

WIRED TO WIRELESS CHANGE GUIDE

Leo Gergs, Principal Analyst

ABiresearch
THE TECH INTELLIGENCE EXPERTS™

Betacom



TABLE OF CONTENTS

**INTRODUCTION:
DIGITAL TRANSFORMATION
IN MANUFACTURING**..... 1

**KEY DRIVERS FOR DIGITAL
TRANSFORMATION & THE NEED
FOR WIRELESS CONNECTIVITY**..... 3

**CELLULAR CONNECTIVITY IN
MANUFACTURING: WHY SHOULD
WE CARE?** 5

**MANAGING INDUSTRIAL
TRANSFORMATION: FROM WIRED
TO WIRELESS CONNECTIVITY** 11

**A GUIDE TO DEPLOYING PRIVATE
CELLULAR NETWORKS** 15

**STRATEGIC RECOMMENDATIONS
FOR MANUFACTURERS**20

INTRODUCTION: DIGITAL TRANSFORMATION IN MANUFACTURING

Looking at today's factory floor, it becomes apparent that fixed-line connectivity is still the name of the game. Industry 4.0, however, calls for a technology upgrade, establishing a more automated factory through wireless cellular connectivity. Connectivity is a key element of hyper-efficient manufacturing operations, and it is crucial to have a singular connectivity protocol that provides ubiquitous connection to all the devices and machinery on the factory floor. The more industrial and manufacturing firms use common standards in their connectivity solutions, the more they eliminate points of friction between robots, systems, and controls to connect to mission-critical processes. Smart manufacturing connectivity should enable the combination of high mobility, high throughput, and low latency to support increasingly automated production processes.

Current macroeconomic conditions—fueled, in part, by geopolitical events—also put manufacturers and their supply chains into a difficult position, as Figure 1 shows.

Figure 1: Geopolitical Effects and Their Impact on Macroeconomic Conditions

(Source: ABI Research)



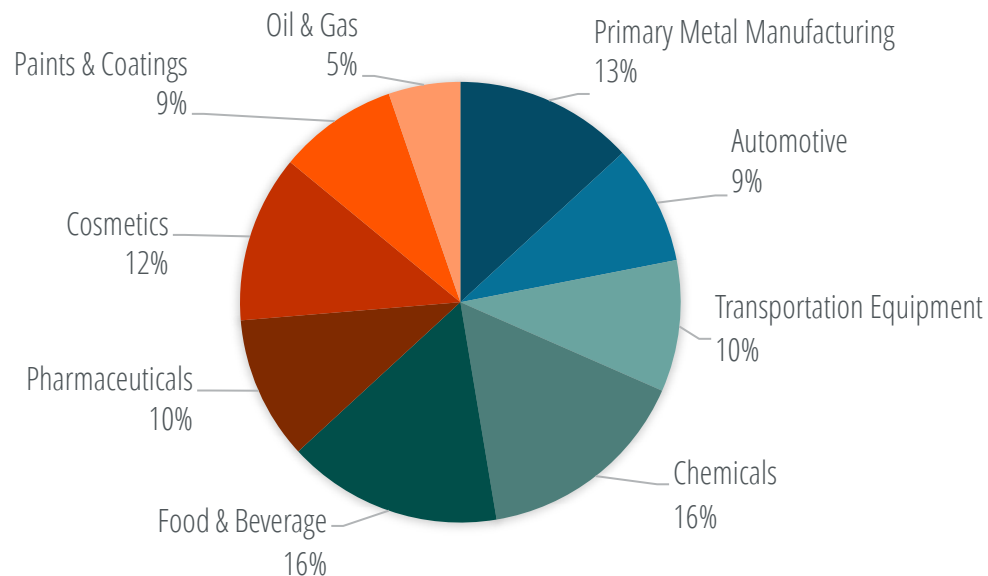
To remain competitive, industrial and manufacturing firms need to invest in digital transformation and evaluate the technology needed to best support these reengineering efforts for maximum Return on Investment (ROI). This whitepaper provides recommendations as manufacturers consider the move from wired to wireless operations.

To inform this paper and gain valuable insights from industry decision makers, the Digital Manufacturing and Cybersecurity Institute (MxD), together with its partners Betacom and ABI Research, conducted a survey among more than 100 decision makers within automotive, metal/steel, and process manufacturing sites in the United States. Key survey findings are included here, offering manufacturers insight into strategic considerations for making the best possible decision on how to support their digital transformation efforts.

Chart 1 reports basic demographics of the survey, which allows the reader to better understand and interpret the results in the context of this guide.

