Strategic Insights: **Private 5G Deployment Considerations for Manufacturing CIOs**

Rajeev Shah
CEO, Celona

celona

REPORT

Contents

Introduction

Private 5G networks are emerging as the CIOs most powerful enabler of business transformation.

As manufacturers progress into advanced stages of digital transformation, the underlying network is becoming the linchpin for determining success or stagnation. Technology layers like cloud, mobile, Big Data and AI deservedly get a lot of attention on the digitization journey. But these critical advances are ineffective when there is a fundamental lack of reliable connectivity to users, machines, and things on the manufacturing floor.

To overcome the longstanding challenges with connectivity, manufacturing CIOs are increasingly acknowledging private 5G networks as mission-critical infrastructure that can deliver what Wi-Fi cannot – high speed connectivity, low latency, security, and reliability in harsh industrial environments.

Private wireless networks also align with manufacturing CIOs' overarching technology strategy and architectural responsibilities. They deliver productivity enhancements, innovation, and supply-chain transformation. And they seamlessly work with technology trends such as cloud computing, artificial intelligence (AI), and cybersecurity, as well as sector-specific technologies like industrial automation and connected vehicles.

In this whitepaper, we explore the industry-specific problems manufacturers routinely encounter with traditional connectivity, and how CIOs can integrate private wireless to extract maximum business value across all facets of operations.

Connectivity: The forgotten infrastructure

No manufacturing organization can survive in today's unpredictable world without making the transition to digital-first operations. Still, manufacturers have long trailed behind other sectors in their business transformation efforts.

Why? Industry-specific connectivity issues means a large gap remains between the promise of transformation and the reality on the ground.

Traditionally, Wi-Fi has been the preferred choice for wireless connectivity in enterprise settings. However, its reliability falters in "carpet-less" environments, such as outdoor yards in distribution centers or factory floors. This is due to a number of issues:

1. Limited range of Wi-Fi
2. Expense associated with installing cabling for access points in these environments
3. Absence of over-the-air prioritization mechanisms for vital traffic, and
4. Susceptibility to interference in industrial environments

These issues compound the connectivity divide, limiting a CIO's ability to enhance operational efficiency and achieve digital transformation success.

Let's now explore how these challenges play out on the factory floor.

Challenge 1: Low productivity of workers

Escalating and persistent labor shortages coupled with the promise of significant productivity gains, underscores the critical necessity of reliable wireless connectivity for modern manufacturers.

Poor connectivity hampers workers' ability to stay connected, or can even lead to frustrating disconnections. Forced to walk back and forth from the production floor to designated "hotspots", field workers are prevented from using modern tools that need reliable wireless – whether they are modern generative AI applications, or even traditional collaboration tools like Zoom and Teams. In turn, workers resort to manual methods, such as pen and paper, for recording data. Not exactly real-time, and far from digital.

Challenge 2: Deploying and scaling robotics solutions

Given the investments manufacturers are making in these automation solutions and the competitive advantages they can offer, the decision to invest in reliable connectivity infrastructure is an easy one.

The last few years have seen incredible advances in automating operations on the manufacturing floor and in warehouses. This includes Auto Guided Vehicles (AGVs), Automated Mobile Robots (AMRs) and robotics solutions for various workflows.

Unfortunately most of these solutions have been limited in their effectiveness due to lack of reliable connectivity. Wi-Fi struggles to provide adequate coverage, or handle reliable handovers. Most organizations realize that these solutions offer a much higher transformational potential if the wireless connectivity issue is solved.

Challenge 3: Rapid establishment of new locations

Implementing a wireless infrastructure that significantly reduces cabling can fundamentally alter the operational dynamics, enabling a more agile business approach.

Geopolitical uncertainties and lessons learned during the pandemic have prompted most organizations to prioritize supply chain resilience. This has resulted in substantial investments in new manufacturing and warehousing facilities with an emphasis on the ability to rapidly establish sites in response to fluctuations in the business environment.

Surprisingly, one of the main obstacles in bringing these sites online quickly is the time required to ensure connectivity throughout the facility. This is largely due to the extensive number of cables needed for wired and Wi-Fi connections – particularly for more sizable facilities.

Challenge 4: Reliability and security of connected machines

Traditional wireless lacks the level of reliability and security required to truly meet the vision of the all-wireless and fully connected manufacturing floor.

