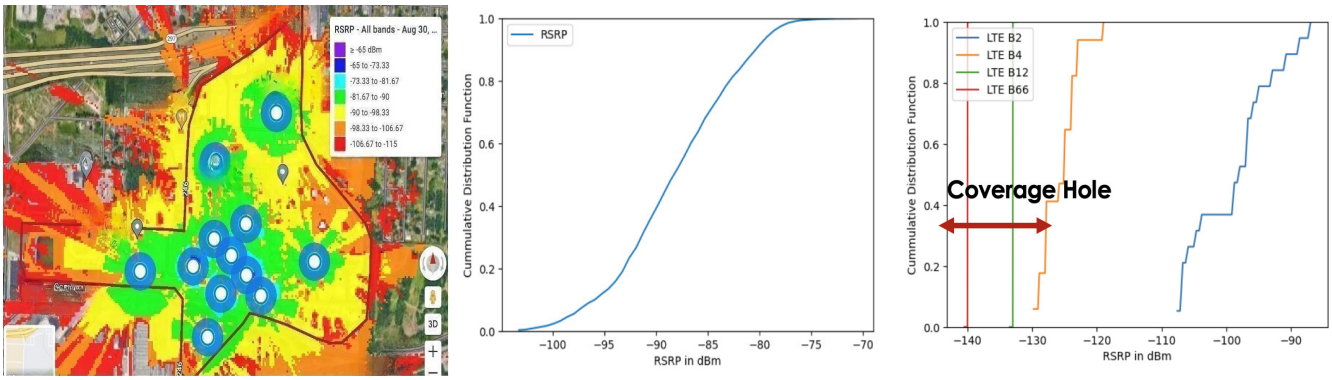
E. BENEFITS OF USING IT OT IN I5G NETWORKS

Industrial 5G networks are becoming vital for Industrial IoT (IIoT), enhancing connectivity and reliability. Securing networks in complex industrial OT/IT environments is challenging due to strict latency requirements, devices that cannot run security agents, and the separation between IT and OT networks. We propose a zero-trust architecture that addresses these challenges through three key technical innovations: SIM-based authentication for agentless devices, dynamic policy enforcement at the network edge, and Micro-Slicing-based traffic isolation. This architecture maintains the deterministic latency requirements of OT systems while providing the security controls necessary for OT/IT convergence on shared infrastructure.[3]

SIM-based Authentication with Unified Zero Trust Enforcement for IT and OT devices eliminates the need for device-side software or agents. Our open API approach provides native integration with best-in-class security services, such as firewalls, network access control (NAC) systems, and SD-WAN solutions, and is agnostic to their deployment

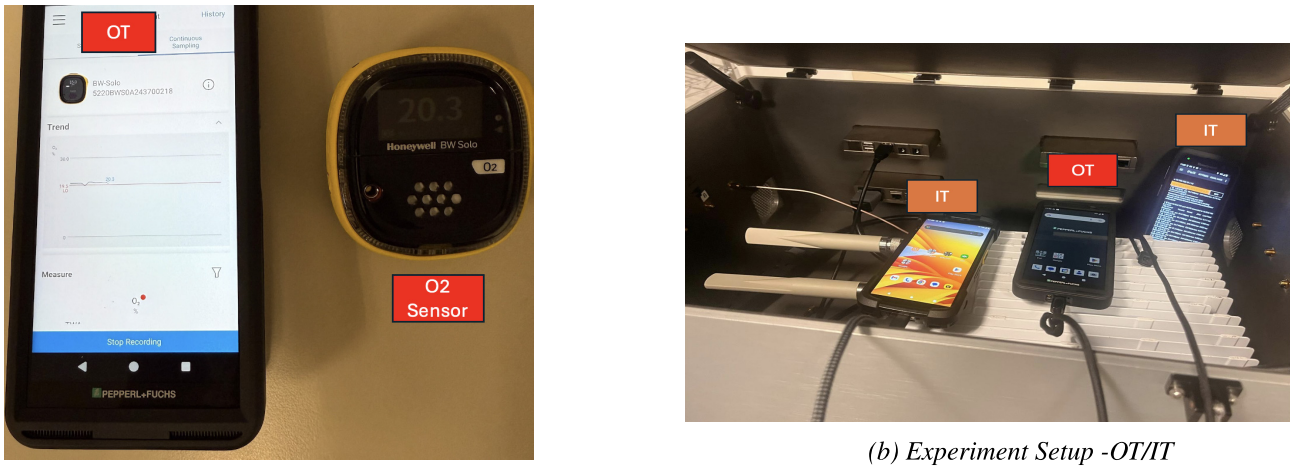
[2]The User Data Plane Function (UPF) leverages the Data Plane Development Kit (DPDK) to achieve high-performance packet processing by providing direct access to the Network Interface Card (NIC), thereby bypassing the traditional Linux operating system and TCP/IP stack. This architecture signif- icantly enhances throughput—by roughly an order of magnitude compared to the Linux stack—and provides greater flexibility by enabling support for Layer 2 features such as bridging and tunneling.