Chart 1: Demographics of the Survey by MxD, Betacom, and ABI Research

(Source: ABI Research)



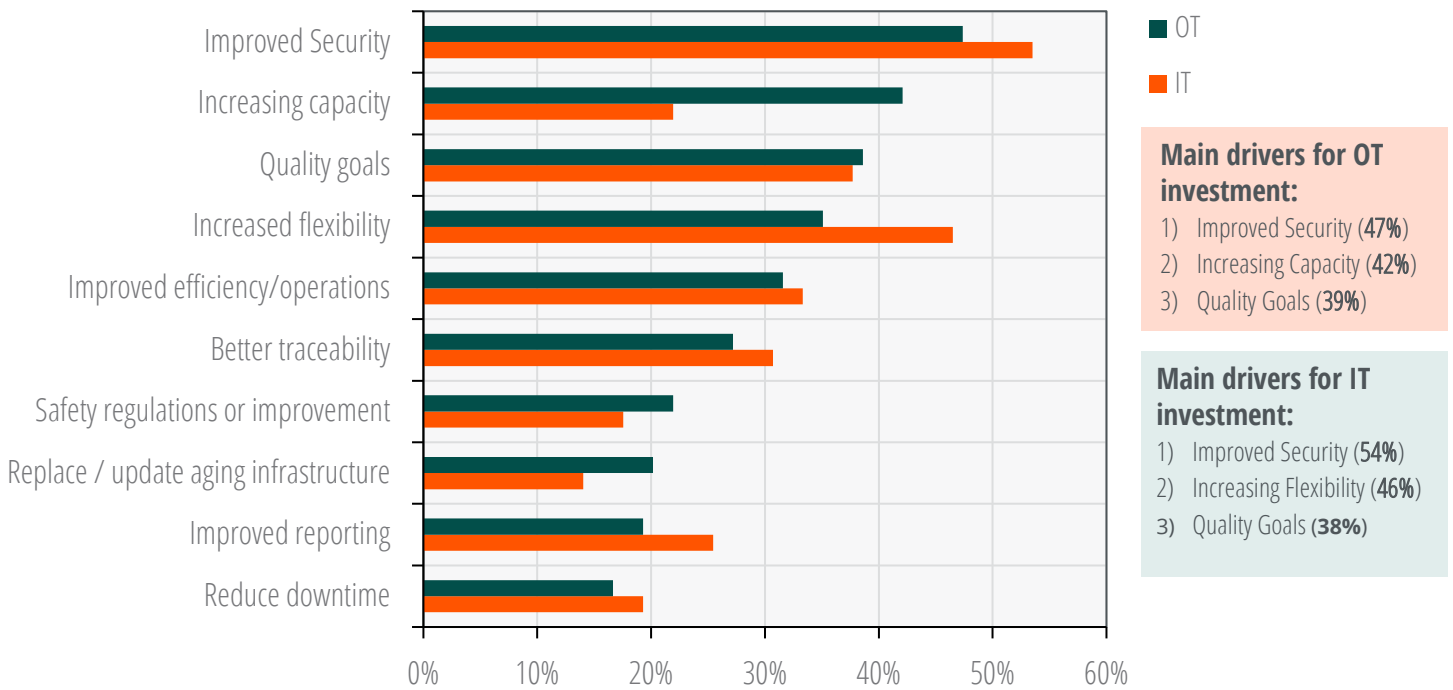
KEY DRIVERS FOR DIGITAL TRANSFORMATION & THE NEED FOR WIRELESS CONNECTIVITY

Industry 4.0 promises factory owners increased efficiency due to a flexible factory layout, opportunities around automated quality control of finished products, predictive and preventative maintenance of production machines, and safety monitoring by using massive wireless sensor networks, Machine Vision (MV), and Artificial Intelligence (AI) capabilities. In this context, providing connectivity to the factory floor becomes increasingly important to enable the growing automation of production processes and transmission of large amounts of data.

As Chart 2 shows, the survey among manufacturers in the United States identifies that digitalization priorities are similar between respondents from Information Technology (IT) and Operational Technology (OT) backgrounds. Both consider security, capacity/flexibility, and quality improvements as their top priority. This means that both IT and OT departments should work together, combine their forces and investment capabilities, and decide on one common connectivity layer to support their digitalization efforts.

Chart 2: Investment Drivers for OT and IT, N=114

(Source: ABI Research)



THE ROLE OF WIRELESS CONNECTIVITY IN THE INDUSTRIAL DIGITIZATION JOURNEY

Even though fixed-line connectivity is well established within manufacturing (ABI Research finds that, currently, only 14% of all connections in industrial manufacturing are wireless), so connecting machines wirelessly becomes increasingly important as it offers distinct advantages. First, production processes become increasingly complex. Automotive manufacturing, for example, is tasked with a growing demand for customization, while process manufacturers face more and more small batch production, requiring more flexibility. All in all, the number of components requiring a connection is constantly increasing. Validated by several discussions with assorted

manufacturing enterprises, ABI Research estimates that a manufacturer faces an average cost of US\$225 per cable drop, which translates to hundreds of thousands of dollars (US\$), assuming that there are at least 50 cable drops per factory. Furthermore, wired connections on constantly rotating machine components need to be replaced frequently, incurring additional deployment costs. All of this underlines the growing importance of wireless connectivity on the factory floor.

