WHITE PAPER

The IT/OT Engineer's Playbook:

Deploying Private Wireless Networks for Oil Refineries and Petrochemical Plants

Authors:

Vanlin Sathya, PhD, Wireless Solution Architect, Celona

Pradhyum Ramkumar, Sr. Dir Product Marketing, Celona

celona

Contents

Introduction 3

Comparing public cellular, Wi-Fi, and private wireless 4

Use cases driving the need for reliable connectivity in oil and gas 5

Design considerations for private 5G deployments in oil and gas 6

Spectrum planning 6

Channel planning 8

Private 4G vs 5G 9

Coverage vs. capacity tradeoffs 10

Multi-vendor vs. end-end solutions 12

Network Architecture 13

Devices and applications 14

Managing device and application QoS 16

Security 17

RF design and installation considerations 18

Location and coverage planning 18

Antennas 18

GPS and PTP 19

Power and connectivity 20

Compliance with hazardous area classifications 20

Environment-related considerations 20

Redundancy and reliability 21

Testing and commissioning 21

How to evaluate Total Cost of Ownership (TCO) 22

Connecting a 0.55 square-mile refinery 22

Measuring performance in the oil and gas environment 23

Comparison between predictive and actual data 23

Coverage Heatmap 24

Mobility and handover or roaming behaviour 24

Throughput performance in downlink and uplink 25

Different use-case application performance 26

Your private 5G network checklist 27

Introduction

Reliable connectivity is essential in the oil and gas industry for production quality, operational efficiency and worker safety. It ensures that workers can communicate effectively and access real-time data, which is crucial for adhering to safety standards and responding promptly to emergencies. Additionally, seamless data transfer and communication are vital for monitoring and managing operations efficiently, including accessing work orders, permits, and instructions in the field. This reduces the reliance on outdated paper-based systems and improves decision-making and operational accuracy.

The oil and gas environment are characterized by its complex infrastructure and challenging conditions. Refineries, for instance, encompass extensive outdoor areas and intricate metal structures, such as pipes and tanks, which can obstruct wireless signals. This makes deploying wireless technologies like Wi-Fi particularly challenging. Wi-Fi access points (APs) typically have lower power transmission, resulting in smaller coverage areas. Covering the entire outdoor footprint necessitates more APs and complex backhaul infrastructure, adding to the challenges of achieving comprehensive coverage.

Public cellular networks also fall short due to poor connectivity at remote sites, where these plants are typically located. Furthermore, these sites communicate sensitive data and there are security concerns using public networks. In contrast, private wireless networks, leveraging the CBRS mid-band spectrum (3.5–3.7 GHz), provide dedicated LTE and 5G connectivity with strong signal penetration, even within metal structures. These networks support IoT, AI, and sensor-driven performance analysis, enhancing maintenance efficiency and minimizing shutdowns. This paper outlines the deployment of private wireless networks in refineries and petrochemical plants, offering a practical guide for IT/OT engineers.

Comparing public cellular, Wi-Fi, and private wireless

	Public Cellular	Wi-Fi	Private Wireless
Coverage	Spotty coverage is influenced by macro tower locations, construction materials, and landscape factors.	Limited outdoor coverage due to low transmission power and susceptibility to spectrum noise.	Reliable coverage with higher transmit power, lower noise floor, and minimal interference.
QoS	Best-effort solution; expensive on-site installations required for better QoS.	No guaranteed QoS due to contention-based access, making prioritization difficult.	Guarantees QoS with deterministic latency and throughput.
Mobility	Good outdoor mobility; struggles indoors with weak signal penetration.	Lacks seamless mobility; device-driven handovers cause disconnection and reconnection delays.	Seamless mobility indoors and outdoors with infrastructure-controlled, precise handovers.
Security and Control	Limited enterprise control over QoS and security policies managed by MNOs.	Relies on pre-shared keys and open SSIDs, increasing security risks.	Full enterprise control over routing, security, and QoS; ensures end-to-end data security with SIM/eSIM.
Cost	Consumption-based charges with overages and complex contracts.	High costs due to numerous APs and expensive trenching/cabling for large-area coverage.	Lower costs with fewer APs; roof-mounted outdoor APs reduce the need for trenching/cabling.

Use cases driving the need for reliable connectivity in oil and gas

Below are some typical use cases driving the need for pervasive and reliable wireless connectivity in the oil and gas industry

Inspection and maintenance

- Access real-time data, conduct remote inspections, and report maintenance needs.
- Use of video conferencing and AR apps for real-time troubleshooting.
- Devices: Ruggedized handhelds/tablets.

Safety, compliance, and security

- Access digital forms and checklists, complete safety protocols, report hazards, and receive real-time hazard warnings.
- Connect safety monitoring systems (e.g., gas detectors, fire alarms) to a central network for real-time alerts and responses.
- Typical devices: iPads, ruggedized handheld computers.

Video surveillance and analytics

- Monitor the perimeter of oil refineries, storage tanks, or offshore platforms to prevent unauthorized access.
- Provide live video feeds of areas with limited human presence due to safety concerns.
- Assist emergency response teams with real-time visuals during fires, leaks, or explosions.
- Enable real-time streaming of video from surveillance cameras, integrated with AI-powered analytics for intrusion detection, hazard monitoring, and operational insights.
- Devices: Security Cameras, Industrial Cellular gateways.

Drone and autonomous vehicle connectivity

- Provide connectivity for drones or autonomous vehicles used for pipeline inspection, site surveying, or equipment delivery in remote oil fields.
- Devices: Industrial Cellular gateways.

Extending network coverage

- Ensure reliable communication for both full time and contractor staff for regular inspections as well as during turnarounds.
- Wireless connectivity for Safety Houses and trailers distributed on-site.
- Devices: Industrial Cellular gateways.

Data collection/digital twin

- Log data, take geotagged photos, and upload information to cloud-based platforms.
- Interact with digital twin models of oil rigs, refineries, or processing plants for visualization and troubleshooting.
- Devices: Ruggedized handheld/tablets, IoT sensors.

Remote monitoring

- Monitor operational systems like flow rates, pressure, and temperatures remotely.
- Real-time pipeline monitoring to identify potential issues like leaks or pressure drops.
- Monitor weather patterns at offshore locations and communicate with onshore teams, perform inspections via AR applications.
- Devices: Ruggedized handheld/tablets, IoT sensors, Industrial Cellular gateways.

Design considerations for private 5G deployments in oil and gas

To ensure optimal performance and security for your operations, we recommend implementing a comprehensive network solution that addresses the following key requirements:

Spectrum planning

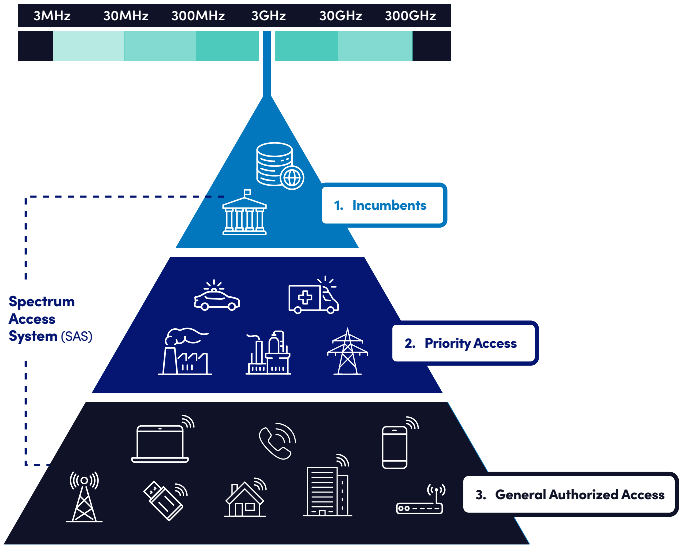
Spectrum allocation in private networks typically involves choosing the right frequency bands, ensuring minimal interference, and optimizing coverage. Enterprises can build private cellular networks using wireless spectrums available in the U.S. and globally

Shared spectrum e.g. CBRS Band (3.5 GHz)

In the U.S., solutions often utilize the CBRS spectrum (3550-3700 MHz), which is a shared spectrum managed by a Spectrum Access System (SAS). The CBRS band has three tiers with different priorities on the network.

- Incumbents: Military radars and fixed satellite stations, which have the highest priority.
- Priority Access Licenses (PAL): Licensed spectrum for enterprise use (obtained through an auction).
- General Authorized Access (GAA): Unlicensed use of the remaining spectrum by enterprises on a first-come, first-served basis.

Enterprises can choose to operate in the GAA unlicensed spectrum or apply/partner with someone with PAL spectrum license for more mission-critical applications.



