PRIVATE 5G DRIVERS & USE CASES IN MANUFACTURING

Leo Gergs
Principal Analyst

TABLE OF CONTENTS

INTRODUCTION: WIRELESS CONNECTIVITY SOLUTIONS IN MANUFACTURING

Recent years have been tumultuous for manufacturers, marked by the recent pandemic, geopolitical tensions, and economic uncertainty. These challenges have affected both consumers and businesses, driving up prices for energy and other resources due to heightened geopolitical tensions and exacerbating labor shortages, which have forced manufacturers to temporarily downscale or even halt production as a direct consequence of staff shortages. As a result, there is a pressing need for industries to adopt more digital and automated approaches to production and quality control, known as Industry 4.0. This shift is crucial for maintaining manufacturers' both short- and long-term profitability. Increased automation will reduce the reliance on manual labor, hence safeguarding business continuity. Furthermore, the increased digitalization will strengthen efficient production, meaning less costs per produced good.

In the framework of Industry 4.0, ensuring seamless connectivity and easy access to operational data is key to success. These elements are essential for adopting technologies such as asset tracking and the use of Automated Guided Vehicles (AGVs), or robotics, digital twins, connected work, and the connected factory. Currently, the main methods for achieving connectivity in manufacturing settings are through fixed or Wi-Fi connections. However, these approaches have their drawbacks:

This whitepaper has been sponsored by Verizon Business.

- Fixed connections require machines and sensors to be physically attached at specific points, making the expansion of facilities or the addition of new connections expensive due to the high costs associated with cable installation, which ABI Research estimates to be 70% to 80% of total connectivity installation expenses, including both hardware and labor.
- Wi-Fi technology, despite its presence in the industrial sector and the advent of Wi-Fi 6, faces challenges such as ensuring reliability, fast handover, and robust communication, which often necessitate the use of specialized access points and devices, leading to increased costs and a limited value chain.

Cellular connectivity, which follows a global standard and benefits from a comprehensive value chain, presents a compelling alternative. Cellular networks are characterized by their mobility, reliability, security, and capacity to support a high density of devices, outperforming other communication standards. The cellular ecosystem has also benefited from economies of scale for many years, making devices and connectivity modules more affordable.

COMMON CONNECTIVITY TECHNOLOGIES USED IN MANUFACTURING

Looking at the factory floor of today, wired connections are still the predominant way of connecting different production machines and components. At the same time, a high degree of technology fragmentation leads to a patchwork rug of connectivity technologies on factory floors, as Table 1 shows.

Table 1: Advantages & Disadvantages of Connectivity Technologies in Manufacturing
(Source: ABI Research)

CONNECTIVITY TECHNOLOGY	ADVANTAGES	DISADVANTAGES
EtherNet/IP	▪ High data transfer rates for real-time communication ▪ Reliable and stable connection for critical applications ▪ Standardization ensures compatibility between devices from different manufacturers.	▪ Maintenance of wired connections can be labor-intensive ▪ Wired infrastructure prevents flexible manufacturing & other dynamic processes
Modbus TCP/IP	▪ Simple implementation ▪ Widely supported across manufacturers, creating scalability effects. ▪ Compatibility with many industrial devices.	▪ Ethernet-based: Reliance on fixed-line connectivity ▪ Limited bandwidth, affecting performance in data-intensive applications ▪ Challenging to implement for large/complex networks
OPC UA	▪ Standardization promotes interoperability between devices and systems from different vendors ▪ Advanced security features ensure secure communication in industrial settings.	▪ Complex implementation, requiring a high degree of expertise ▪ OPC UA may require more resources compared to simpler protocols
PROFINET	▪ Support for real-time communication ▪ Easy scalability ▪ Provision of advanced diagnostics & maintenance measures ▪ Seamless integration with existing IT systems	▪ Complex implementation ▪ High initial deployment cost (incl. switches & devices) ▪ Specialized hardware required ▪ Resource intensive (bandwidth & processing power)
Wi Fi	▪ Enhanced security for manufacturing operations ▪ Cost-effective deployment of wireless connectivity ▪ Familiarity with industrial Wi-Fi provides an incumbent advantage	▪ Limited range compared to other connectivity options ▪ Potential for interference in crowded Wi-Fi environments ▪ Security vulnerabilities in certain implementations ▪ No robust handovers prevents high mobility use cases ▪ Sensitive to environmental factors, e.g., temperature