It's the holy grail of future manufacturing operations – deploying a network of highly connected and fully automated machines. Attaining this vision raises valid concerns about the reliability and security of the connection. Traditional wireless technologies lack both the reliability and the robust security features necessary for such critical operations, instead relying on weak security measures like "shared keys" that could make the machines vulnerable to security breaches with potentially catastrophic consequences.

Private wireless and the next generation of connectivity

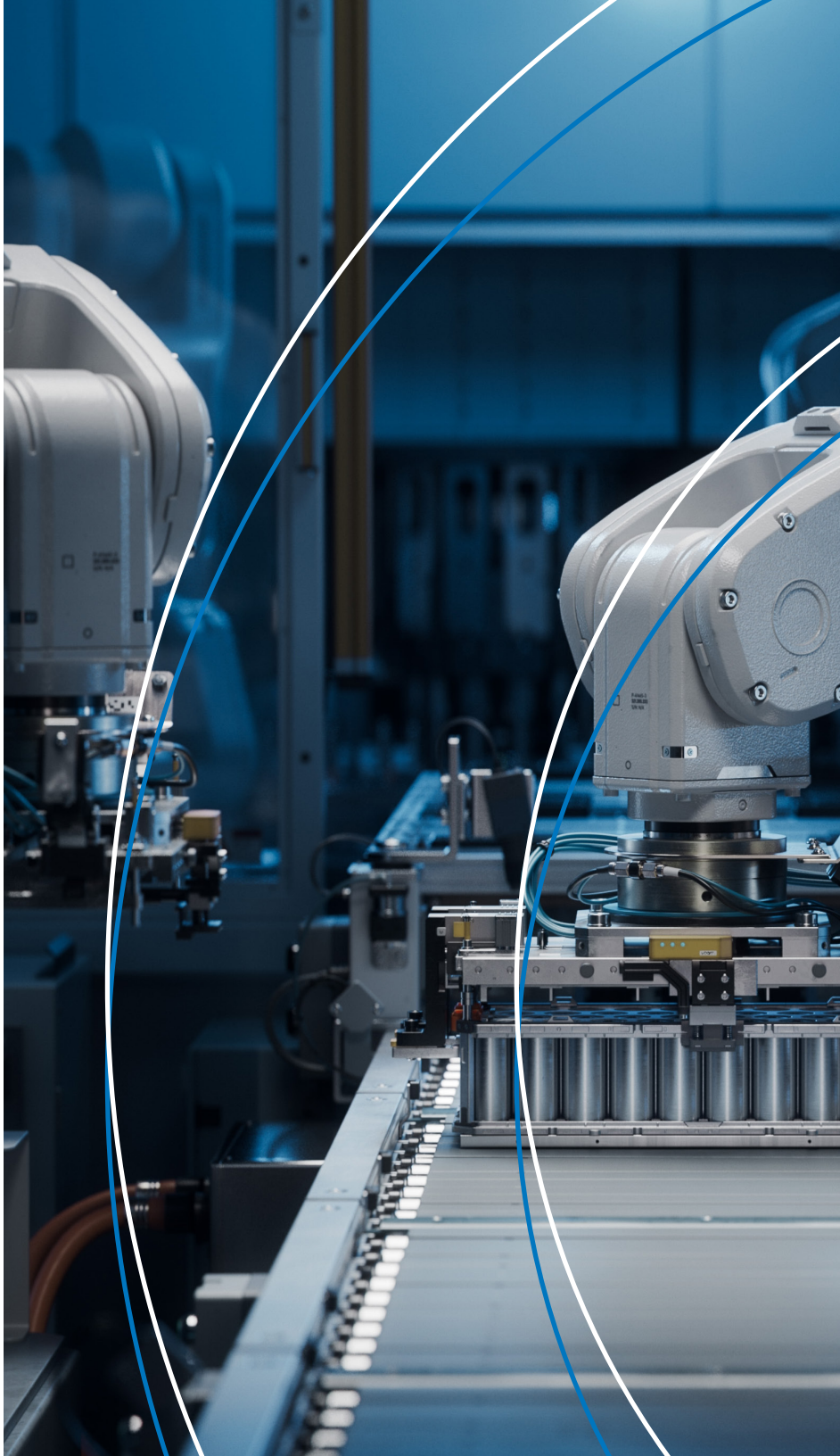
Private mobile networks have emerged in recent years to address these challenges. It started with governments all over the world releasing private spectrum for non-operator organizations to use to build their own mobile networks. This includes CBRS in USA, n77/n78 in UK/Europe, Brazil, Australia, n79 in Japan, Korea and many SE Asian countries. In fact most countries around the world have now responded with models to enable private mobile networks.