Reference: https://ongoalliance.org/the-technology-behind-spectrum-sharing-the-spectrum-access-system

Licensed spectrum

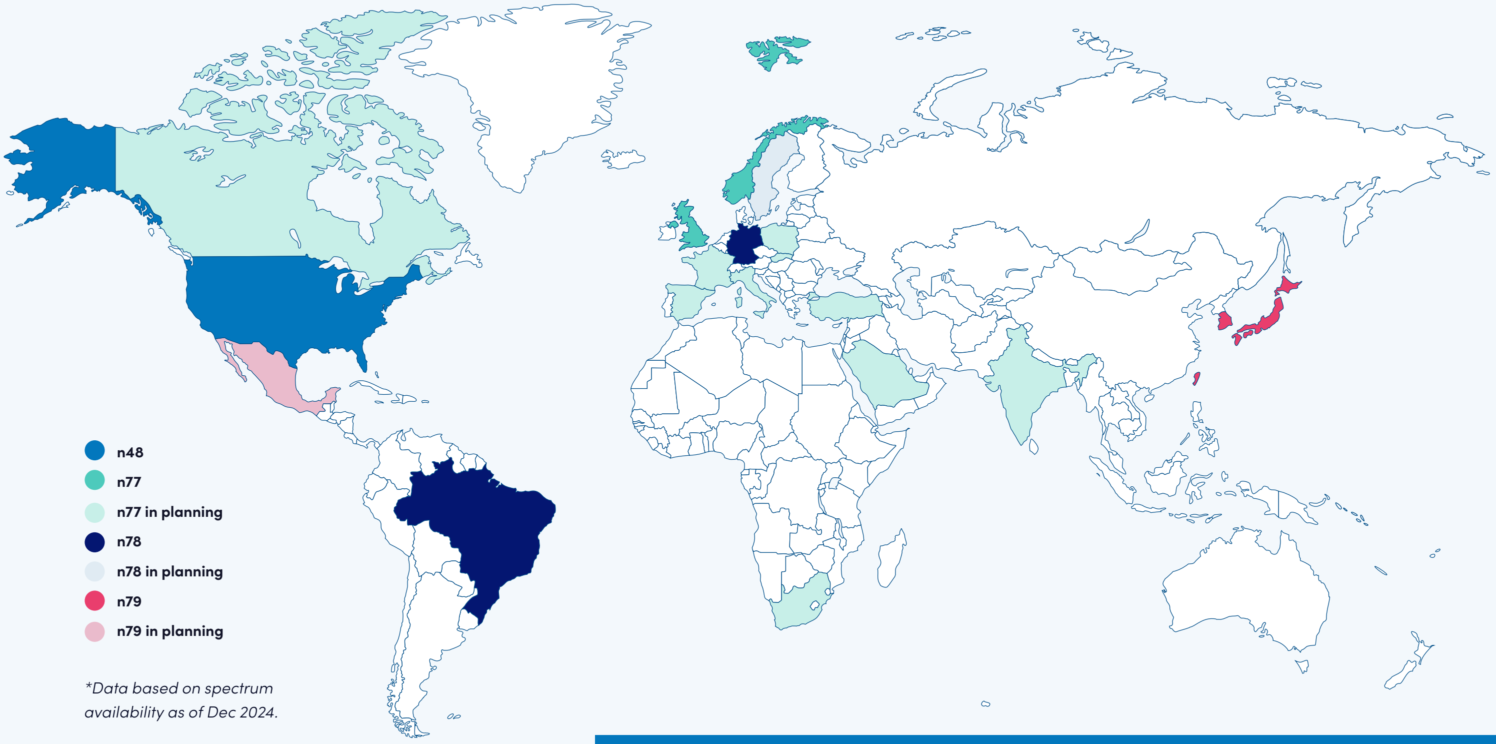
In some regions or scenarios, solutions may leverage licensed spectrum, allowing enterprises with licensed frequency allocations to run their private networks.

Other frequency bands

Depending on the region and the customer requirements, solutions can work with spectrum allocations in the 5 GHz and other industrial frequency bands used for private LTE/5G.

Key considerations:

- **Availability of shared spectrum:**
  Many countries and regulatory bodies are opening spectrum for shared use. For example, in the United States, Band 48 offers 150 MHz of spectrum for general use across the country. Similarly, other countries in Europe, the UK, the Middle East, Southeast Asia, and Japan are also opening spectrum in the mid-band range, such as the n77 and N78 bands. Shared spectrum frameworks ensure reliable, interference-free, and secure communication, allowing scalable and flexible connectivity tailored to industry needs.
- **Mission-critical applications:**
  Using licensed spectrum rather than shared spectrum provides a more controlled environment for mission-critical use cases in oil and gas refineries, where reliable connectivity is crucial for safety, for example, operational technology, safety systems etc.
- **Cost-effectiveness:**
  Shared spectrum eliminates the need for expensive licensed spectrum, significantly reducing the cost of deploying private 5G networks. This makes it feasible for businesses of all sizes to benefit from the advantages of private 5G without the financial burden of acquiring exclusive spectrum licenses.
- **Device ecosystem:**
  Many device manufacturers support shared spectrums opening across the world, which means more device choices and open device ecosystems without compromising on performance or compatibility.
- **Standards support:**
  The private wireless implementation needs to be compliant with the 3GPP standards for shared and licensed spectrum protocols. This will ensure that future mobile devices (iPhones, iPads, Androids), modems, and routers in the market work with reliable, and high-performance private 5G networks.



**Data based on spectrum availability as of Dec 2024.*

Celona offers the 5G LAN solution in a wide range of licensed and shared spectrums including PAL.

More at celona.io/access-points >

Channel planning

Channel planning ensures that available spectrum is used efficiently to minimize interference and maximize coverage and capacity. This is especially important in industrial environments such as oil and gas, where interference from machinery, steel structures, and environmental factors can degrade network performance.

- **Frequency reuse:** In a private network, particularly one using CBRS or other licensed/unlicensed bands, frequency reuse is essential for maximizing spectrum efficiency. Proper channel planning ensures that adjacent cells or sectors use different frequencies to avoid co-channel interference.
- **Interference management:** Techniques to minimize interference, both internal (from other parts of the private network) and external (from other nearby networks or public networks).
- **Power and coverage optimization:** Along with frequency selection, the power levels for each cell or sector need to be planned to ensure good coverage without causing unnecessary interference or exceeding regulatory power limits.

Key considerations:

How is channel planning automated in the private 5G solution

- Channel assignment to APs.
- Load balancing with fluctuating user density or high-traffic areas.
- Interference mitigation.
- Cell coverage optimization.
- Fault detection and recovery.