[3]The architecture and techniques presented have been implemented in I5G commercial platform under the Aerloc feature set, with deployments in multiple industrial facilities validating the approach.



(a) I5G Coverage - Refinery *(b) RSRP Distribution – I5G* *(c) RSRP Distribution – MNO*

FIGURE 9. **Coverage distribution in dense deployment and entire refinery regions.**



(a) OT Device - O2 Sensor *(b) Experiment Setup -OT/IT*

FIGURE 10. **Refinery coverage and experiment deployment setup.**

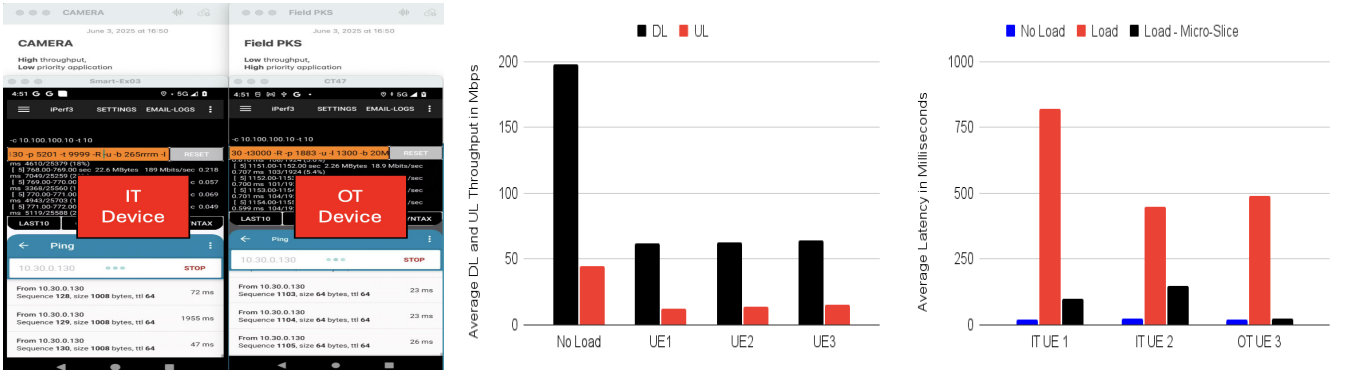
– whether in the cloud, on-premises or in a hybrid setup. Our Aerloc integrates with other leading enterprise security solutions, including Palo Alto Networks Cortex XSOAR and Next Generation Firewall (NGFW), Network Access Control (NAC) such as Cisco ISE, and Aruba ClearPass.[4] Our solution continues to integrate with other top-tier security vendors through its open API framework to meet evolving enterprise needs.

Dynamic and Distributed Policy Enforcement to integrate with posture assessment tools, IoT security solutions, and security orchestration automation platforms. Aerloc provides a collaborative security architecture enabling localized and responsive security policy enforcement at a granular level—down to the individual device or user – and at the very edge of the network to significantly reduce the attack surface.

Air Gap Between OT and IT Traffic using our Micro-Slicing technology. IT and OT traffic can be securely segmented both physically and logically over the air, on the LAN and within the shared 5G LAN network. This unique intent-based segmentation of IT and OT traffic ensures the separation of critical operational data from general enterprise traffic to maintain security and performance integrity across both environments.