The widespread use of disparate technology and dependence on wired connections prevent manufacturers from fully leveraging the improvements and efficiencies promised by Industry 4.0. Understandably, manufacturers are hesitant to completely overhaul their current connectivity setups, given their proven reliability over many years; therefore, different wired and wireless connectivity technologies will continue to exist alongside each other. Moreover, upgrading these systems to modern standards involves extensive modifications to production equipment, which can be costly. Instead, manufacturers are encouraged to adopt connectivity technologies capable of integrating various protocols and existing automation systems into a wireless framework, thus overcoming the limitations of wired connections. In this context, 5G technology can play a crucial role for manufacturers on their path to digital transformation—particularly in greenfield deployments, where no reconfiguration and/or retrofitting would be necessary.

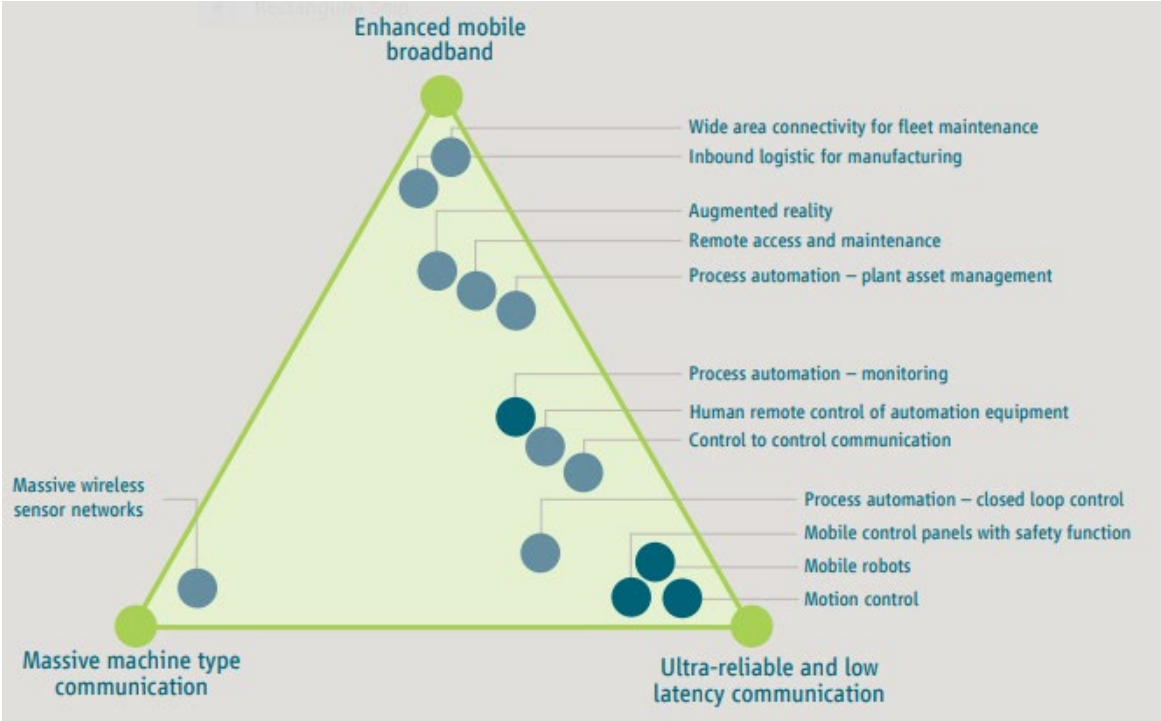
PRIVATE 5G CAPABILITIES FOR MANUFACTURING

When it comes to the manufacturing world, 5G connectivity offers three main capabilities that can enable a uniquely wide set of industrial use cases, namely Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communication (URLLC), and Massive Machine-Type Communication (mMTC).

Figure 1 presents the different manufacturing cases that can be addressed through 5G. The lighter the grey dot, the easier it is to implement the use case.