Celona Self-Organizing Networks (SON) offers fully automated channel management

More at celona.io/network-architecture/self-organizing-network ›

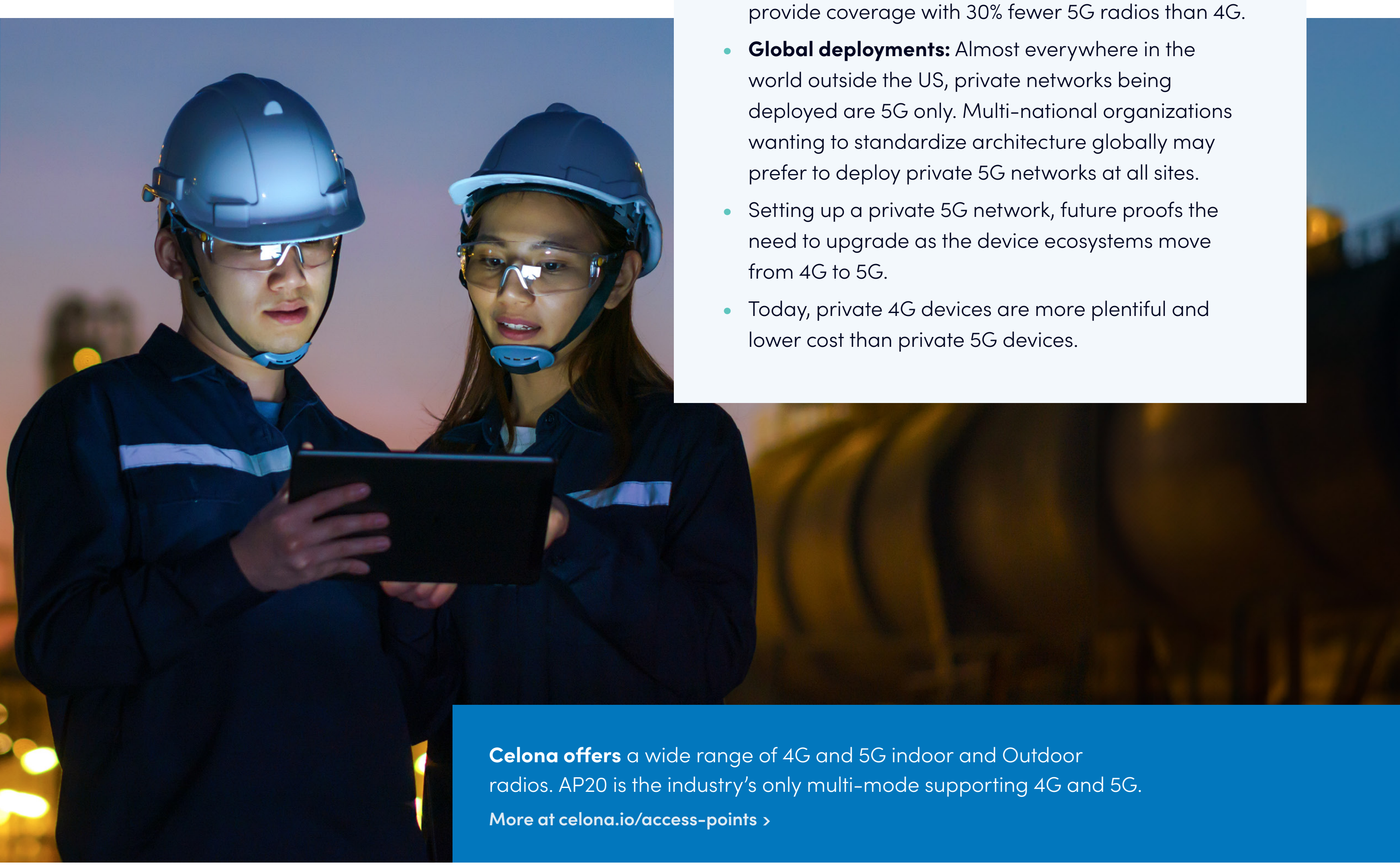
Private 4G vs 5G

Private 4G and 5G networks are dedicated mobile networks for private use by a company or public administration. They offer superior coverage, enhanced performance, and cost efficiency compared to Wi-Fi and public cellular networks.

While the gap is closing, the cost of deploying private 5G network is higher today in comparison to Private 4G. However, private 5G networks are better suited for ultra latency-sensitive industrial automation applications due to their lower latency and higher data throughput.

Key considerations:

- **Uplink/downlink:** Private 5G networks generally provide higher uplink and downlink speeds than 4G, making them suitable for applications requiring high data throughput like HD security cameras.
- **Latency requirements:** 5G networks have significantly lower latency than 4G, which is crucial for real-time applications and mission-critical operations like OT applications.
- **Coverage and capacity:** 5G networks offer better coverage and capacity, higher device density and data rates. This is essential for handling massive IoT deployments and ensuring reliable connectivity in challenging environments. In many cases 5G offers significantly improved performance and efficiency. For example in a refinery deployment, Celona could provide coverage with 30% fewer 5G radios than 4G.
- **Global deployments:** Almost everywhere in the world outside the US, private networks being deployed are 5G only. Multi-national organizations wanting to standardize architecture globally may prefer to deploy private 5G networks at all sites.
- Setting up a private 5G network, future proofs the need to upgrade as the device ecosystems move from 4G to 5G.
- Today, private 4G devices are more plentiful and lower cost than private 5G devices.



Celona offers a wide range of 4G and 5G indoor and Outdoor radios. AP20 is the industry's only multi-mode supporting 4G and 5G.

More at celona.io/access-points ›

Coverage vs. capacity tradeoffs

In terms of coverage, capacity, and performance, the network must support wide-area coverage to connect both centralized control systems and remote locations. High capacity is essential for handling massive IoT deployments (e.g., sensors, cameras) and low-latency communication is required for mission-critical operations like drilling and safety monitoring.

The coverage vs. capacity tradeoff in wireless networks reflects the challenge of balancing geographical reach with the ability to support high data rates and user density - which 5G does.

For oil and gas operations in rural areas and large campuses spanning up to 70 million square feet, mid-frequency bands with superior propagation are ideal for providing wide-area coverage. Combined with max transmit power, these bands ensure reliable connectivity across vast, remote environments, supporting critical operations and communication needs effectively.

In urban areas, where there may be security zones and a high density of people during turnarounds, capacity is optimized using wider bandwidths, high-frequency spectrum, and dense deployments of radios. Advanced techniques such as MIMO enhance network efficiency, ensuring high-speed, reliable connectivity to handle heavy data demands in these dynamic environments.

Enhancing one often compromises the other, as increasing coverage typically reduces the resources available for high-speed connections. To manage this tradeoff, networks use overlap deployments, carrier aggregation, dynamic spectrum sharing, and adaptive resource allocation, tailoring solutions to traffic demand and service requirements.

Coverage vs. capacity tradeoffs

Key considerations:

- **Uplink:** In coverage-focused networks, uplink performance is limited by the lower transmit power of user equipment, making it difficult to maintain strong connections in extended areas, though low-frequency bands (for example: mid-band 3.5 GHz range) improve propagation. In capacity-focused scenarios, uplink performance can be affected by interference in dense deployments and higher path loss at high frequencies, restricting robust connectivity.
- **Downlink:** Downlink generally benefits from base station max transmit power, but coverage-optimized networks may face reduced throughput at the cell edge due to lower bandwidth and poor SINR. In capacity-focused networks, higher bandwidth and advanced technologies like beamforming improve downlink performance, though interference in dense areas can degrade signal quality.
- **Choice of TDD configuration:** TDD (Time Division Duplex) is a wireless communication method where uplink and downlink transmissions share the same frequency band but occur at different times, separated by a timing schedule. This allows dynamic allocation of resources, making it ideal for asymmetric traffic patterns like those in 5G networks.
  TDD configuration choices must align with the network's traffic characteristics and deployment goals. Uplink-biased configurations are better for coverage-focused networks to enhance uplink performance, while downlink-biased configurations suit capacity-optimized deployments to meet heavy downlink demand. Advanced techniques like adaptive TDD in 5G NR provide flexibility to manage the tradeoff dynamically.
- **Latency requirements:** Coverage-optimized networks experience higher latency due to longer signal travel distances and retransmissions at the cell edge, while low-frequency bands offer limited mitigation. Capacity-optimized networks typically have lower latency due to shorter signal paths in dense deployments, though interference can occasionally increase delay through retransmissions.

Celona's offers include strategies like carrier aggregation, dynamic resource allocation, overlap deployment networks, and advanced scheduling to balance the tradeoff, improving uplink, downlink, and latency performance across coverage and capacity-optimized networks.

More at docs.celona.io/en/articles/device-test-matrix-and-tdd-config-slot-pattern >

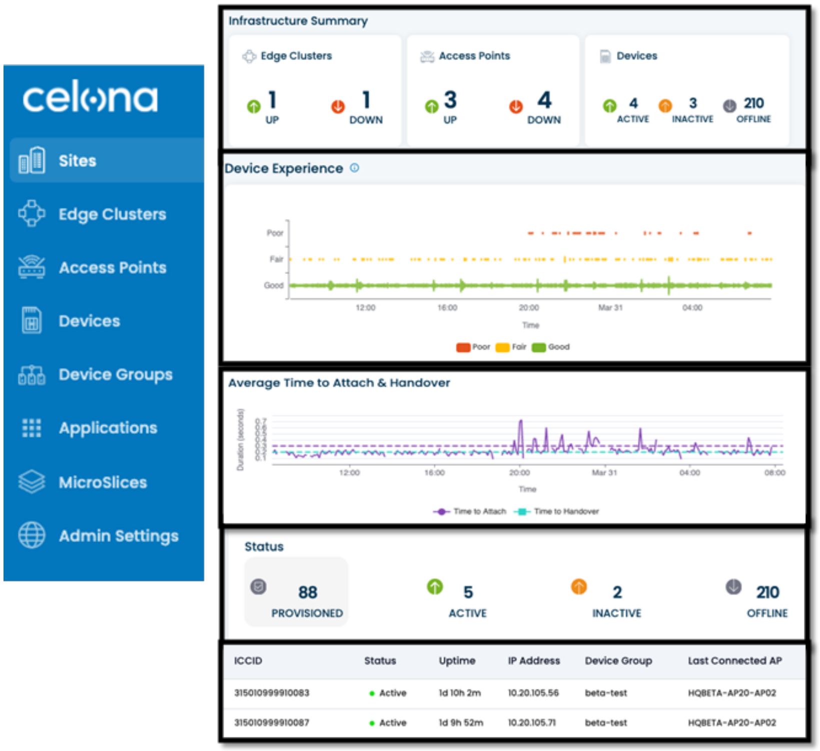
Multi-vendor vs. end-end solutions

For multi-vendor solutions, RAN, Core and orchestration/management systems come from multiple vendors. All these components need to be integrated together typically by an SI. The integration complexity and support challenges increase manifold, often leading to poor customer experience due to the lack of a single point of ownership and longer times to resolve issues. Furthermore, customers need a swath of skills to manage and administer their own network or depend on a managed service provider.

On the other hand, turn-key solutions like Celona 5G LAN offer all elements of the infrastructure Radios, Core, SIMs/eSIMs and Orchestration platforms that have been developed in-house, allowing seamless operation with each other. Single pane dashboard to manage devices, network and subscribers; single point of contact for troubleshooting the network; Orchestrator tools for customers to manage their own network if they choose to.

Key considerations:

- Single vs. multiple systems/dashboards to manage all elements of the solution (core, radio and SIMs)?
- Expertise needed to manage the cellular network.
- Is there a single point of contact for support/troubleshooting components?
- Who owns what element of software? Do elements have their own software lifecycle?
- How are software upgrades/configuration changes across different elements managed?
- Are APIs available to manage different elements of the network?