Role Based Access Control (RBAC) for OT/IT – The goal is to establish separate IT and OT roles to achieve isolation in terms of configuration and monitoring on the management system. Our proposed solution involves physically connecting the IT and OT interfaces to separate Ethernet ports (ETH 1 for IT and ETH 2 for OT). This setup ensures that any actions related to ETH port 2 can only be performed by the ''OT Admin'', while actions related to ETH port 1 can only be performed by the ''IT Admin''. Consequently, the IT admin will not have visibility into the external network domains created by the OT admins or the devices assigned to those network domains.

[4]Following successful SIM authentication, the I5G Edge issues an authorization request to the enterprise NAC platform using device identifiers to retrieve the corresponding policy. The NAC system returns the authorization profile, which I5G Edge applies dynamically during device onboarding. In the first phase of the implementation, the system automatically assigns the appropriate device group and configures the associated networking and security parameters on the private network. These include QoS enforcement, admission control rules, and IP/VLAN segmentation, ensuring policy-driven, scalable, and secure device operation across the entire enterprise environment.



(a) OT/IT with & without Micro-slice *(b) Average Throughput (Mbps)* *(c) Average Latency (ms)*

FIGURE 11. Throughput performance and average latency.

TABLE 4. I5G OT/IT experiment parameters.

Parameter	Value
Number of APs	12
Number of Bandwidth per AP	40 MHz
Operating Band	48
Operating Frequency	3570, 3630, 3650, 3690
Channel Selection	SAS
Micro-Slicing	Enabled
MIMO	2 x 2
Carrier Aggregation	Enabled
Spectrum	CBRS
Tools	QPOC, Ipref and Ping

The convergence of OT and IT networks in Industrial 5G deployments requires rethinking traditional security architectures. The proposed architecture demonstrates that cryptographic traffic isolation, combined with SIM-based authentication and distributed policy enforcement, can deliver the low-latency communication (10-20ms one-way) required for industrial applications while maintaining the security boundaries critical to operational cybersecurity. Field deployments in multiple refineries, petrochemical and chemical processing facilities confirm that this architecture enables unified OT/IT network infrastructure while maintaining the deterministic latency and isolation required for critical control systems.

V. OT/IT EXPERIMENT ENVIRONMENT AND CONFIGURATION

In this section, we discuss the Industrial 5G deployment setup and the performance of the IT and OT system with respect to throughput and latency.

A. COVERAGE

In this sub-section, we show the coverage of the commercial refinery location site, where 12 industrial 5G radios are deployed to cover approximately 7.9 million square feet (181 acres). Coverage validation was performed using QPOC and NSG RF analysis tools to ensure no dead zones exist within the operational area. As shown in Fig. 9 (a), RSRP measurements confirm adequate signal strength throughout the facility, including traditionally problematic areas such as pipe alleys and tank farms where metallic structures typically cause signal shadowing. The deployment parameters are summarized in Table 4.

Fig. 9 (b) shows the RSRP distribution of the entire plant, which indicates no coverage hole on the network, also 99% of the users are in the high throughput covergae region. Table 4 shows the deployment parameters used in this refinery location to enable the network. Similarly, Fig. 9 (c) shows the RSRP distribution of the MNO coverage. As the deployment in the rural area, we observed only 4G LTE and not 5G NR. The 4G bands B2, 4, 12 and 66, have poor coverage. Hence, its challenging to enable the OT network on the un-reliable connection.

B. IT OT EXPERIMENT SETUP

In this experiment setup, we configured one AP in our HQ test network connected to the I5G edge server via switch and router. The router was configured to provide DHCP services, automatically assigning IP addresses to connected devices (UEs, AP, and Edge). The radio is placed in the RF shield box to ensure the control test environment. The AP operated with 40 MHz bandwidth using the CBRS spectrum grant (Band n48) allocated by Spectrum Access System (SAS). The SAS is responsible for the channel allocation, transmission power, and bandwidth for the I5G AP or radio. The professional signal tool QPOC is used to measure the throughput, and latency. The script based campaign on QPOC are executed to measure the performance.