In simple terms, it has allowed businesses to create their own high-speed, secure LTE or 5G networks.

Since 2020, businesses have been deploying these networks, a move that has opened up a range of new opportunities across various industries.

In the manufacturing sector, private LTE/5G networks are being deployed to complement or replace existing Wi-Fi infrastructures, a vital step for supporting modern digital communication in harsh manufacturing facilities. By implementing privately managed cellular networks, manufacturing plants are gaining greater control over their network infrastructure, while ensuring reliable internet access in areas with high user density and bandwidth-intensive operations that use, for example, autonomous machinery.

These private LTE/5G networks represent a cost-effective investment, more often than not leading to reduced operational expenses. There is little doubt that the versatility and reliability of private LTE/5G networks is making them mission-critical assets for ultra-demanding manufacturing environments.



Evaluating the alternatives

Sticking with what you know: My current network works just fine.

The perception that the current network does the job overlooks the significant business enhancements achievable with a truly reliable wireless network in industrial environments.

Before dismissing private wireless, conduct a user survey and operational analysis to determine whether any of the previously mentioned issues or opportunities exist – and if they're caused by the existing wireless connectivity. Based on our experience, this proves to be the case without fail.

Improving existing network coverage: Adding more Wi-Fi access points.

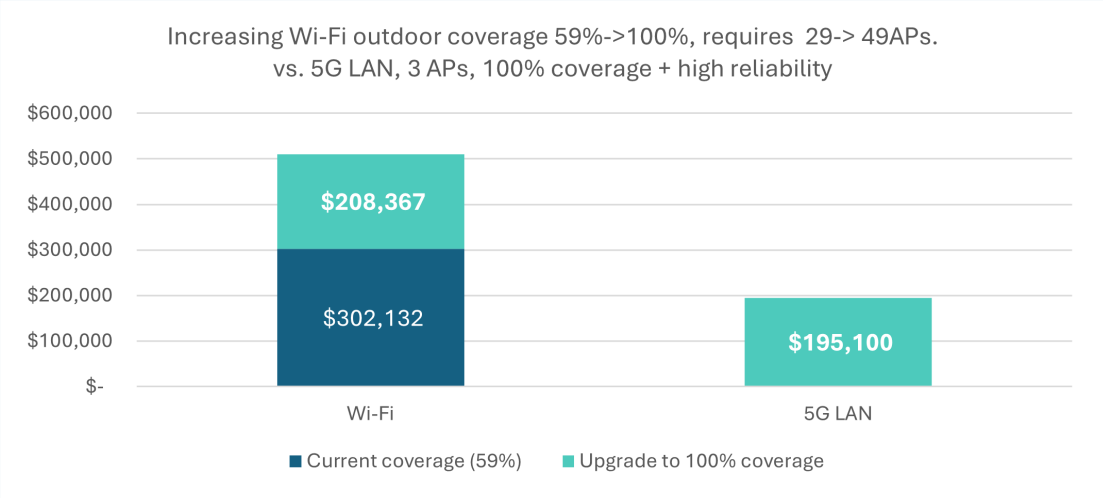
Opting to add more Wi-Fi access points to enhance coverage may initially appear to be the "easiest" solution, and it's no surprise if your traditional wireless vendor recommends this approach. But in many cases, this can exacerbate the problem and lead to:

- Increased RF interference, resulting in reduced performance of existing access points
- Heightened mobility issues as robots are transferred between access points more frequently
- Elevated costs associated with deploying additional hardware and cabling
- Greater operational complexities in managing the additional network element.

Instead, you could consider redirecting the same investment towards the appropriate wireless technology. Taking this approach often leads to cost savings within a year.

Here is an example where the cost is lower to add highly reliable 5G LAN than add more Wi-Fi at an outdoor yard.