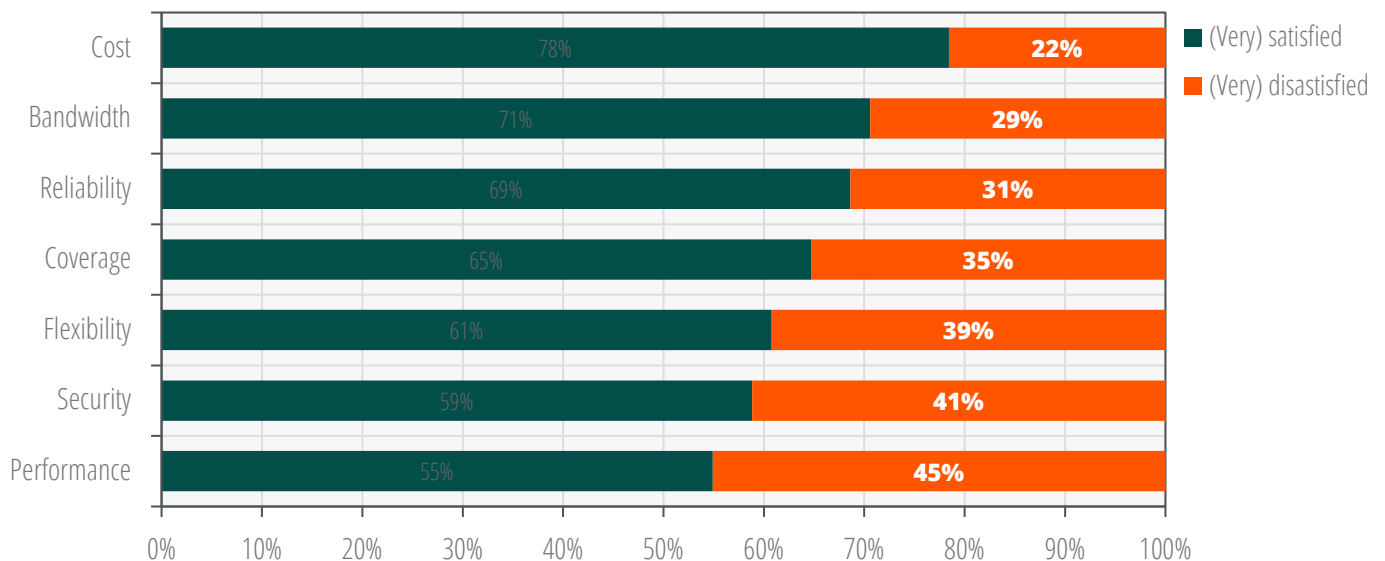
SATISFACTION WITH WI-FI

Wi-Fi provides one of the possibilities for wireless connectivity on the factory floor, based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. Given its compatibility with wired Ethernet (often referred to as wireless Ethernet) and the fact that Ethernet-based automation networks, such as PROFINET or Modbus, are still significantly used on the factory floor, one of the clear advantages of using Wi-Fi is that it allows any of those Ethernet-based machines or devices to be configured wirelessly. However, it uses frequencies on the Industrial, Scientific, and Medical (ISM) bands, which are used by one-fourth of industrial devices, resulting in a high risk of interference. Furthermore, devices using the ISM bands are required to employ what is often referred to as “listen before talk” (or “listen before transmit”), whereby a radio transmitter first needs to sense its radio environment before it starts a transmission. Waiting for this sensing of the environment introduces an additional source of latency in the machine communication and results in a breakdown of the network in case of a jamming incident.

Consequently, Wi-Fi receives particularly high scores from manufacturers when it comes to cost and bandwidth considerations, while it lags behind in aspects like performance and security, as Chart 3 shows. This is mainly due to issues with mobility use cases, as the transmission of connectivity from one access point to another can result in unpredictably high latencies, and poor outdoor coverage. Furthermore, indoor access points would need to be deployed a lot more densely to achieve at least similar coverage levels as private 5G.