The test configuration included an OT device (O2 sensor, shown in Fig. 10(a)) and two IT devices: Zebra TC26 and Honeywell CT47 (shown in Fig. 10(b)). These IT devices represent high-throughput users, simulating bandwidth-intensive applications such as surveillance cameras commonly deployed in refineries. Dedicated network slices were configured at the orchestrator using port-based

classification to guarantee QoS for the OT device. This dedicated network slicing capability is implemented in our I5G platform as the Micro-Slicing feature.

C. THROUGHPUT PERFORMANCE

In this experiment, we used the iPerf tool to record all the throughput performance. The iPerf server runs on the industrial network edge in the test network, which avoids any additional back-haul delay added by the network. We used TCP traffic with a parallel stream of 15 to mimic the behavior of multiple users in the network. We started our experiment with a single UE to understand the full potential of downlink and uplink performance. Then, in the next step, we added three devices to understand the fairness and load sharing of radio resources among the devices. Fig. 11 (b) shows the average downlink (DL) and uplink (UL) throughput performance for a single UE and multiple UEs on the network. We expected the average throughput to be close to 200 Mbps. Also, we noticed that when the load increased from one to three UEs, the resource blocks were fairly shared among the devices. This is mainly due to the cellular scheduling algorithm allocating the slots efficiently.

Similarly the average UL throughput exhibited comparable behaviour. In the single UE case, the average uplink performance achieved was 46 Mbps, and when the load increased from one to three devices, we noticed that similar to downlink, the resource block allocations were fairly scheduled by the scheduling algorithm. Compared to other technologies evaluated in this paper, LoRa's limited throughput (50 Kbps maximum) cannot support high-bandwidth applications, while Wi-Fi lacks the reliability required for industrial environments. This performance gap becomes critical as emerging OT applications, including autonomous drones, AI-enabled robots, and real-time video analytics, demand substantially more bandwidth than traditional sensors. Industrial 5G uniquely combines high throughput with extensive coverage, enabling these next-generation applications without compromising the reliability essential for critical OT operations.

D. IT AND OT LATENCY PERFORMANCE

Fig. 11 (a) shows the latency observed on the IT and OT devices when the network is fully loaded. With the dedicated network slice enabled on the OT device, its latency remains within the expected threshold. Similarly, Fig. 11 (c) shows the average latency under no-load and loaded scenarios for both IT and OT devices. Under no-load conditions, both device types maintain minimal latency, averaging 25 ms. However, in the loaded scenario with full buffer traffic in both DL and UL, latency increases significantly for all devices. After enabling the dedicated network slice on the OT and OT device, its latency remains low even under load, comparable to the no-load scenario.

Hence, ensuring good coverage, throughput and latency, which fundamentally support reliable and deterministic networks.

VI. PROPOSED FRAMEWORK BE GENERALIZED BEYOND REFINERIES AND PETROCHEMICAL PLANTS

The same enterprise framework is applicable for other Industrial sectors such as chemical processing, pharmaceutical processing, automotive manufacturing and warehousing logistics markets for their IT and OT use-cases.

IT and OT devices together enable seamless integration between the digital and physical worlds across industries such as manufacturing, automation, healthcare, logistics, and distribution. IT encompasses systems for storing, processing, and analyzing data—such as servers, databases, cloud platforms, and enterprise applications like ERP and MES. OT includes hardware and software systems that directly monitor and control physical processes—such as sensors, actuators, PLCs, and SCADA systems. The convergence of IT and OT, often driven by Industrial IoT (IIoT), allows organizations to collect and analyze operational data for improved visibility, efficiency, and automation.

In manufacturing and automation, key OT devices include PLCs, industrial PCs, edge gateways, HMIs, and various industrial sensors. These systems control machinery and collect data, which are then shared with IT platforms for analytics and predictive maintenance. Reliable connectivity and precise time synchronization are critical in these environments. In logistics and distribution centers, OT devices such as autonomous mobile robots (AMRs), automated guided vehicles (AGVs), barcode/RFID scanners, and environmental sensors help track goods, optimize routes, and ensure real-time inventory management. These devices interface with IT systems to support warehouse management and supply chain analytics.

I5G cellular network offers a plug-and-play deployment model designed for rapid, secure, and automated setup in enterprise environments. Once powered and connected to the local network, I5G radios automatically connect to the Orchestrator, download their configurations, and begin broadcasting the I5G cellular signal—without any manual tuning or complex setup. This zero-touch provisioning simplifies the deployment of I5G networks and ensures seamless integration with existing enterprise LAN, DHCP, DNS, and NTP systems.