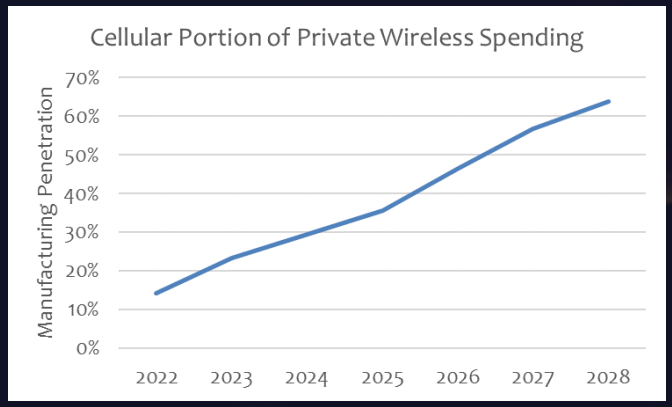
Find out more >



Why it's time for manufacturing CIOs to take action

Private 5G is a field-proven, industrial-grade wireless network solution purposefully engineered to tackle manufacturers longstanding and prickly networking challenges. They already deliver the control, security, and agility that manufacturers require to get their transformations back on track, and they will remain pivotal as they step in to handle increasingly demanding use cases.

By 2027, over half of wireless spending in factories will be directed towards LTE or 5G technology*, a notable departure from Wi-Fi, Zigbee, and other unlicensed approaches. The uptake of private 5G signifies a significant architectural shift for new factory plans, with new buildouts adopting these technologies, while the migration of the installed base will proceed at a slower pace.



Source: Mobile Experts

Since 2019, leading manufacturers such as BMW, Audi, Volkswagen, Siemens, Bosch, John Deere, and many others have piloted production lines, validating the benefits of LTE and 5G. As a result, these manufacturers have begun expanding the adoption of these technologies as mainline factories are built or upgraded.

Major technology shifts like these often create winners and losers. Choosing to make the investment in 5G will determine whether you lead your industry or risk being left behind by the status quo.

Assessing key architectural factors of Private 5G

We've discussed why a technology leader in manufacturing should embrace private mobile networks. Now, it's crucial to understand the key factors to consider when selecting your partner for this journey. Not all private mobile networks are created equal. Many solutions are still rooted in their origins as telco-built platforms for large public networks. Making the wrong choice can result in unfavorable outcomes and unfulfilled promises.

Let's explore these factors, why they matter and how to evaluate your choices.

Bespoke versus integrated | In the market, you have the option to select the components that comprise a private mobile network - namely, the radios, the "core," and the management system - and integrate them. Conversely, as the market has progressed from proof of concepts (POCs) to large-scale production networks, a few vendors now provide end-to-end solutions, akin to enterprise Wi-Fi. On paper, the bespoke model offers the advantage of providing the most flexibility and avoiding vendor lock-in. However, there are numerous hidden costs and challenges that warrant consideration.

- **Ongoing maintenance** - Consider a scenario where a new feature or a critical bug needs fixing. This often results in complex, multi-company discussions, intricate issue triangulation (and finger-pointing between vendors), coordination of release roadmaps, and management of upgrade cycles. For production-grade, mission-critical networks, this level of management is impossible to manage.
- **Cost of integration and interoperability** - While private 5G components are designed to be interoperable using standards, there is always the practical challenge of initial integration. Maintaining interoperability becomes even more crucial and complex as each component undergoes its own software lifecycle, incorporating new features and updates. Enterprise focused integrated architectures such as Celona's 5G LAN offer end-to-end solutions similar to existing enterprise Wi-Fi solutions. Each component has been designed and developed to seamlessly integrate with existing enterprise networks.

5G LAN Routing Whitepaper >

Security architecture | Private mobile networks come with robust built-in security features, including SIM-based authentication and over-the-air strong encryption. However, many solutions were not originally designed to seamlessly integrate with existing enterprise security architectures. In traditional telco-based private wireless architectures, existing firewalls may not have the same level of visibility into the devices and applications connecting to the private mobile networks. Given that this is unacceptable to enterprise organizations, there may be a need to invest in additional security equipment for the new network. Worse, your security teams will have to learn and build new systems to manage the networks security posture.