Infrastructure Summary

Edge Clusters: 1 UP, 1 DOWN

Access Points: 3 UP, 4 DOWN

Devices: 4 ACTIVE, 3 INACTIVE, 210 OFFLINE

Device Experience

Average Time to Attach & Handover

Status

88 PROVISIONED, 5 ACTIVE, 2 INACTIVE, 210 OFFLINE

ICCID	Status	Uptime	IP Address	Device Group	Last Connected AP
315010999910083	● Active	1d 10h 2m	10.20.105.56	beta-test	HQBETA-AP20-AP02
315010999910087	● Active	1d 9h 52m	10.20.105.71	beta-test	HQBETA-AP20-AP02

Celona offers an end-end turn-key enterprise-friendly solution that can be managed with Celona Orchestrator - a single pane of glass nework management system. Day N operation of the Private 5G network can be easily managed like Wi-Fi networks.

More at docs.celona.io/en/collections/3990613-network-monitoring ›

Network Architecture

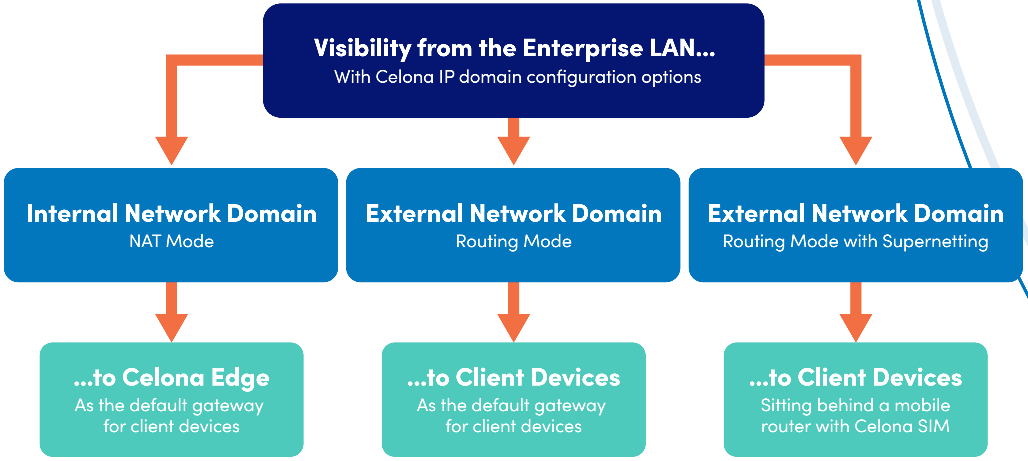
Cost drivers for deploying a private 5G network include the network architecture and the type of private 5G solution. Traditional private 5G networks, adapted from macro network designs, create a separate network not integrated with the enterprise network, leading to additional costs for new fiber cabling, dedicated switches, baseband units, new routers, and potentially VPNs for accessing internal enterprise applications. Control of network access is often handed over to the Mobile Network Operator (MNO) or the entity managing the network.

In contrast, a modern enterprise private 5G network design integrates seamlessly with the existing enterprise IT environment. Radios plug directly into existing cabling and switching infrastructure, allowing the reuse of existing assets. This design provides native local application access, making the private 5G network and its clients an extension of the existing enterprise IT environment. The enterprise retains end-to-end control over network access and visibility into client devices and their activities on the network.

This significant difference in network architecture results in varying cost drivers, and network visibility/manageability for a private 5G network.

Key considerations:

- What additional networking components (new wiring, switches, firewalls) are required for the integration?
- Will devices on the Private Wireless network have visibility from the enterprise network to set up routing and security policies? How about the visibility of devices?
- Does the solution integrate into existing AAA/NAC services in use?
- Does the solution have flexibility in routing? Does your Private Wireless system enable the use of enterprise DHCP for dealing out IP addresses to Private Wireless devices on the network?
- How does your network integrate into existing L2 networks like Profinet?



Visibility from the Enterprise LAN...
With Celona IP domain configuration options

Internal Network Domain
NAT Mode

...to Celona Edge
As the default gateway for client devices

External Network Domain
Routing Mode

...to Client Devices
As the default gateway for client devices

External Network Domain
Routing Mode with Supernetting

...to Client Devices
Sitting behind a mobile router with Celona SIM

Celona's offers the industry's most enterprise-friendly architecture, allowing you to directly plug into existing enterprise network, without the need for additional cabling, switching infrastructure and firewalls.

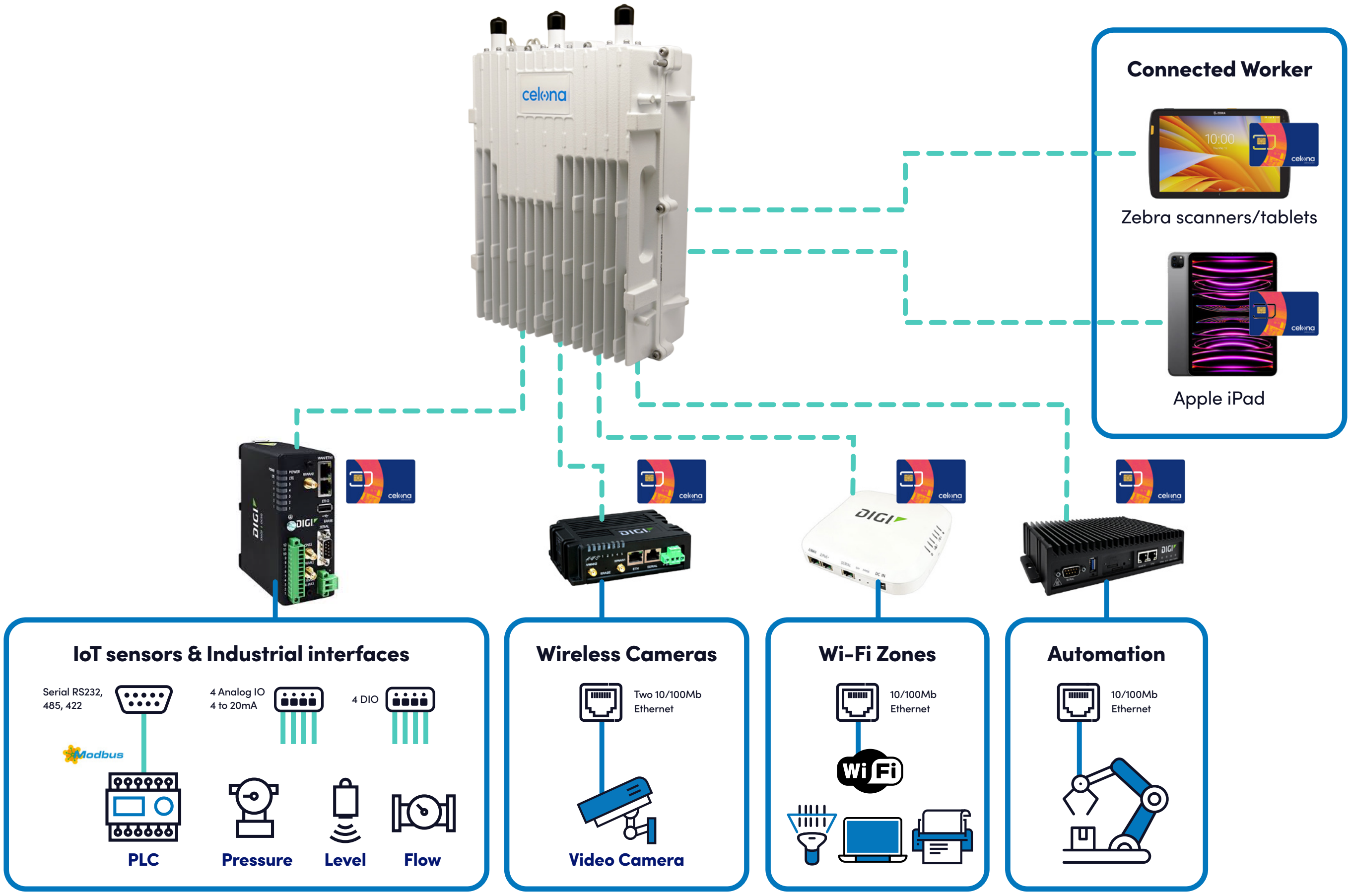
More at celona.io/WP-Routing-Architecture >

Devices and applications

The devices used in oil and gas comprise equipment, some of which have native private cellular support and some without.