Figure 1: 5G Capabilities for Manufacturing

(Source: 5G-ACIA)



- **Enhanced Mobile Broadband (eMBB)** offers high bandwidth for large files, enabling applications like Ultra High-Definition (UHD) video, Augmented Reality (AR)/Virtual Reality (VR) training or remote operations for manufacturers.
- **Ultra-Reliable Low Latency Communication (URLLC)** enhances 5G with minimal latency and high reliability, vital for manufacturing applications needing constant connectivity and highly-critical applications, such as Condition-Based Monitoring (CBM) of hazardous environments or emergency shutdown/worker safety applications.
- **mMTC** expands device connectivity with 5G, supporting extensive sensor networks in manufacturing for monitoring large or hazardous areas.

NETWORK SECURITY & INTEGRITY

One of the key operational advantages of a private cellular network is the fact that access to this network can strictly be monitored and access will only be granted to authorized devices.

This ensures that no malicious device will enter the network and gives manufacturers full control over all devices accessing their communication infrastructure. Furthermore, deterministic networking and dedicated frequencies will reduce the overall number of devices present within the network. Wi-Fi operates on Industrial, Scientific, and Medical (ISM) bands, which are also used by 25% of industrial devices. As these devices must adopt a "listen before transmit" approach, requiring these devices to sense their environment before starting to transmit), this increases the vulnerability to jamming incidents.

Private cellular networks can use properly licensed mobile network spectrum, so devices are not constrained by the same mechanisms. Not only does this strengthen the network against jamming incidents, but it also bodes well for more reliable and predictable measures for network availability and latency, increasing overall connectivity reliability.

ROBUST HANDOVERS BETWEEN ACCESS POINTS

One of the most important shortcomings of alternative wireless connectivity technologies arises when devices move across the factory floor and signals need to be handed over from one access point to the other. When handing over these signals, the latency increases unpredictably high, meaning that manufacturers must factor this in when planning for highly mobile use cases that would enable a fully flexible factory floor.

Through a combination of advanced technical capabilities, private 5G prevents this unpredictable jump of latencies and provides what is referred to as robust handovers. On a practical level, this will allow manufacturers to operate any use case that requires a high degree of mobility—AGVs or Autonomous Mobile Robots (AMRs), for example—at a higher speed and with greater reliability.