A better alternative is enterprise-focused solutions such as Celona's 5G LAN. In this case, the private mobile network seamlessly integrates with existing security infrastructure, requiring no changes or additions. In fact, it offers network and security teams deeper visibility and even more granular tools.

Read Security brief >

Network operations | Ongoing operations is a key consideration for building a private mobile network. Many vendors believe that these technologies are too complex for enterprise IT organizations to run by themselves and therefore can only be consumed as a managed service.

This limitation is isolated to products that have not been designed with enterprise IT in mind. An enterprise should have a choice of network operations - whether they self-manage, use a fully managed service, or pick from an à la carte set of services. We strongly recommend choosing an architecture that has been designed to offer this level of flexibility from the outset.

Celona Orchestrator ›

Device compatibility | Private mobile networks should be designed to accommodate as many use cases as possible. This requires interoperability with the broadest range of devices on the market. Over the past few years, Celona's device ecosystem has expanded significantly to include robust support from key players such as Apple, Zebra, Honeywell, Sierra Wireless, Digi, and many others.

It's essential to select a partner who has made substantial investments in building strong technical and business partnerships with a diverse array of companies. This way, you receive the best overall solution available in the market. At Celona, we firmly believe in the importance of these alliance partnerships to serve our customers. To facilitate this, we have dedicated over 2 years to our device certification program and boast the industry's broadest and deepest device partnership program.

Learn more about our device certification program ›

Spectrum strategy | It's important to develop a comprehensive global spectrum strategy that utilizes private spectrum where available and collaborates with local operators and spectrum owners as necessary. A partner with extensive expertise and experience in global spectrum management will be able to assist your team in navigating the complexities of spectrum allocation and utilization, ensuring optimal coverage and performance for your private mobile network.

Summary of key architectural factors

	Key architectural factor	How to assess
Bespoke versus integrated	Build approaches vary depending on each vendor and will impact ongoing maintenance and interoperability challenges	Consider the pros and cons of bespoke versus integrated solutions with a focus on ongoing issue resolution, network stability and long-term integration costs
Security	Integrating with existing security architectures may cause visibility issues, and/or require additional investments	Prioritize security considerations to ensure seamless integration and control
Network operations	Many vendors only offer managed service solutions, limiting the choice to self-management or service selection	Assess and select based on internal capabilities and network management preferences
Device compatibility	Not all networks are compatible with devices from major manufacturers	Prioritize device compatibility and range when selecting a vendor
Spectrum strategy	Developing a robust global spectrum strategy is key to optimizing network coverage and performance	Partner with spectrum management experts to develop your network performance strategy

Real life success: The business case for private 5G

The business value of private 5G is most effectively achieved through real-world examples. Below we showcase how manufacturing customers have benefited from private mobile networks utilizing the Celona 5G LAN architecture.

Case Study:

Del Conca

CUSTOMER:
Del Conca USA

VERTICAL:
Manufacturing (tiles)

LOCATION:
Loudon, Tennessee

CUSTOMER SIZE:
30-acre indoor/outdoor manufacturing facility

CHALLENGE:
Eliminate wireless network downtime, disruptions and reliability issues slowing down manufacturing, material handling, inventory control and order fulfillment processes.

Before with Wi-Fi

- **Unstable connections**
  Machinery, congested areas, and metal structures hindered Wi-Fi signals.
- **Connectivity issues with AGVs and forklifts**
  Disrupted work order receipt, longer loading times, errors, and time wasted searching for goods.
- **Additional maintenance**
  Worker communication via Push-to-Talk relied on a separate network.