Chart 3: Satisfaction with Current Wi-Fi Technologies, N=114

(Source: ABI Research)

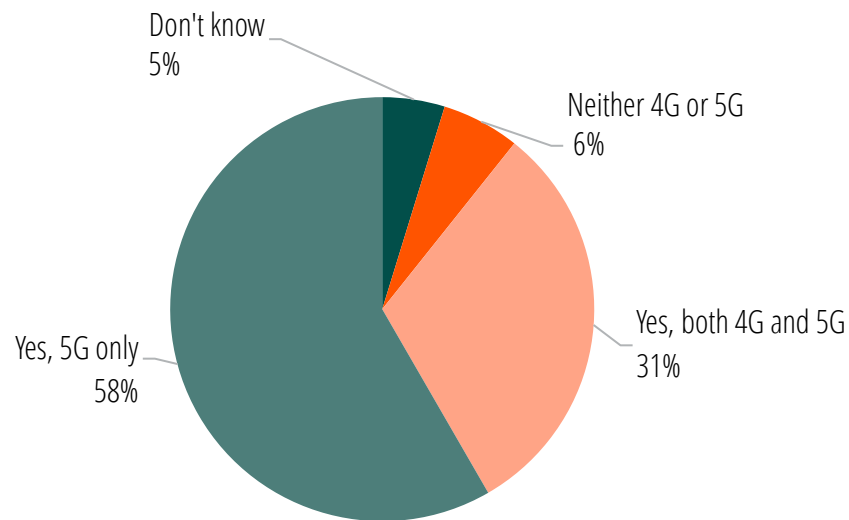


THE ROLE CELLULAR CONNECTIVITY PLAYS IN MANUFACTURING TRANSFORMATION

Because of its unique capabilities, as discussed at length in Section 3.1.1, private 5G can become an integral part of a manufacturer's transformation and digitalization strategy. In fact, discussions with manufacturing enterprises (specifically in automotive, aerospace, and process manufacturing) support this assumption. As Chart 4 shows, the interest in deploying private cellular for manufacturers is high. This shows that cellular connectivity already plays a key role in enabling manufacturers' digitalization projects.

Chart 4: Manufacturers' Plans for Investing in Private Cellular, N=114

(Source: ABI Research)



There is a general interest in using cellular connectivity for manufacturing transformation. At the same time, it should also serve as a critical call to action for manufacturers to use this current exploratory phase to identify realistically achievable use cases. Advanced features like Ultra-Reliable Low Latency Communication (URLLC) and full support for Time-Sensitive Networking (TSN) require specific chipsets and devices that are not expected to emerge until 1Q 2024.

CELLULAR CONNECTIVITY IN MANUFACTURING: WHY SHOULD WE CARE?

Several connectivity technologies can deliver some of these requirements, such as industrial Wi-Fi, often referred to as Industrial Wireless Local Area Network (IWLAN), which is a proprietary extension to conventional Wi-Fi from one of the prominent factory automation vendors—Bluetooth, and other Internet of Things (IoT)-specific technologies. This approach, however, inevitably results in the factory operator having to employ a multitude of different connectivity solutions on the factory floor, leading to an unnecessarily high amount of infrastructure investment needed to deploy each connectivity system. When digitalization first hit the manufacturing sector, manufacturers connected machines via Ethernet, and then used Wi-Fi to connect their IT and workers' tablets, and used Bluetooth for beacons. As machines and other production equipment have a very long lifecycle of several decades, all of these different connectivity technologies still exist on the factory floor today and concurrently managing them individually consumes workers' resources.