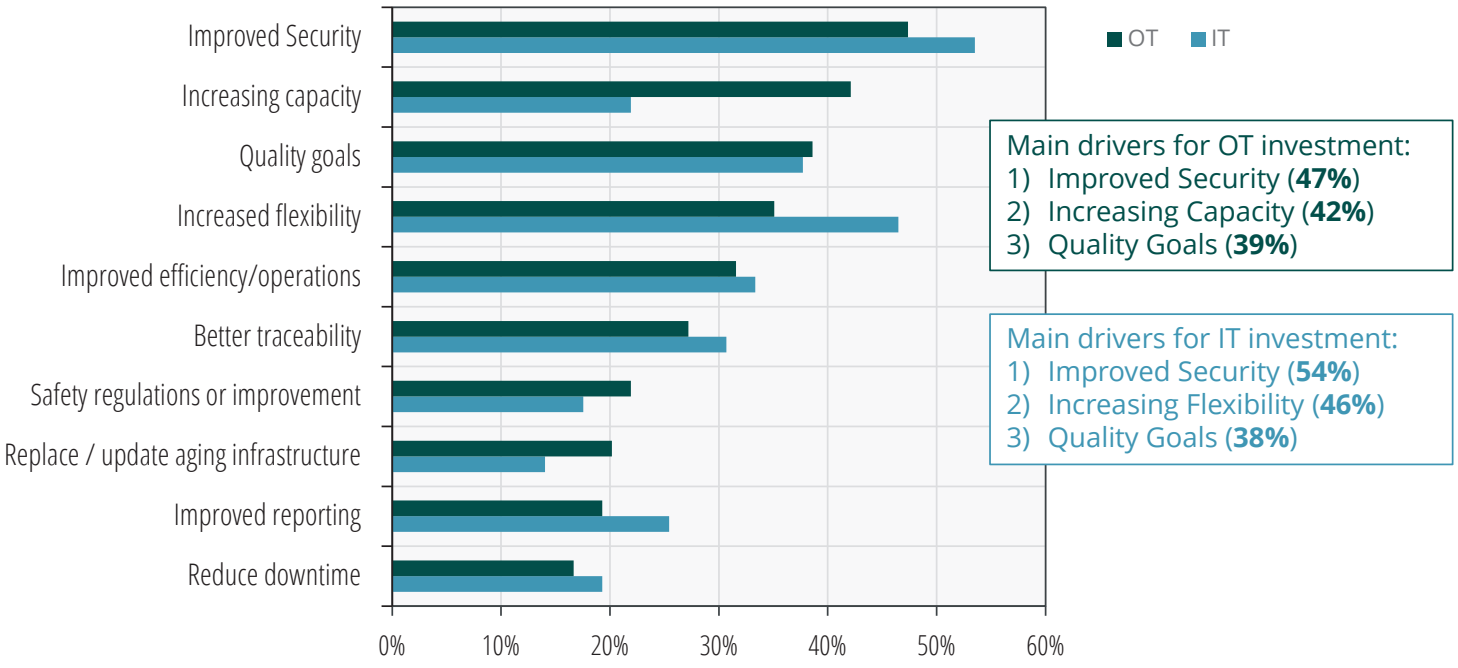
PRIVATE 5G USE CASES IN MANUFACTURING

The combination of eMBB, URLLC, and mMTC capabilities with deterministic networking enables private 5G for manufacturing use cases from two different dimensions. First, it allows addressing existing connectivity use cases in a much more efficient way than is possible with current connectivity alternatives.

Second, 5G capabilities allow manufacturers to address new safety and security use cases that had to rely on fixed-line connectivity before. As a survey among manufacturers in the United States undertaken by ABI Research together with the Digital Manufacturing and Cybersecurity Institute (MxD) shows, these use cases are on top of manufacturers' minds.

Chart 1: Investment Drivers for Manufacturers' OT and IT, N=114

(Source: ABI Research)



SECURITY APPLICATIONS & SAFETY PROVISIONING

By providing highly reliable, low latency communication, 5G allows manufacturers to automate and digitize highly safety-critical & emergency applications more effectively than other wireless alternatives. First, 5G will allow manufacturers to deploy **real-time surveillance and monitoring** across the entire production line. Second, 5G connectivity will allow the implementation of **secure remote access solutions for manufacturers' Internet of Things** (IoT) solutions. This also ensures that maintenance and monitoring activities do not compromise the integrity of the manufacturing process. This is especially crucial for operations requiring remote oversight or interventions.

Furthermore, the low latency guaranteed by private 5G will enable manufacturers to **automate emergency alerts**. Private 5G networks enable the swift dissemination of emergency alerts to devices and personnel within the facility, facilitating immediate action, whether evacuating affected areas or initiating lockdown procedures, which, so far, manufacturers had to do over wired fixed-line connections.

In addition, it allows for the remote control of safety systems and reliable communication in the case of power outages. The low latency and high availability of 5G connectivity allows manufacturers to control key safety systems remotely via private 5G networks, allowing for instant response actions, such as activating ventilation systems or emergency shutdowns, thereby mitigating risk and potential damage. Furthermore, private 5G networks can maintain operational communication channels even during power outages, ensuring that critical communications remain uninterrupted during emergencies.

CONNECTED WORKERS & WORKER SAFETY

In addition to safety and emergency applications, a private 5G network can also play an instrumental role in improving workers' safety by strengthening a fully connected workforce. A private 5G network is particularly well-suited as it provides comprehensive **coverage across entire manufacturing facilities** and reaches areas where Wi-Fi might struggle. The prevalence of metal infrastructure and production machines often poses a challenge to Radio Frequency (RF) waves. As private 5G networks emit waves at a higher power than Wi-Fi, 5G can reach the most remote production areas that Wi-Fi might not be able to reach.

Workers equipped with IoT devices, wearables, and mobile technology can access real-time data, machine status, and operational insights, facilitating informed decision-making and swift response to production changes or issues. This connectivity also supports the use of AR or VR for training and maintenance, allowing workers to perform complex tasks with greater accuracy and efficiency. Furthermore, the **robust security features of private 5G networks** can help manufacturers secure their most valuable production data in combination with dedicated security software solutions.

PROCESS & CONDITION-BASED MONITORING

Manufacturing environments are often particularly hazardous environments. The ability to continuously monitor manufacturing processes and the condition of production assets will be an important enabler for predictive and preventative maintenance. Consequently, it will be an important building block in manufacturers' strategies to strengthen their resilience and increase their business continuity efforts.