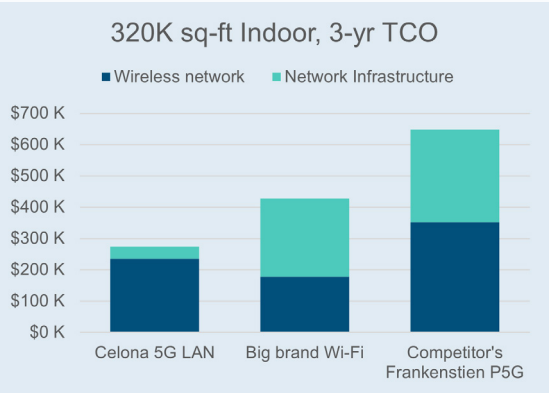
After with Celona

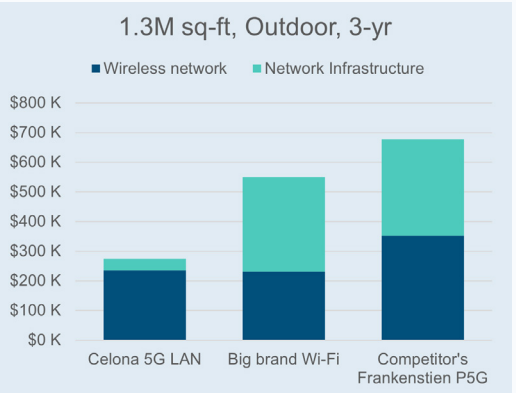
- **Extended range**
  Comprehensive coverage across the entire factory.
- **Support for autonomous vehicles**
  Automated Guided Vehicles (AGVs) and forklifts work seamlessly across the entire site.
- **Reliable and secure communications**
  Network connected eSIM-enabled smartphones and tablets.

Del Conca TCO comparison

- **Far fewer APs**
  Only 8 indoor APs and 4 outdoor APs to cover a similar area.
- **Lower installation costs**
  Outdoor APs mounted on buildings to cover yards, reducing trenching and cabling.
- **Less infrastructure**
  No need for additional routers, switches, or backhaul, unlike non-integrated PCN networks.

Read full case study ›





Case Study:

US Steel manufacturer

CUSTOMER:
U.S. Steel manufacturer

VERTICAL:
Industrial Manufacturing

LOCATION:
Pennsylvania

CUSTOMER SIZE:
Leading manufacturer and only producer of forged steel wheels for railcars and locomotives in North America

CHALLENGE:
Eliminate production disruptions, downtime, and process problems due to problematic wireless connectivity

Before with Wi-Fi

- **Unreliable signals**
  Caused by metal buildings, machinery, powerful magnets, and high temperatures.
- **Poor communication**
  Production staff couldn't efficiently exchange critical instructions with back-end database systems.
- **High network latency**
  Particularly when moving around the facility between Access Points.
- **Expensive disruptions**
  Five to six disruptions weekly in scrap yard operations resulted in approx. 264 disruptions per year.

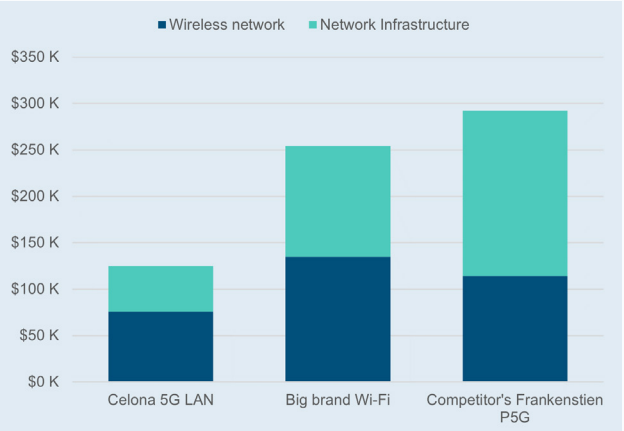
After with Celona

- **Fewer APs**
  Replaced six Wi-Fi APs in the scrap yard with one Celona private LTE outdoor AP.
- **Minimal disruptions**
  Less than five disruptions from the private cellular network occurred in the last 18 months.
- **70 times less downtime**
  Unplanned downtime in the scrap yard operation reduced significantly with ROI payback in under 3 months.
- **No network latency**
  Which means no more application disconnects.
- **Improved mobility**
  Reduced roaming disconnections.

TCO comparison

- **70% reduction in operational disruption**
  Compared to Wi-Fi saved over $2M in annual material/labor costs.
- **Less APs**
  4 to 6x fewer cellular wireless access points relative to Wi-Fi.
- **Total savings**
  3-year total network cost savings of 39% for indoor and 31% for outdoor.