In manufacturing, plug-and-play deployment enables reliable connectivity for robotics, sensors, (OT) and handheld devices (IT) across factory floors where Wi-Fi often struggles with interference and mobility. Devices such as AGVs and quality inspection tablets can stay connected throughout production zones with predictable latency and throughput. In petrochemical and energy facilities, I5G plug-and-play network supports safe, secure, and resilient communications across large outdoor areas. Rugged outdoor APs can be installed in hazardous or remote environments to provide connectivity for field instruments (IT), worker safety systems (IT), and monitoring sensors—without disrupting existing control networks (OT).

Across all these industries, I5G plug-and-play private network delivers fast deployment, effortless scaling, and predictable performance—making it ideal for digital transformation initiatives where reliability, security, and low latency are essential.

VII. CONCLUSION

This paper provided a comprehensive overview and comparative analysis of wireless technologies for industrial applications, with detailed examination of wired networks, Wi-Fi, public cellular (MNO), and Industrial 5G (I5G) architectures. The paper presented an I5G architecture for secure OT/IT convergence in industrial environments, specifically targeting oil and gas refinery and petrochemical applications. The proposed Micro-Slicing approach enables per-application traffic isolation while maintaining deterministic latency requirements for critical control systems.

The key contributions include:

- Per-GTP-tunnel encryption architecture enabling secure OT/IT traffic separation without physical air-gapping (Section D).
- Granular QoS enforcement framework through Micro-Slicing supporting QCI classes 1-9 for diverse industrial applications (Section C).
- Deployment architecture for 40 MHz CBRS spectrum supporting isolated traffic flows within single access points (AP) (Section D).

Technology selection analysis and deployment experience demonstrate that I5G architectures offer distinct advantages for industrial environments: coverage efficiency (fewer access points required in metal-dense refinery environments, seamless mobility management, and enhanced security isolation.

The I5G architecture for OT/IT convergence provides a framework for next-generation industrial automation, enabling applications including predictive maintenance, digital twins, and autonomous mobile robotics in safety-critical environments.

VIII. FUTURE DIRECTION

There are some future research directions which include:

- Extending Micro-Slicing granularity to support sub-5ms ultra-low latency applications through dynamic resource allocation optimization.
- Integrating AI-driven network orchestration for predictive traffic management and autonomous slice provisioning based on real-time operational patterns.
- Validating interoperability of I5G Micro-Slicing architecture with legacy industrial protocols (Modbus, PROFINET, EtherNet/IP) to enable gradual OT modernization.
- Developing enhanced threat detection mechanisms leveraging per-GTP-tunnel traffic pattern analysis for zero-trust security architectures, and
- Extending deployment validation across additional industrial sectors including manufacturing, pharmaceuticals, and critical infrastructure to establish generalized I5G design patterns for diverse OT/IT convergence scenarios.

REFERENCES

[1] C. Williamson, "Internet traffic measurement," *IEEE Internet Comput.*, vol. 5, no. 6, pp. 70–74, Jun. 2001.

[2] G. Murray, M. N. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," in *Proc. 15th Austral. Inf. Secur. Manage. Conf.*, C. Valli, Ed., Perth, WA, USA: Edith Cowan Univ., Dec. 2017, pp. 149–155.

[3] S. Kumar and H. Vardhan, "Cyber security of OT networks: A tutorial and overview," 2025, *arXiv:2502.14017*.

[4] N. H. Ghoson, K. Benfriha, V. Meyrueis, T. Guiltat, and C. El Zant, "ShieldFlow: A novel framework for OT cybersecurity in the context of industry 4.0," *Int. J. Inf. Secur.*, vol. 24, no. 4, pp. 1–22, Aug. 2025.

[5] P. Danielis, H. Puttnies, E. Schweissguth, and D. Timmermann, "Real-time capable internet technologies for wired communication in the industrial IoT–A survey," in *Proc. IEEE 23rd Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 1, Sep. 2018, pp. 266–273.