From a connectivity perspective, this carries two main requirements. First, any network needs to support many connected devices/sensors. After all, manufacturing processes are highly complex procedures, often involving several thousands of individual assets. Second, any wireless connectivity network also needs to be highly reliable and available at all times. These monitoring systems will be used to warn workers of hazardous conditions, so any network outage can potentially have devastating consequences.

By bringing mMTC and URLLC capabilities, 5G will be perfectly positioned to provide connectivity for enhancing the monitoring of manufacturing processes and conditions, contributing to important enhancements discussed in the next section.

ADDRESSING KEY CONCERNS: EXPERT Q&A FOR U.S. MANUFACTURERS

Although the benefits of a private 5G network for manufacturing operations is well studied by now, using cellular connectivity—5G specifically—for manufacturing processes is newer compared to established connectivity technologies like Wi-Fi. To help manufacturers gain confidence in deploying a private cellular network, this section will answer the most prominent questions.

How can private 5G improve operational efficiency and productivity in manufacturing processes?

Private 5G networks can significantly improve operational efficiency and productivity in manufacturing processes, as a look at existing deployments in the manufacturing space shows.

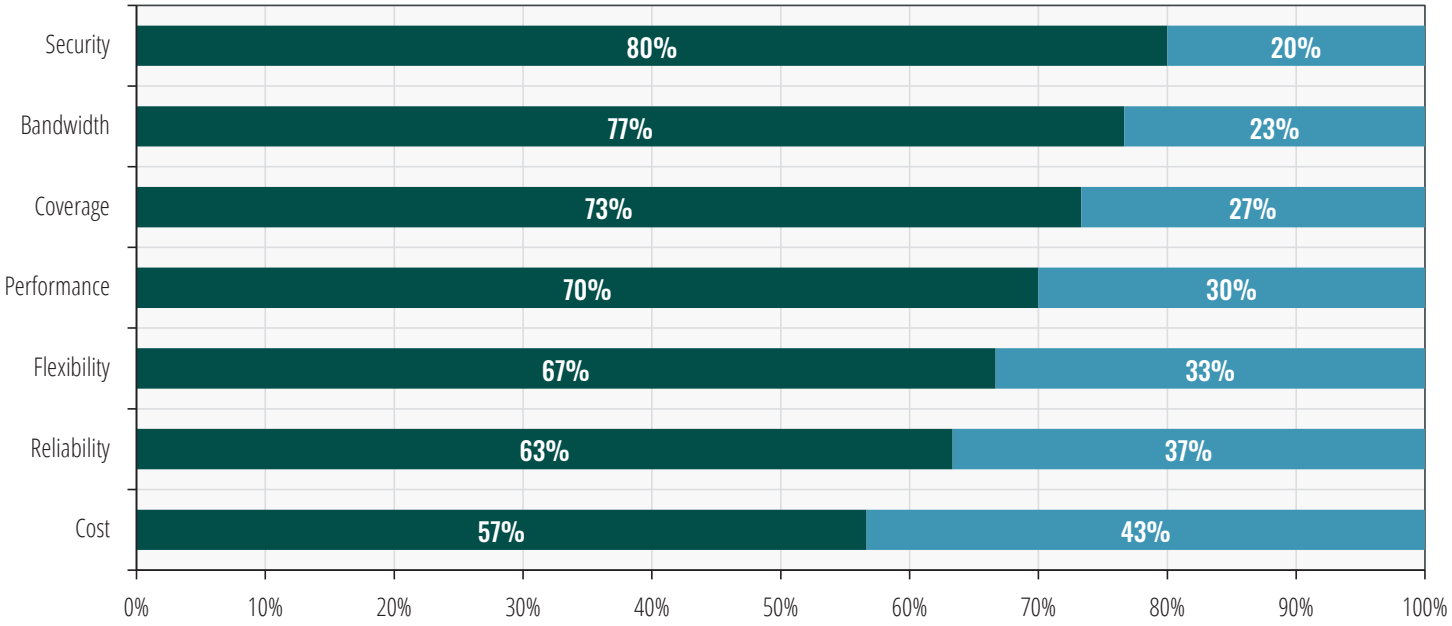
- Different ABI Research discussions with manufacturers conclude that facilities have seen **productivity improvements of up to 30% by minimizing downtime and optimizing operations** after deploying a private cellular network. In addition, robust handovers allow manufacturers to operate AGVs at 30% higher speed.
- According to ABI Research's qualitative research discussions, manufacturers have documented **reductions in operational costs, including energy savings of up to 20% and maintenance cost reductions of 25% to 30%,** driven by higher efficiency of operations, and predictive and preventative maintenance.
- With better connectivity, manufacturers can implement more comprehensive safety measures, including real-time monitoring of equipment and environments. As ABI Research has learned in qualitative discussions, this has led to a reported **decrease in workplace accidents, in some cases by more than 40%.**