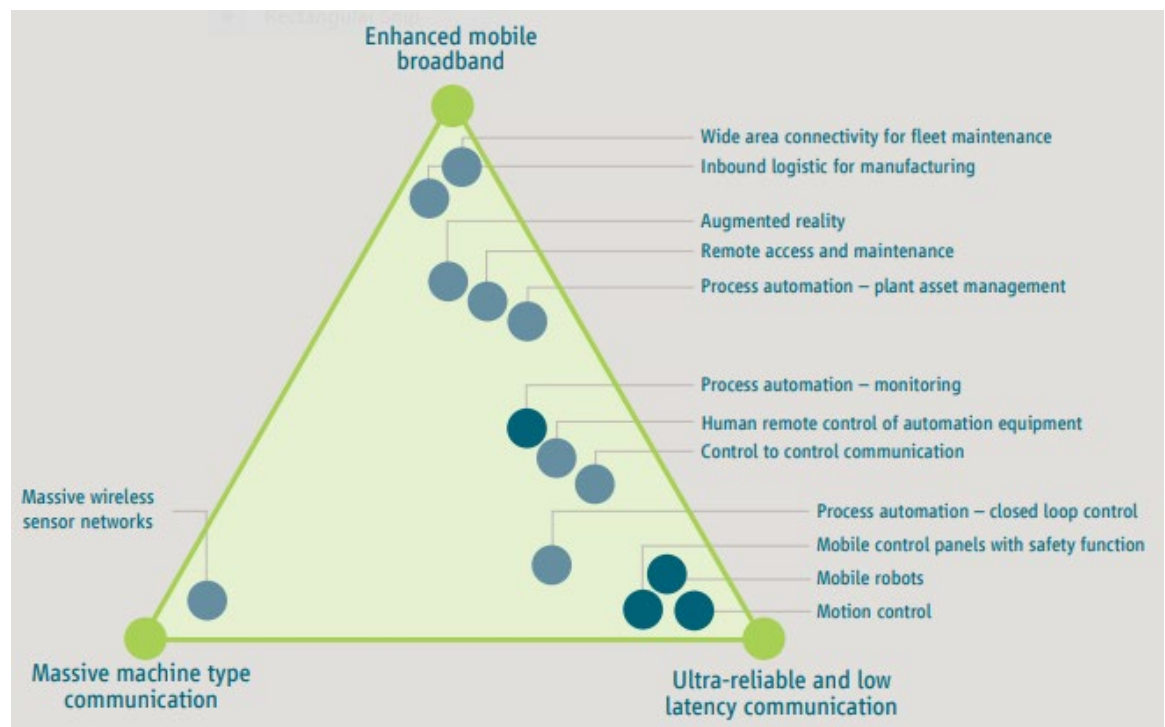
From a technology point of view, non-cellular connectivity technologies like Wi-Fi often use unlicensed spectrum, which compromises reliability and predictive latency, so they cannot be used for business-critical applications. By providing dedicated spectrum, cellular connectivity offers a high degree of data safety and network integrity by design. Latency can also be brought down to a minimum, which is arguably even more important for guaranteed business continuity on a predictable basis. Furthermore, Wi-Fi is lacking in terms of security provision, mainly due to two factors. First, the so-called ISM bands, which Wi-Fi devices use for spectrum, are open to everyone. Without additional security solutions, the network would remain open for unauthorized access. Second, devices on the ISM bands must employ what is often referred to as “listen before transmit,” whereby a radio transmitter first needs to sense its radio environment before it starts a transmission. Waiting for this sensing of the environment introduces an additional source of latency in the machine communication and leaves the network vulnerable to jamming incidents.

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 2: 5G Capabilities for Manufacturing

(Source: 5G-ACIA)



- **Enhanced Mobile Broadband (eMBB)** describes the provision of particularly high bandwidth for transmitting data-intensive files. For manufacturers, eMBB will enable data-intensive applications, such as 4K/8K Ultra High-Definition (UHD) videos, Augmented Reality (AR)/Virtual Reality (VR), cloud gaming, and enhanced mobile media.

- **Ultra-Reliable Low Latency Communication (URLLC)** is arguably the key enabler for 5G to support innovative use cases for manufacturers. In addition to particularly low latencies (in the range of several milliseconds), the high availability and reliability renders 5G as an interesting connectivity technology for particularly critical use cases that require a constantly available network.
- **Massive Machine-Type Communication (mMTC)** describes the density of supported connections. With 5G, manufacturers will be able to connect a much larger number of devices than with Wi-Fi or previous generations of cellular connectivity. This enables deploying, for example, large sensor networks for condition-based monitoring of hazardous production areas or large outdoor facilities, such as oil & gas fields.