Read full case study >



Case Study:

Manufacturing campus of a global auto maker

CUSTOMER:
Global luxury car maker

VERTICAL:
Automotive manufacturing

LOCATION:
United States

CUSTOMER SIZE:
20,000 employees with more than 30 production and assembly facilities

CHALLENGE:
Reliably connect automated yard trucks to enable just-in-time inventory management and manufacturing

Why Wi-Fi/Public cellular was not an option

A manufacturing plant spread out over 1.5 square miles (726 football fields), needed to deploy 20-30 driverless yard trucks to move trailers filled with auto parts from the storage yard to the plant for just-in-time manufacturing.

- The number of access points required and additional RF design requirements.
- The expense of trenching and providing fiber and power to each access point.
- Inconsistent connectivity for mobile devices crossing multiple access points.
- With public carrier services, data is metered, less secure and billed based on usage.
- Unreliable public cellular coverage.

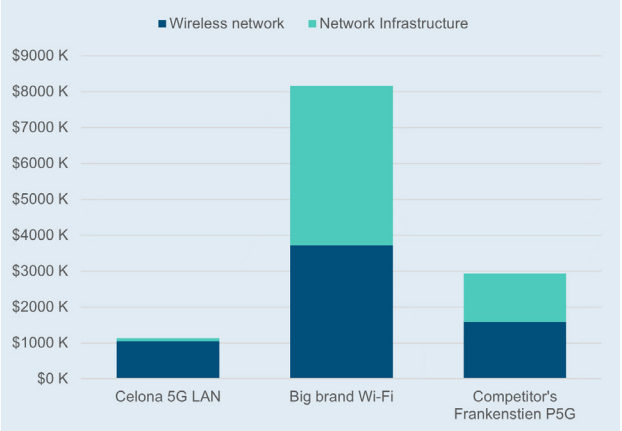
After with Celona

- **Full coverage**
  A low-latency, ubiquitous network across the entire 1.5 sq-mi facility.
- **High resilience to failures**
  Both RF and 5G core are in High Availability (HA), Active configuration, ensuring high resilience to failures.
- **High reliability outdoor network**
  Over 20 holter trucks operate autonomously throughout the property.
- **Data remains local**
  It's seamlessly integrated into existing enterprise network and IT policies.
- **New use cases**
  Support for 5G-native handheld scanners, ruggedized laptops, printers, push-to-talk communication devices, 5G wireless security cameras, and autonomous robots.

TCO comparison

- **Ubiquitous coverage**
  18 5G access points provide reliable coverage across the 1.5 square mile manufacturing facility.
- **Cost reduction**
  50 or more autonomous yard trucks operating at a fraction of the cost of wireless alternatives.

Read full case study >



Future proof your network with Celona private 5G

A large majority of manufacturers are stuck in connectivity purgatory, unable to rely on connectivity to adequately support their digital transformation efforts.

When compared to Wi-Fi alternatives, private mobile networks deliver a range of technical benefits such as reduced wireless interference, uninterrupted mobility of wireless clients as they move between wireless access points, and predictable performance with the ability to enforce specific latency and throughput service levels.

In this paper, we have only scratched the surface of what's made possible with Celona private LTE/5G networks.

To learn how industrial strength private wireless can enable true digital transformation, we recommend one of two options:

Calculate your TCO with Celona 5G LAN

Make an informed purchasing decision by estimating the cost-effectiveness of Celona 5G LAN compared to Wi-Fi and other private wireless solutions, based on inputs from your own manufacturing environment.

Learn more and try our TCO and ROI calculator >

Request an actionable proof of concept

Validate private wireless in your environment with a rapid proof of concept and see firsthand the power of our technology.

Learn more and register your interest >

ABOUT CELONA

Based in Silicon Valley, Celona is a pioneer and leading innovator of enterprise private wireless solutions. The company is credited with developing the industry's first 5G LAN system, a turnkey 4G/5G system that enables enterprises and mobile network operators to address the growing demands for more deterministic wireless connectivity for critical business applications and vital use cases not met by conventional wireless alternatives.

Celona's products and technology have been selected and deployed by a wide range of customers including Verizon, NTT, SBA Communications, Standard Steel, and Haslam Sports Group. To date, the company has raised $135 million in venture funding from Lightspeed Venture Partners, Norwest Venture Partners, NTT Ventures, Cervin Ventures, DigitalBridge and Qualcomm Ventures.

For more information, please visit celona.io and follow Celona on LinkedIn @ linkedin.com/company/celonaio

celona hello@celona.io

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