Many industrial equipment manufacturers such as Zebra, Apple, Panasonic, Getac are now readily available with support for Private 5G spectrums. These typically support a SIM or an eSIM, which is used to authenticate the device on the network

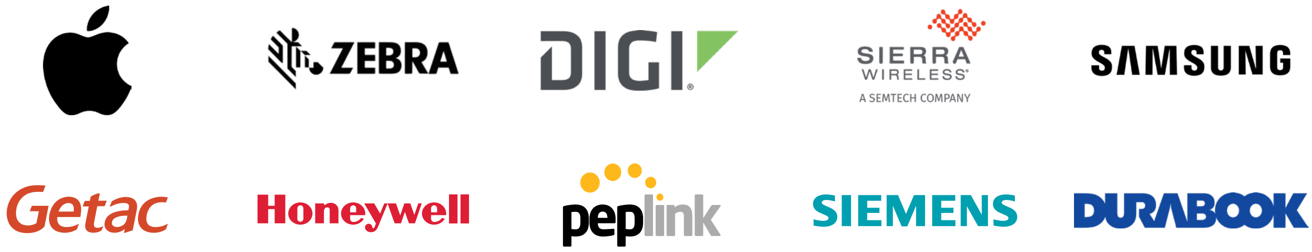
Legacy equipment such as PLC, 4 to 20mA circuits, and wired security cameras do not have a cellular modem and will require a Gateway like Digi IX30 to connect to the Private network. These gateways support legacy interfaces and can backhaul the traffic on a private network, giving the flexibility to connect equipment, anywhere on site.



Key considerations:

- Does the device have native Private wireless connectivity (e.g. eSIM/SIM)?
- If not, what type of gateway is required to connect?
- Does the Private 5G solution support eSIM and MDM for bulk device onboarding?
- To what extent has the interoperability testing been done for the gateway/ device connecting to the private 5G network:
    - Basic connectivity
    - Uplink/Downlink throughput testing in different TDD configurations
    - Latency testing
    - Roaming testing
    - Routing testing
    - International bands like n77, n79 etc.
- Are the devices of popular industrial device manufacturers like Zebra, Apple, Honeywell, Digi rigorously tested. Are there test reports available?
- What tools does the solution have to continuously monitor device experience?
- How is the device provisioned at scale on the network? Does it support eSIM provisioning using MDM?

Celona compatible end user devices



Celona 5G LAN device certification program tests for comprehensive device interoperability. This outcome provides our customers with confidence in the performance characteristics and feature support for devices when connected to a Celona 4G/LTE or 5G network. Celona also supports eSIM and provisioning using MDM tools.

More at celona.io/devices >

Managing device and application QoS

Quality of Service (QoS) plays a critical role in the oil and gas industry in ensuring reliable, secure, and efficient communication. The diversity of devices and applications in this sector requires differentiated QoS settings tailored to specific operational needs.

Critical applications like Microsoft Teams and emergency communications require seamless operation with no delays or packet loss. QoS mechanisms prioritize bandwidth for real-time tasks in congested networks.

QoS by device: Devices in the oil and gas sector, such as sensors, actuators, mobile devices, and drones, have distinct QoS requirements. Industrial IoT sensors need low latency and high reliability for real-time monitoring, while actuators and control systems demand ultra-reliable and low-latency communication to ensure the timely execution of commands. Field personnel's mobile devices require moderate QoS with emphasis on throughput, and drones or robots need high-bandwidth, low-latency connections for live data streaming and remote control in hazardous environments.

QoS by application: Applications like Microsoft Teams on iPad, video surveillance, and emergency communication have diverse QoS needs. Teams' application requires reliability and low latency for real-time inspection during on-site problem-solving. Similarly, video surveillance requires high bandwidth for HD video feeds with moderate latency tolerance. Emergency communication systems need top-priority QoS to ensure availability during critical events.

Key considerations:

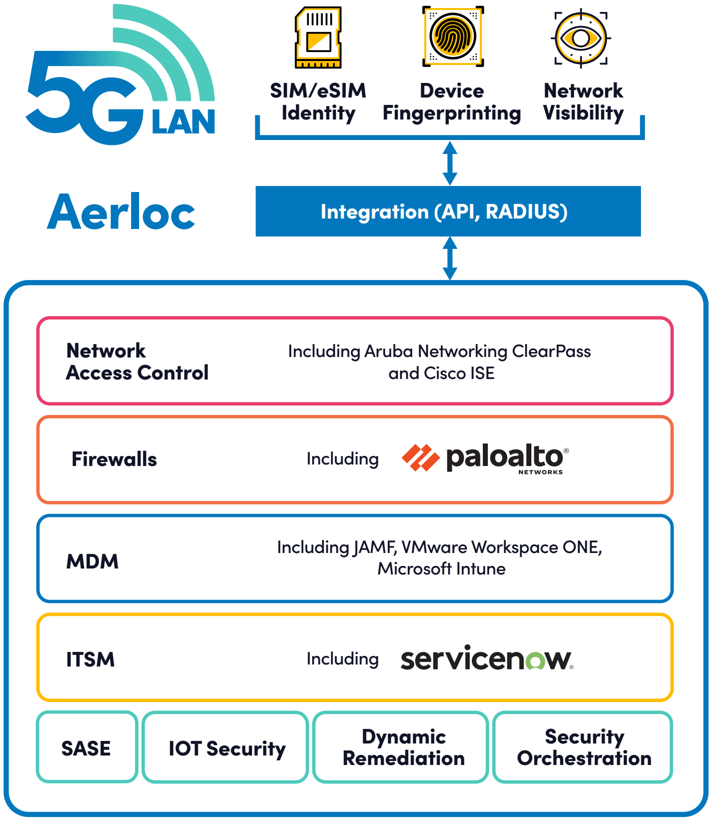
- How does the network guarantee QoS for business-critical uplink/downlink applications?
- How does the network segment critical and non-critical traffic.
- Is the QoS policy granular and can it be applied to a device or based on an application?
- Does the QoS policy apply to the air interface as well as to the physical network?
- Does QoS require configuration changes on each device, or can it be done centrally on the infrastructure?

Celona MicroSlicing™ provides Quality of Service on a per-device per-application basis, delivered efficiently through AI and policy settings. MicroSlicing™ - QoS for business-critical apps

More at celona.io/WP-Microslicing >

Security

Security requirements are stringent, with a focus on zero-trust architectures to ensure that only authorized devices and personnel can access critical OT systems. Existing firewalls and security policies, including AAA (authentication, authorization, and accounting) and NAC (network access control) systems, should be leveraged to maintain strong security controls and prevent unauthorized access or cyber-attacks on sensitive operational assets.



Key considerations:

- How does the private 5G solution integrate into existing security frameworks like AAA (authentication, authorization, and accounting) and NAC (network access control) systems?
- Will it support zero-trust architecture for devices on the Private 5G network?
- Does the Private 5G solution work with existing firewalls or does it require new ones?
- Does the solution allow for IT/OT convergence with sufficient air-gapping provisions to maintain different levels of security?

Celona Aerloc architecture provides a unified architecture with full visibility and control to secure increasingly digitized industrial IT and OT systems.

More at celona.io/aerloc ›

RF design and installation considerations

Coverage modeling is essential in determining the placement and quantity of APs. This involves assessing the number of devices, application characteristics, and the required bandwidth. The goal is to ensure adequate coverage and capacity while considering the spectrum availability in the specific location

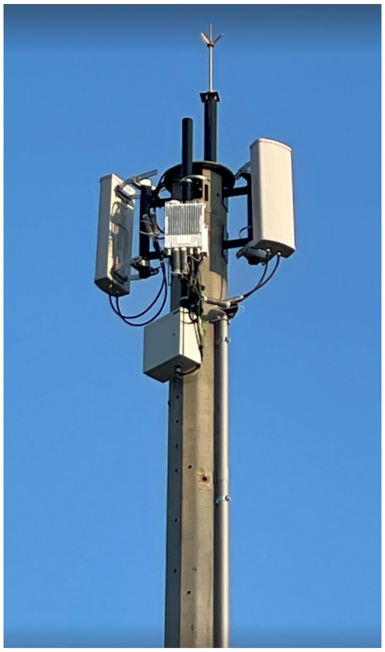
Location and coverage planning

- **Signal propagation:** Conduct a wireless site survey to map coverage areas and identify obstructions such as steel structures, tanks, and other large equipment that may impede signal propagation.
- **Interference mitigation:** Evaluate interference from other wireless systems, like industrial control systems, and plan the AP placement to minimize disruptions.
- **Height and mounting:** Install APs at appropriate heights to avoid physical damage, ensuring they are clear of any obstacles that may affect wireless signal quality.

Antennas

- Omnidirectional antennas provide 360-degree horizontal coverage, making them suitable for environments where coverage is needed in all directions. They are ideal for general coverage in open areas but have a lower gain, which means they may not provide strong signal strength over long distances.
- Sectorized antennas, on the other hand, focus the signal in a specific direction, resulting in higher gain and stronger signal strength over longer distances. This makes them suitable for targeted coverage in specific areas, such as along a pipeline or in a particular section of a refinery. However, they require careful planning and alignment to ensure optimal coverage and may not be as effective in providing broad, all-around coverage.

Omni-directional antenna



Sector antenna

Celona Offers a range of omni-directional and sectorized antennas.

More at docs.celona.io/en/articles/7132235-accessories-antennas-ptp-clock >

GPS and PTP

GPS and PTP are complementary in cellular networks, with GPS offering global synchronization and location services, while PTP provides precise timing over IP networks as a backup or alternative in scenarios where GPS is limited.