[6] L. Muguira, J. Lázaro, S. Alonso, A. Astarloa, and M. Rodriguez, "Secure critical traffic of the electric sector over time-sensitive networking," in *Proc. 35th Conf. Design Circuits Integr. Syst. (DCIS)*, Nov. 2020, pp. 1–6.

[7] B. Sliwa and C. Wietfeld, "Empirical analysis of client-based network quality prediction in vehicular multi-MNO networks," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–7.

[8] F. Marzouk, A. Radwan, H. R. Chi, and J. P. Barraca, "Highly flexible and traffic isolating RAN slicing: A consumer IoT-based use case," *IEEE Trans. Consum. Electron.*, vol. 69, no. 4, pp. 709–718, Nov. 2023.

[9] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," *IEEE Access*, vol. 7, pp. 127639–127651, 2019.

[10] R. K. Saha, S. Nanba, K. Nishimura, Y.-B. Kim, and K. Yamazaki, "RAN architectural evolution framework toward 5G and beyond cellular—An overview," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2018, pp. 592–593.

[11] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. C. Zhang, "Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 212–217, Apr. 2020.

[12] R. Askar, J. Chung, Z. Guo, H. Ko, W. Keusgen, and T. Haustein, "Interference handling challenges toward full duplex evolution in 5G and beyond cellular networks," *IEEE Wireless Commun.*, vol. 28, no. 1, pp. 51–59, Feb. 2021.

[13] N. Führling, I. A. M. Sandoval, and G. T. F. de Abreu, "A robust routing protocol for 5G mesh networks," 2025, *arXiv:2503.15173*.

[14] D. Xenakis, A. Tsiota, C.-T. Koulis, C. Xenakis, and N. Passas, "Contractless mobile data access beyond 5G: Fully-decentralized, high-throughput and anonymous asset trading over the blockchain," *IEEE Access*, vol. 9, pp. 73963–74016, 2021.

[15] P. Muñoz, O. Sallent, and J. Pérez-Romero, "Self-dimensioning and planning of small cell capacity in multitenant 5G networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4552–4564, May 2018.

[16] X. P. Sebastiao, R. R. de Oliveira, W. Moreira, and A. Oliveira-Jr., "Channel-aware federated analytics in B5G/6G networks: Dynamic power allocation with NS-3 5G-lena," in *Proc. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), pp. 826–839, 2025.*, 2025, pp. 826–839.

[17] U. Paul, J. Liu, S. Troia, O. Falowo, and G. Maier, "Traffic-profile and machine learning based regional data center design and operation for 5G network," *J. Commun. Netw.*, vol. 21, no. 6, pp. 569–583, Dec. 2019.

[18] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle, "When HART goes wireless: Understanding and implementing the WirelessHART standard," in *Proc. IEEE Int. Conf. Emerg. Technol. Factory Autom.*, Sep. 2008, pp. 899–907.

[19] S. M. Hassan, R. Ibrahim, K. Bingi, T. D. Chung, and N. Saad, "Application of wireless technology for control: A WirelessHART perspective," *Proc. Comput. Sci.*, vol. 105, pp. 240–247, Feb. 2017.