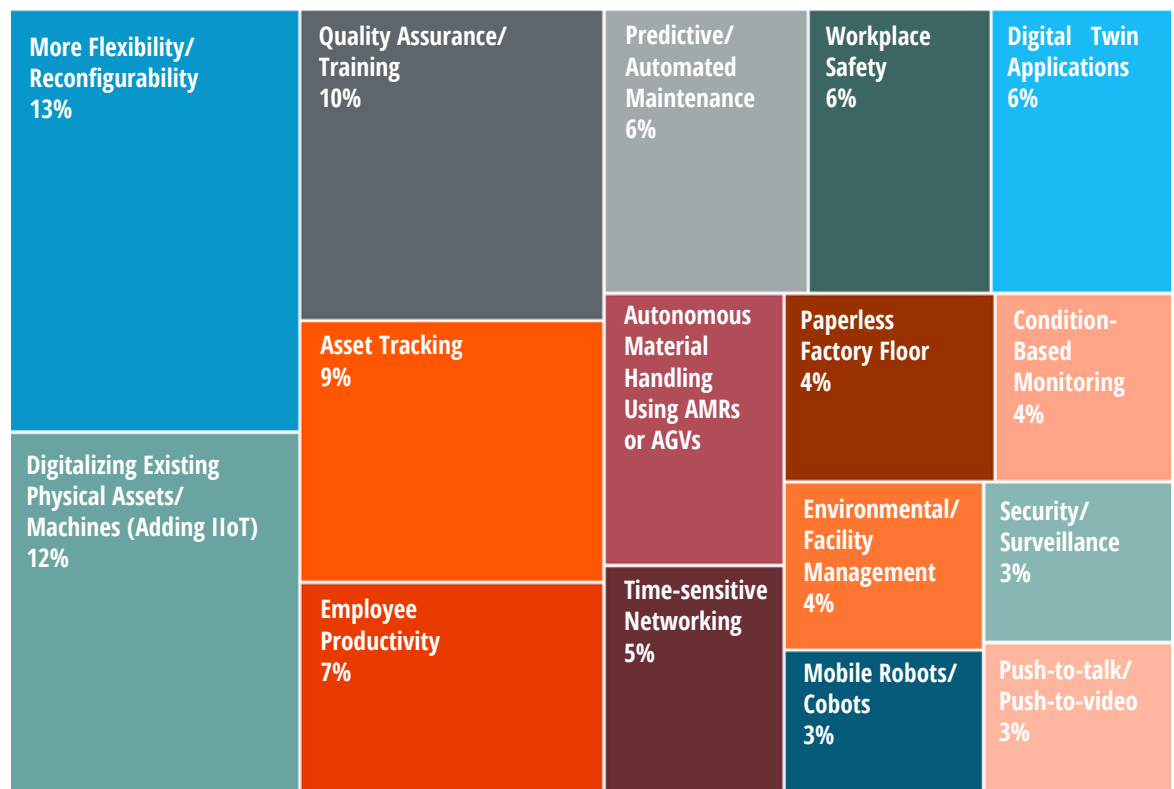
5G's unique feature set can make 5G an umbrella technology that manufacturers use to address a range of both critical and non-critical use cases on their factory floors. Therefore, 5G connectivity can help manufacturers replace the current patchwork of different technologies and instead manage and operate processes concurrently.

5G USE CASES FOR MANUFACTURING

5G connectivity is particularly well suited for very critical, highly mobile use cases. As found during the survey (see Figure 3), manufacturers are expecting to predominantly address flexible and reconfigurable manufacturing, digitize physical assets (e.g., the Industrial IoT (IIoT)), and ensure quality assurance use cases by deploying private cellular connectivity.

Figure 3: Anticipated Use Cases for Enterprise Cellular, N=86

(Source: ABI Research)



Enterprises currently considering transforming their operations should use these as a guide and consider private cellular connectivity, particularly for use cases that either require a high degree of flexibility (e.g., flexible manufacturing lines or the use of Automated Guided Vehicles (AGVs) and Autonomous Mobile Robots (AMRs)) or highly-critical use cases (e.g., emergency shutdown, condition-based monitoring, or emergency push-to-talk/push-to-video use cases), while other applications could be sufficiently served with other technologies like Wi-Fi. Automotive, metal forging, and process manufacturing are emerging as the most interesting sectors for private 5G deployments in the short term, so the remainder of this section discusses the most prominent use cases for these three sectors.

Automotive Manufacturing

The need for flexible manufacturing is particularly high within the automotive sector, as rigid production lines—and, therefore, reliance on fixed-line connectivity—entails important shortcomings. In today's world, cars are increasingly customized products based on end customers' requirements, so they need to be fitted with different components. Juggling these tasks, in addition to a particularly fast production pace, strains production line workers. Furthermore, this is a potential source for errors, as every wrong pairing of components and car model will need to be corrected. A flexible factory layout with moving production units/workstations can make working in these environments much more stress free and less prone to mistakes, minimizing the amount of preventable machine downtime.

In this context, 5G can be used as a connectivity technology to power AGVs and AMRs to create a modularized production layout and provide the foundation for a fully flexible manufacturing layout. This becomes even more important, as cars become smarter and more complex, requiring several thousand different components. AMRs, in this context, will be much more efficient and accurate in providing and mounting all of these individual components.

Steel/Metal Manufacturing

To make industrial production more sustainable, steel and metal manufacturing has a particularly long way to go. Calculations from the International Energy Agency (IEA) suggest that the production of 1 ton of steel results in emitting 1.4 tons of Carbon Dioxide (CO₂), due to current crude steel production. 5G connectivity can play an integral role in reducing emissions and leading to more sustainable steel production.

First, 5G can enable the large-scale adoption of smart roller loaders. These can be fitted with MV technology that compares actual footage with an AI algorithm to ensure proper functionality. The grinding of metal and steel typically generates exceptionally high temperatures, which, in a traditional setting, must be controlled by three staff members. As 5G connectivity helps reliably monitor their condition by using MV in combination with AI algorithms, it allows the remote operation of these roller loaders. While in a traditional setting, three engineers are needed to monitor one roller, 5G allows one engineer to operate one intelligent roller loader remotely. Even though these rollers are not mobile, 5G connectivity is an important enabler for large-scale deployment, as the transmission of MV data requires high bandwidth with as low latencies as possible.