Both are critical for ensuring seamless operation, advanced features, and network reliability.

Need for GPS in Cellular or Private Network

- **Synchronization:** Provides precise timing and frequency synchronization essential for Time Division Duplex (TDD) operations to avoid interference between cells.
- **Location services:** Enables location-based services (LBS), emergency call positioning, and user tracking for enhanced network capabilities.
- **Handover support:** Assists in optimizing handovers between cells by aligning timing parameters in mobile networks.
- **Network planning:** Facilitates precise placement of base stations by integrating geographic coordinates for optimal coverage and performance.
- **Interference management:** Synchronizes adjacent base stations to minimize interference, especially in densely deployed networks.

Need for PTP in cellular/private network

- **Backup for GPS:** Provides alternative synchronization when GPS signals are unavailable (e.g., indoors, in tunnels, or in GPS jamming scenarios).
- **Enhanced timing accuracy:** Delivers nanosecond-level timing precision for advanced cellular technologies like 5G NR.
- **Synchronization over IP:** Enables accurate timing over packet-switched networks without reliance on satellite systems.
- **Cost efficiency:** Reduces dependency on GPS receivers at each base station, lowering infrastructure costs.
- **Support for fronthaul and backhaul:** Ensures timing consistency between remote radio heads (RRH) and baseband units (BBU) in centralized RAN (C-RAN) architectures.

https://docs.celona.io/en/articles/10581128-celona-ptp-guidelines-and-best-practices

Power and connectivity

- Power source: Ensure that the power source to the AP complies with hazardous area electrical standards (e.g., intrinsically safe power supplies).
- Power over Ethernet (PoE) may be suitable in some installations.
- Cable protection: Use shielded cables with appropriate conduit systems to protect against mechanical and environmental damage, ensuring that they also meet hazardous area requirements.
- Fiber optic backhaul: In many cases, fiber optic cables are preferred for data backhaul in hazardous environments due to their immunity to electrical interference and sparks.

Standard	Power Delivery	Supported Devices
IEEE 802.3af (PoE)	• Up to 15.4W	• Standard devices like IP cameras and access points
IEEE 802.3at (PoE+)	• Up to 30W	• Standard devices like IP cameras and access points
IEEE 802.3bt (PoE++)	• Up to 60W or 100W	• High-power devices like LED lighting, pan-tilt-zoom cameras, and advanced IoT systems

Celona AP portfolio offers PoE and PoE++ options

More at celona.io/access-points ›

Compliance with hazardous area classifications

- Zone classification: Identify if the installation area is classified as hazardous (e.g., Zone 0, Zone 1, or Zone 2 for gas, or Zone 20, 21, or 22 for dust).
- Ensure that APs or their enclosures are certified for use in the corresponding hazardous zones (e.g., ATEX, IECEx, or UL certifications for explosive atmospheres).
- Explosion-proof enclosures: In high-risk areas, APs should be housed in explosion-proof or intrinsically safe enclosures designed to prevent sparks or flames.

Environment-related considerations

- Ingress Protection (IP) Rating: Ensure that APs are installed in enclosures with a high IP rating (typically IP65 or higher) to protect against dust, water, and corrosive chemicals.
- Temperature ratings: Select AP models and enclosures that can operate in extreme temperature ranges, typically found in oil and gas facilities.
- EMI/EMC compliance: Oil and gas facilities often have high levels of electromagnetic interference (EMI). Ensure the APs are compliant with Electromagnetic Compatibility (EMC) standards.

Redundancy and reliability

- Failover planning: For critical operations, design the network with redundancy in mind, placing backup APs and using a mesh network configuration to provide failover capabilities.
- Regular maintenance: Implement a maintenance schedule to inspect and clean APs, especially if installed outdoors or in dusty environments.

Celona offers multi-node Edge Cluster configuration for high availability and scaling

More at docs.celona.io/en/articles/7132039-multi-node-edge-cluster-configuration-for-high-availability-and-scaling ›

Testing and commissioning

- Pre-installation testing: Perform thorough testing of the APs in non-hazardous zones before installing them in the operational areas. This helps ensure that all configurations are correct.
- Post-installation testing: Once installed, perform RF coverage and interference testing to verify that the APs are functioning as intended and to check for potential signal degradation.

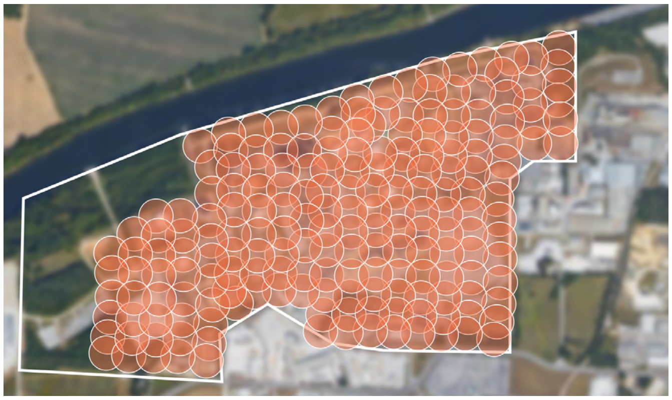
Celona offers a variety of Access Points with different IP ratings and C1 D2 certifications. In addition, they offer a variety of mounting options, and redundant architectures to operate safely and effectively in an oil and gas environment, providing reliable wireless connectivity without compromising safety or compliance with regulatory requirements. More details on installation are available here

More at docs.celona.io/en/collections/3905504-physical-installation-of-celona-edge-and-access-points ›

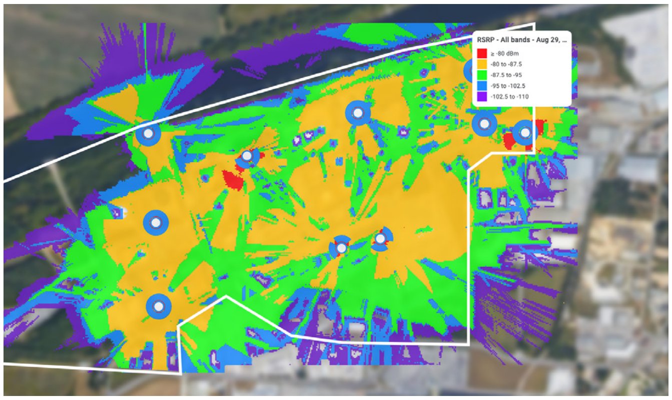
How to evaluate Total Cost of Ownership (TCO)

Connecting a 0.55 square-mile refinery

Area: 260 football fields



300x Wi-Fi APs



10x 5G LAN APs

Consider all the cost elements to establish the total cost of ownership

Hardware costs:

- Access Points
- Antenna, GPS/PTP etc.
- Appliance to run 5G core
- Additional switches, routers and firewalls needed to integrate into an enterprise network.
- SIMs/eSIMs.

Software costs:

- Licensing costs for RAN, Core, and Network Operations dashboard
- Annual maintenance, and updates
- Reconfiguration charges

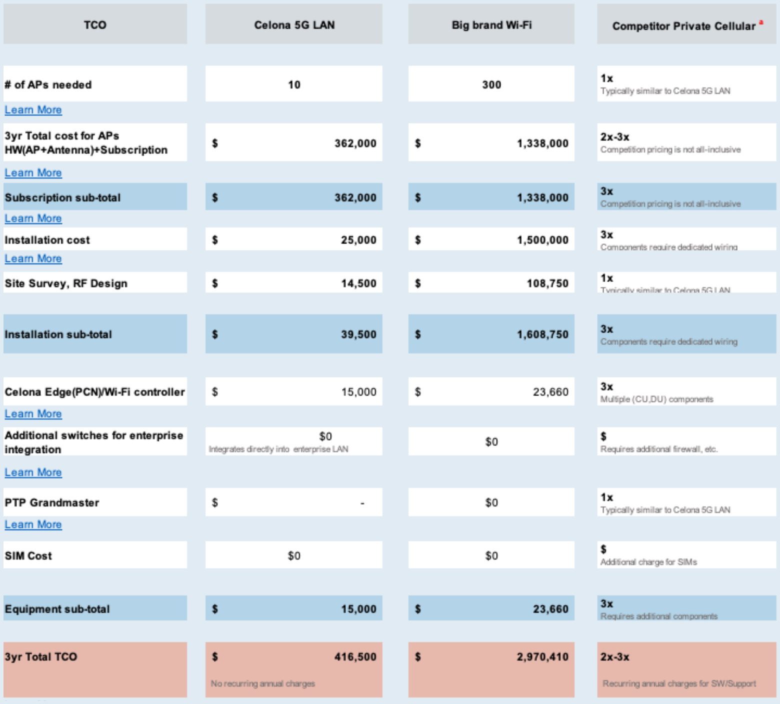
Installation costs:

- Site survey/RF design
- Pole/wall mounting, cabling, power

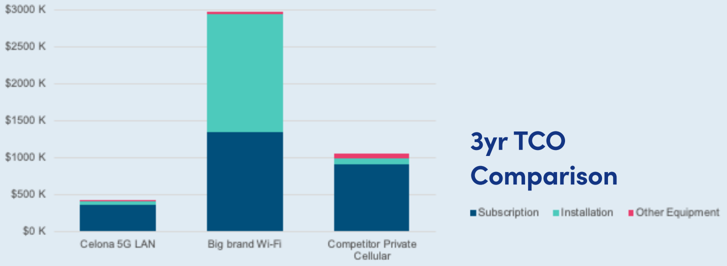
Evaluate your TCO

celona.io/tco-calculator

Cost Breakdown



TCO	Celona 5G LAN	Big brand Wi-Fi	Competitor Private Cellular *
# of APs needed Learn More	10	300	1x Typically similar to Celona 5G LAN
3yr Total cost for APs HW(AP+Antenna)+Subscription Learn More	$ 362,000	$ 1,338,000	2x-3x Competition pricing is not all-inclusive
Subscription sub-total Learn More	$ 362,000	$ 1,338,000	3x Competition pricing is not all-inclusive
Installation cost Learn More	$ 25,000	$ 1,500,000	3x Components require dedicated wiring
Site Survey, RF Design	$ 14,500	$ 108,750	1x Typically similar to Celona 5G LAN
Installation sub-total	$ 39,500	$ 1,608,750	3x Components require dedicated wiring
Celona Edge(PCN)/Wi-Fi controller Learn More	$ 15,000	$ 23,660	3x Multiple (CU,DU) components
Additional switches for enterprise integration Learn More	$0 Integrates directly into enterprise LAN	$0	$ Requires additional firewall, etc.
PTP Grandmaster Learn More	$ -	$0	1x Typically similar to Celona 5G LAN
SIM Cost	$0	$0	$ Additional charge for SIMs
Equipment sub-total	$ 15,000	$ 23,660	3x Requires additional components
3yr Total TCO	$ 416,500 No recurring annual charges	$ 2,970,410	2x-3x Recurring annual charges for SW/Support



3yr TCO Comparison

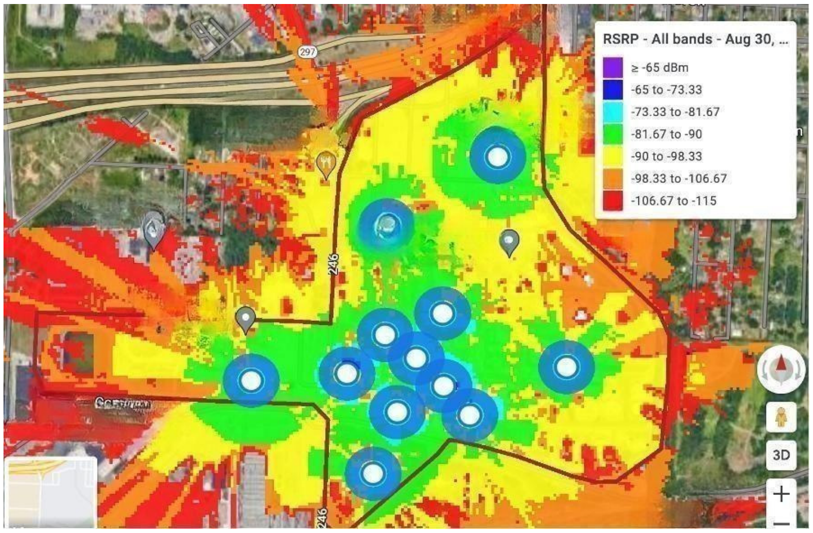
Measuring performance in the oil and gas environment

In this section, we will share a sample performance measurement report for a private wireless network at an oil refinery. This testing and reporting is performed by a Celona or Partner Solution architect.

- All radios operate on the CBRS spectrum band 48.
- Radios connect to a centralized controller with a Self-Organizing Network (SON) algorithm.
- SON algorithm handles channel assignment and Physical Cell ID (PCI) allocation.
- This avoids PCI collision or confusion on the network.
- The deployment environment is outdoor.
- Radios use the existing refinery back-haul network and switches.
- No additional cost for infrastructure.
- 12 radios are deployed in the setup.
- Radios operate on Omni antennas with two antenna ports connected to the AP.
- Omni antennas provide 360-degree coverage.
- GPS antennas are connected to the AP for synchronization between cellular frames.

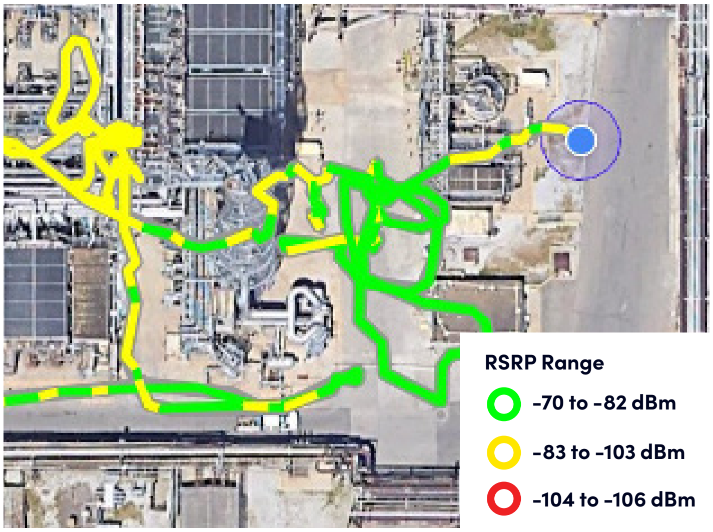
Comparison between predictive and actual data

This image illustrates illustrates the private network deployment throughout the refinery. The RSRP heat map was generated using the Google network planner tool, which incorporates factors like multipath, reflection, shadowing, building blockage, and metal obstruction. The RSRP predictions depend on AP transmission power and blockage effects. We compared the predicted RSRP footprint with actual measurements from APs and devices (UEs) across the refinery. We found a 4 to 5 dBm difference between predictions and actual results, reinforcing the predictive model's accuracy in estimating AP counts in challenging environments.



Coverage Heatmap

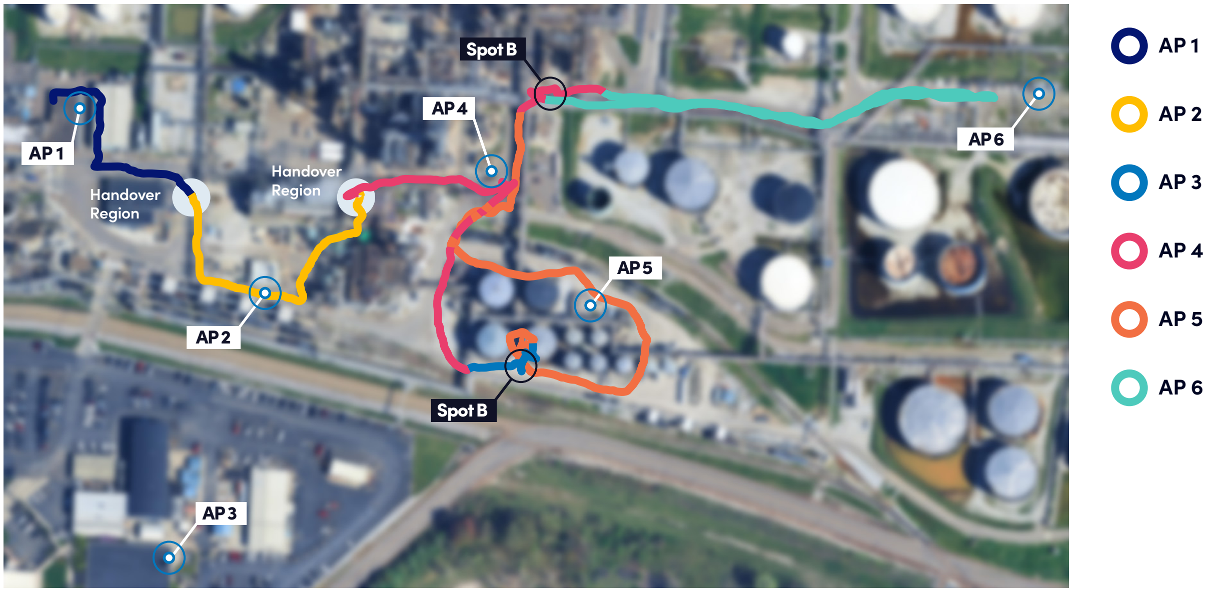
- The image on the right shows illustrates shows the coverage heat map of the refinery premises.
- The coverage map is based on the RSRP signal strength from the connected APs or PCIs.
- The images include refinery regions inside and outside the pipes, where employees require connectivity for routine inspections
- No coverage holes were observed in the entire facility, even deep inside the deep metal pipe surroundings.