[20] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "WirelessHART: Applying wireless technology in real-time industrial process control," in *Proc. IEEE Real-Time Embedded Technol. Appl. Symp.*, Apr. 2008, pp. 377–386.
[21] M. Kostadinovic, D. Dobrilovic, G. Jausevac, G. Jotanovic, Z. Stojanov, and V. Brtka, "Performance investigation of WirelessHART in the coexistence with Wi-Fi networks," *Mobile Netw. Appl.*, vol. 28, no. 3, pp. 1116–1125, Jun. 2023.
[22] D. Yang, Y. Xu, and M. Gidlund, "Coexistence of IEEE 802.15.4 based networks: A survey," in *Proc. 36th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Nov. 2010, pp. 2107–2113.
[23] S. Raza and T. Voigt, "Interconnecting WirelessHART and legacy HART networks," in *Proc. 6th IEEE Int. Conf. Distrib. Comput. Sensor Syst. Workshops (DCOSSW)*, Jun. 2010, pp. 1–8.
[24] C. Li and Z. Cao, "LoRa networking techniques for large-scale and long-term IoT: A down-to-top survey," *ACM Comput. Surv. (CSUR)*, vol. 55, no. 3, pp. 1–36, 2022.
[25] J. P. S. Sundaram, W. Du, and Z. Zhao, "A survey on LoRa networking: Research problems, current solutions, and open issues," *IEEE Commun. Surv. Tut.*, vol. 22, no. 1, pp. 371–388, 1st Quart., 2020.
[26] S. Devalal and A. Karthikeyan, "LoRa technology—An overview," in *Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Mar. 2018, pp. 284–290.
[27] A. I. Petrariu, A. Lavric, and E. Coca, "LoRaWAN gateway: Design, implementation and testing in real environment," in *Proc. IEEE 25th Int. Symp. Design Technol. Electron. Packag. (SIITME)*, Oct. 2019, pp. 49–53.
[28] Z. Lin, Z. Huang, B. Gu, S. Gong, Z. Su, and M. Guizani, "CORA: Channel occupancy-aware resource allocation in LoRa wireless networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 11, pp. 17083–17094, Nov. 2024.
[29] C. Chen, J. Luo, Z. Xu, R. Xiong, D. Shen, and Z. Yin, "Enabling large-scale low-power LoRa data transmission via multiple mobile LoRa gateways," *Comput. Netw.*, vol. 237, Dec. 2023, Art. no. 110083.
[30] V. Sathya, E. Savage, and M. Yavuz, "A measurement of commercial outdoor private network deployment in refinery industry," in *Proc. IEEE 100th Veh. Technol. Conf. (VTC-Fall)*, Oct. 2024, pp. 1–7.
[31] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019.
[32] M. Pozza, P. K. Nicholson, D. F. Lugones, A. Rao, H. Flinck, and S. Tarkoma, "On reconfiguring 5G network slices," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 7, pp. 1542–1554, Jul. 2020.

VANLIN SATHYA received the B.E. degree in computer science and the M.E. degree in mobile and pervasive computing from Anna University, Chennai, India, in 2009 and 2011, respectively, and the Ph.D. degree in computer science and engineering from Indian Institute of Technology Hyderabad, India, in 2016. He is currently the Director of Research and Solutions Innovation, Celona Inc., USA. He is an Expert in wireless communications and network technologies, with a focus on next-generation connectivity solutions. In the past, he was a Senior Research Member with the CTO Group, Celona Inc. Previously, he was a Postdoctoral Scholar with The University of Chicago, focusing on 5G and LTE-Wi-Fi coexistence. He published more than 100 research articles in the top journal and conferences. He has contributed to advancements in private 5G, Wi-Fi innovations, and spectrum management, working closely with industry and academic institutions to improve network performance, reliability, and security. He Celona's work emphasizes the integration of emerging wireless standards to support mission-critical applications across diverse sectors, such as healthcare, manufacturing, and logistics. His expertise and research have garnered recognition within the telecommunications community, making him a leading voice in the evolution of wireless networks. His research interests include interference management, LTE networks, device-to-device communication, and private 5G networks.

STEVE TOTEDA received the B.S. and M.S. degrees in engineering from Lehigh University and the M.B.A. degree from UC Berkeley. He is currently an strategic Advisor and an Industry Consultant, with a specializing in edge AI computing and private wireless networking for telecommunications and industrial applications. Over his 25-year career, he has led go-to-market strategies across optical transport, microwave and millimeter wave systems, VoIP, and industrial wireless technologies—including the productization of WirelessHART and ISA100. He has held leadership roles at Harmonic, Cisco, and Aviat Networks, serves as an Advisor to the R42 venture fund. His current focus encompasses private 5G deployments, the industrial IoT architectures, and edge AI infrastructure for mission-critical industrial environments.

RAJEEV SHAH is currently the Chief Executive Officer and the Co-Founder of Celona, where he leads the development and deployment of enterprise-focused private cellular network solutions. He has over two decades of experience in wireless networking, spanning product development, systems engineering, and business leadership. Prior to founding Celona, he held senior product management and engineering roles at Aruba Networks, where he was instrumental in advancing enterprise Wi-Fi and cloud-managed networking technologies. His work focuses on bridging cellular and enterprise networking domains to enable secure, reliable, and scalable connectivity for mission-critical applications across industries.