What are the security advantages of private 5G networks compared to public networks or previous wireless technologies?

Compared to other wireless connectivity technologies, the deployment of a private cellular network offers a plethora of mechanisms to safeguard the network against unauthorized access. First, a private network requires specifically designated Subscriber Identity Module (SIM) cards to grant devices access to that network, creating an additional physical layer of security. Furthermore, the deployment of a private 5G network allows all connectivity infrastructure to remain on enterprise premises. Therefore, all sensitive networking data can remain on the manufacturing site and can be clearly separated from any public network using a combination of traffic segregation, encryption, and granular access controls.

But all this theoretical talk would be nothing without the experience of fellow manufacturers. As Chart 2 illustrates, U.S. manufacturers that have already deployed a private cellular network for their operations are particularly satisfied with the sophisticated security provision.

Chart 2: Satisfaction with Enterprise Cellular, N=86
(Source: ABI Research)



How scalable and flexible are private 5G networks to meet future expansion needs or adapt to new manufacturing technologies?

Private 5G networks offer a significant level of scalability and flexibility to meet the evolving demands of future expansions or the integration of new manufacturing technologies. Built on a foundation designed to support a vast number of devices and high-speed data transmission, these networks can easily accommodate the growing number of IoT devices and sensors used in modern manufacturing processes. Furthermore, the architecture of private 5G networks is inherently adaptable, enabling businesses to tailor their network infrastructure to specific operational needs. Furthermore, the capabilities of network slicing allow adjusting the network size and performance without having to deploy new infrastructure.

To take full advantage of that, private network management software solutions can help manufacturers easily operate the network and scale it to meet their needs. Not only does this include adding new end devices or commissioning new network slices, it also includes incorporating new applications and targeting additional use cases.

What is the anticipated Return on Investment (ROI) for deploying a private 5G network, and what are the cost considerations?

To be able to assess the value of a private 5G network, manufacturers should not only look at the ROI, but also the Cost of Inaction (COI)—in other words, the additional revenue that they would miss out on by not deploying a private 5G network. ABI Research has modeled both ROI and COI.

Key findings of the modeling exercise, published in a dedicated whitepaper, **Unlocking The Value Of Industry 4.0,** suggest that over a 5-year period, a U.S.-based electronics manufacturer that adopts private cellular will realize the following benefits:

- **A 7.6% increase in gross profit margin**
- **An operational cost savings (including labor efficiencies) of US$1.05 billion**
- **A ROI of US$49.3 for every US$1 spent**

HOW TO GET STARTED: A GUIDE TO DEPLOYING PRIVATE CELLULAR NETWORKS

The discussions within this whitepaper showed that wireless connectivity technology deployment should be the end point to a carefully carved out digital transformation process. Therefore, the discussions from this report lead to important strategic recommendations on how manufacturers should plan this journey to ensure it leads to the desired outcome.

1. PRE-DEPLOYMENT

Define use cases and technology capabilities

Manufacturers should assess IoT applications and use cases for a private 5G network by analyzing costs and benefits, including automation impacts and identifying bottlenecks such as downtime and rewiring costs. Understanding key areas like real-time monitoring and autonomous vehicles is vital for optimizing the network. Financially, they need to weigh the investment in self-managed networks against the cost savings of partnering with managed service providers. Manufacturers should plan for a gradual expansion of the private network deployment—not only in terms of coverage area, but also in terms of use cases addressed. Consequently, manufacturers should develop a thorough understanding of which use cases they want to realize and when. Their immediate focus should be on private networks in greenfield deployments to avoid unnecessary complexities. Technology partners like Verizon can then translate these use cases into technology requirements and plan out an upgrade/retrofitting path for brownfield deployments.