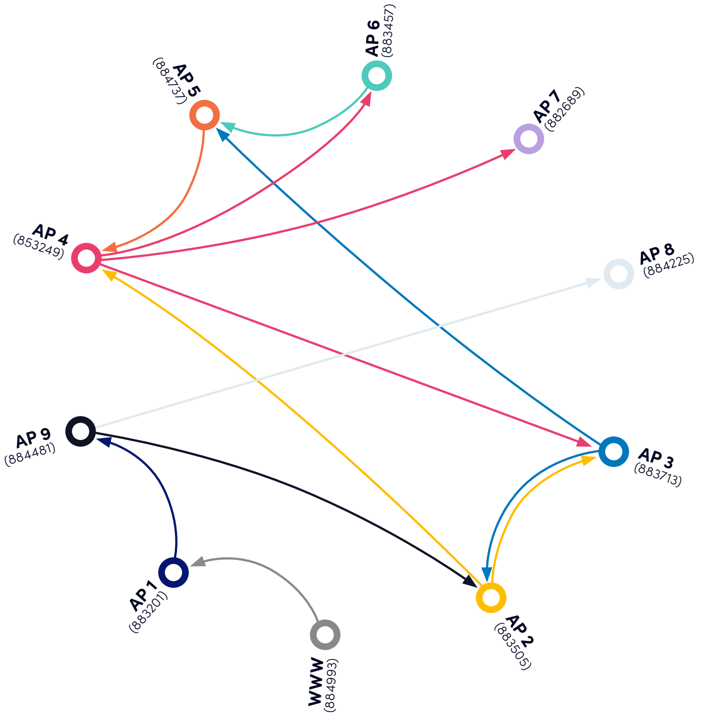
Mobility and handover or roaming behaviour

Testing handover and roaming involves walking the facility testing coverage along all critical paths at the facility, specifically ensuring handovers occur reliably and without perceivable latency.

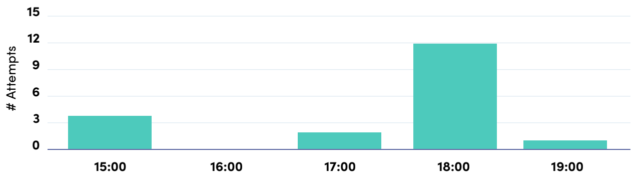
- The blue dots indicate the location of the Access Points (mounted on the existing building, wooden poles, and metal pipes)
- The walk route is shown below in multiple colors. Each color represents a device connected to a particular AP.
- For example, the orange path shows when the device is connected to AP 5 at ATC and the yellow path shows that the device is connected to the AP 2 at the boiler.
- The handover occurs when the device sees a stronger signal (RSRP) from one AP versus the current one. The hand-over regions are depicted on the map as well.



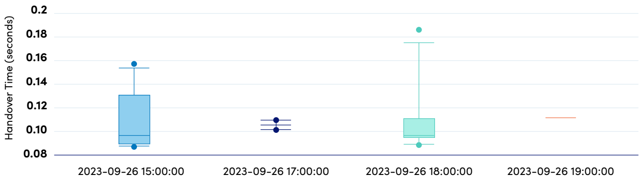
Handover between APs



Average Total Number of Handovers

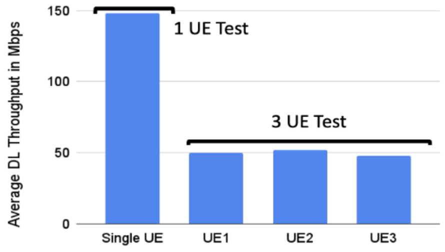


Time Taken for Successful Handovers

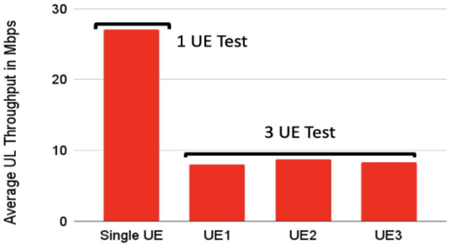


Throughput performance in downlink and uplink

- The iPerf tool was used to record throughput performances, with the server running on the private network edge to avoid back-haul delay.
- TCP traffic with a parallel stream of 15 was used to mimic the behavior of more users in the network.
- The experiment started with a single UE to understand downlink and uplink performance (as shown in the graphs below), then added three devices to study fairness and load sharing.
- With carrier aggregation enabled (40 MHz), the expected average downlink throughput was close to 150 Mbps, and resource blocks were equally shared among devices.
- In uplink, without carrier aggregation, the average uplink performance was 26 Mbps for a single UE, and resource block allocations were fairly scheduled among devices when the load increased to three UEs.



(a) Average DL Throughput

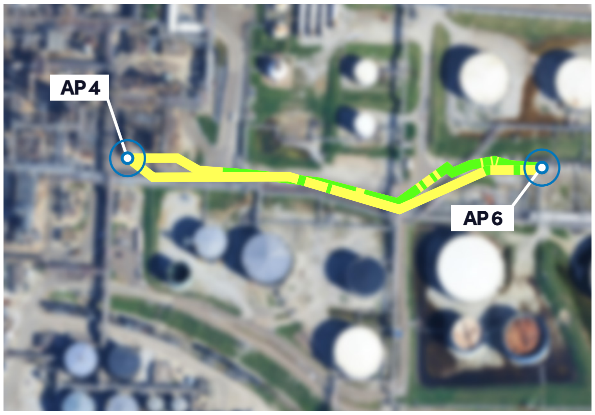


(b) Average UL Throughput

Different use-case application performance

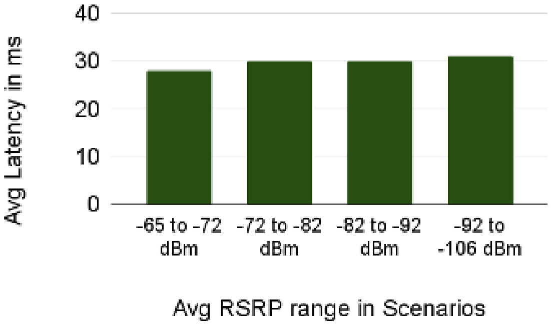
Teams application call

- Refinery employees may need to call remote teams to show problem areas, allowing for prompt assessment and action.
- An audio and video team call were conducted with UE 1 (stationary, connected to AP 4) and UE 2 (moving from AP 4 to AP 6).
- A seamless handover was observed between the two APs within the refinery premises.



Ping latency traffic

- The experiment considers four average RSRP scenarios to measure performance: S1 (-65 to -72 dBm), S2 (-72 to -82 dBm), S3 (-82 to -92 dBm), and S4 (-92 to -106 dBm).
- The graph on the right shows the average latency of ping traffic for these scenarios, with an observed average latency of approximately 30 ms.
- This latency allows employees to run their mission-critical applications in all refinery regions.



Streaming and file download and upload

- No issues were observed with the streaming application from 4 bars to 1 bar signal strength, and the buffer ensured smooth video playback without glitches.
- Different upload and download file size scenarios were tested with 4 bars to 1 bar signal strength.
- Applications reliably transmitted data in all scenarios.

Signal Strength	File Download	File Upload	Teams Call and Streaming
-65 to -72 dBm	✓	✓	✓
-72 to -82 dBm	✓	✓	✓
-82 to -92 dBm	✓	✓	✓
-92 to -106 dBm	✓	✓	✓

Your private 5G network checklist

Use cases

- □ Connected worker
- □ Security Cameras
- □ Connecting to equipment/machinery/sensors
- □ Integration with SCADA, DCS, and real-time monitoring
- □ IT, OT, Converged IT/OT.

RF planning

- □ Shared vs. Licensed spectrum tradeoffs
- □ Spectrum/Channel planning
- □ 4G vs 5G
- □ Building for capacity vs coverage
- □ Latency requirements for critical applications
- □ Handover and Mobility planning
- □ C1D2 hazardous environments and other certifications.

Network planning

- □ Multi-vendor vs. end-end solutions
- □ Stand alone or needs to be integrated into existing Enterprise?
- □ Additional wiring infrastructure needed
- □ IP network visibility
- □ Network resilience and uptime requirements
- □ Require visibility into devices sitting behind gateways
- □ Implementing QoS.

Security requirements

How does the new Private 5G

- □ Fit into your existing security framework?
- □ Integrate into existing AAA (authentication, authorization, accounting)
  and NAC (network access control) policies?
- □ Support IT/OT airgapping?
- □ Support ZTNA for IT and OT devices?

Devices and applications

- □ What devices will connect to the network?
- □ What applications will run on the network?
- □ What QoS is needed on devices and applications?
- □ Connectivity for non-cellular enabled devices
- □ How are SIMs/eSIMs provisioned in bulk.

Success criteria

- □ Network uptime, latency, coverage, device throughput, energy consumption
- □ Impact on production efficiency and safety.

TCO

- □ Infrastructure costs
  - □ Private 5G/LTE radio, core
  - □ Network operations platform
  - □ Additional routing and security infrastructure
  - □ Installation and Cabling costs
- □ Network management costs
- □ Recurring annual software/licensing charges.

celona.io

hello@celona.io

900 E Hamilton Ave Suite 200,
Campbell, CA 95008, United States

Visit celona.io/refineries