Second, stacker reclaimers are used to transfer coal ore and iron ore in the stockyard, with workers usually operating them outdoors in the open, where they are exposed to strong sunlight, coal powder, and ore dust. The stockyard environment is harsh, and operators need to climb into the cab on top of the vehicle to control the crane. This results in very inefficient operations in particularly harsh environments. By providing the needed networking reliability, as well as low latencies even for outdoor deployments, 5G can enable remote control of these stackers, increasing efficiency considerably. Furthermore, 5G can be used to control welding operations as they happen or enable the automatic identification of steel coil Inside Diameters (IDs).

Process Manufacturing

Process industries (including chemicals and oil & gas) find themselves under immense pressure, fueled by current macroeconomic conditions and recent geopolitical events. Furthermore, extraordinary global events, such as the outbreak of the COVID-19 pandemic, highlighted the importance of a fully transparent supply chain to anticipate sudden changes in demand and supply, adjusting production accordingly. What is true for every manufacturing segment holds particular importance for process industries—unplanned downtime is the enemy of productivity. Therefore, reliability, availability, and predictability are much more important technological capabilities than the provision of extremely low latencies.

Pulp and paper mills are characterized by large single pieces of machinery converting wood pulp into paper-based products. Process industries are embracing sustainability by using recycled materials and have clearly embraced the circular economy. Despite these steps, the giant machines within a paper mill are a single point of failure. Against this background, 5G can be used to connect scanners, smartphones, and tablets for emergency use cases to monitor production capabilities. As these process industry sites are often more than 3,000 feet long with several steel structures and concrete walls, Wi-Fi reaches its propagation limits.

In addition, 5G can be used to map factories and storage areas, forklifts, and raw material areas as digital twins to assess the impact of new production processes and tweak the workflow before it is applied to the production line. This allows manufacturers to try out new innovative processes, while ensuring the continuity of their core business. As the name suggests, process manufacturing requires highly accurate and precise workflows. With 5G connectivity, process manufacturers can deploy real-time monitoring and control systems for critical processes—thanks to particularly low latencies and highly reliable connectivity. This allows operators to remotely monitor equipment performance, collect data, and adjust in real time to make sure no process is further disrupted. Thereby, 5G will be an important building block in increasing the Overall Equipment Efficiency (OEE) and minimizing unforeseen plant downtime because of either faulty production or machine breakdowns.

DIFFERENT DEPLOYMENT MODELS FOR ENTERPRISE 5G



To digitalize/automate production workflows and realize the efficiency and quality enhancements, manufacturers can choose between different deployment models and architectures. There are three different architectures that should be discussed in this context:

- 1) A dedicated private network, where all necessary connectivity infrastructure (e.g., Radio Access Network (RAN), core, grandmaster, and security gateway) and functions remain within the perimeters of the respective manufacturer.
- 2) A hybrid network architecture, which uses a private network for on-premises operations and augments it with public wireless network solutions for off-premises use cases, such as for supply chain monitoring.
- 3) A public cellular network, with no dedicated connectivity infrastructure deployed on manufacturing sites, meaning that all data will have to leave the respective premises. This is also known as “network slicing.”

As all these different deployment models have their own unique characteristics, they have distinct benefits and shortcomings for manufacturers, as Table 1 reports.

Table 1: Benefits and Disadvantages of Different Deployment Models

(Source: ABI Research)