Plan the network & partnership strategy

After identifying key use cases, manufacturers should proceed with planning the network deployment, focusing on determining the necessary coverage area and setting a specific timeline to ensure accountability. Additionally, manufacturers must decide between a Do-It-Yourself (DIY) approach—handling the deployment, management, and operation of the network themselves—or partnering with a managed service provider for a comprehensive solution that frees them from the complexities of network planning, allowing them to focus on production.

Design the network

Manufacturers advancing to network design must tackle key decisions, including choosing the cellular network spectrum best suited to their needs, influenced by trade-offs in coverage and data rates:

- Low band spectrum offers broad area coverage.
- High band (Millimeter Wave (mmWave)) spectrum delivers high data rates, but limited propagation.
- Mid band spectrum presents a balanced choice, providing substantial coverage and throughput.

This step requires careful RF planning to align infrastructure with coverage and use case needs. It is crucial to define the network infrastructure, including end devices, cloud components, security systems, and SIM cards. Establishing an operating model for monitoring, updates, and repairs, along with negotiating Service-Level Agreements (SLAs) with vendors are key to maintaining network reliability and performance.

2. DEPLOYMENT & COMMISSIONING

Install cellular connectivity infrastructure

In the initial phase of deployment and commissioning, manufacturers are tasked with setting up the connectivity infrastructure, which involves installing small cells, and implementing the required Information Technology (IT) and cellular core network infrastructure. Given that network equipment comes from various vendors, the integration process may be complex and extend over several days. Additionally, provisioning SIM cards and integrating industrial end devices for specific use cases into the network is crucial for ensuring comprehensive connectivity.

Initial post-deployment tests & commissioning of the network

After the infrastructure is in place and integrated, it is essential to conduct thorough testing to confirm everything works as intended. This involves not only checking each networking component on its own, but also ensuring they work together seamlessly. Using software with user-friendly interfaces can facilitate this process. Following successful interoperability tests, the network is ready to be deployed across production units for real-time commercial use.

Create the right structures to operate the network

After the infrastructure is in place and integrated, it is essential to conduct thorough testing to confirm everything works as intended. This involves checking each networking component on its own, and ensuring they work together seamlessly. Using software with user-friendly interfaces can facilitate this process. Following successful interoperability tests, the network is ready to be deployed across production units for real-time commercial use.

Ensure warranty & support arrangements

In addition to setting up internal mechanisms for managing and operating the cellular network, manufacturers must secure warranty agreements with component vendors for level-2 support and higher. Choosing the right partners, such as managed service providers, can alleviate the burden on manufacturers by including installation and commissioning services in their offerings.

3. POST-DEPLOYMENT

Continuously monitor network performance and adjust

After deploying their private 5G networks, manufacturers must implement a system for monitoring and optimizing network performance, using predefined Key Performance Indicators (KPIs) such as availability, reliability, data rates, and latency. They can leverage existing solutions from leading test and measurement providers, avoiding the need to develop these systems from scratch. Network service providers like Verizon will be prepared to provide manufacturers with the required SLAs to make sure that manufacturers can focus on what they are best at—manufacturing products—without having to worry about network operation and performance. Additionally, identifying and proactively addressing areas for improvement is crucial for a future-proof network. Software solutions, including Artificial Intelligence (AI) algorithms, can facilitate network expansion simulations and the creation of a digital twin to assess potential impacts on performance without real-world testing.

Private 5G networks offer significant opportunities for manufacturers to digitize operations and enhance communication infrastructure as part of a broader digital transformation strategy. However, with ongoing advancements in cellular technology, manufacturers should partner with experts linked to the telecoms industry to ensure their network remains upgradable and future-proof, facilitating the transition from wired to wireless connectivity in factory settings.

Published May 2024

157 Columbus Avenue 4th Floor

New York, NY 10023

+1.516.624.2500

About ABI Research

ABI Research provides actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today. ABI Research's global team of analysts publish groundbreaking studies often years ahead of other technology advisory firms, empowering our clients to stay ahead of their markets and their competitors.