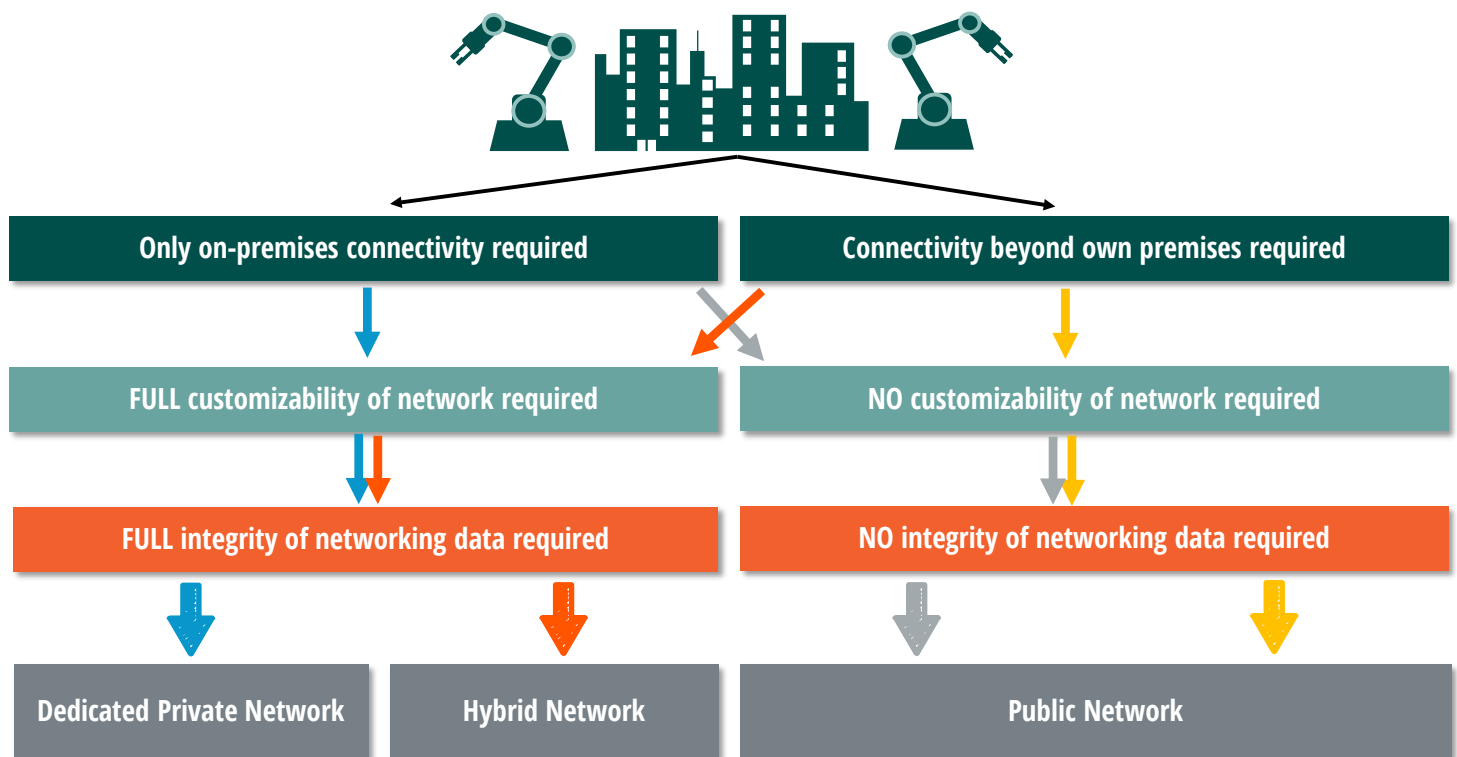
		
Dedicated Private Network	<ul style="list-style-type: none"> ▪ Full control over network functions & performance ▪ Full ability for network customization ▪ Maximum degree of data integrity ▪ Full guarantee of non-interference 	<ul style="list-style-type: none"> ▪ Cost & resource-intensive deployment ▪ Solid partnership strategy needs to be in place
Hybrid Network	<ul style="list-style-type: none"> ▪ Control over network functions & performance ▪ A certain degree of data integrity can be guaranteed ▪ Connectivity beyond enterprise sites 	<ul style="list-style-type: none"> ▪ Roaming arrangements between private and public network provider ▪ Devices need to support two networks ▪ Growingly complex management & customization
Public Network	<ul style="list-style-type: none"> ▪ Competitive price point, as no additional infrastructure needs to be deployed ▪ No/minimal CAPEX component, mostly OPEX based 	<ul style="list-style-type: none"> ▪ Inconsistent network coverage & performance ▪ No control over network functions, integrity, interference management ▪ Additional arrangements for data integrity

These deployment models come with their own technological characteristics, so each will be more applicable to different use cases. Most importantly, a dedicated private network with all equipment deployed on enterprise premises will be an important building block to automate highly critical (mission- or even life-critical) use cases. As the manufacturing environment is characterized by predominantly very harsh production environments, where workers are often under extreme pressure, this requires a maximum degree of control over network performance. Figure 4 illustrates these key considerations and their implications. Using public cellular connectivity provided from a Mobile Network Operator (MNO), even in the form of a network slice, is not

considered a viable option for most industrial enterprises because it lacks security and customizability and provides little to no local control over network management and functionality. The downside of a completely dedicated network is that it only offers connectivity within the respective manufacturing site, while some use cases might require connectivity beyond that. In the current manufacturing process, for example, “just-in-time” manufacturing is still widely adopted. Ensuring- smooth operations greatly benefits from being able to track individual manufacturing components, such as a control element for cars or individual ingredients for medication or cosmetics, along the entire supply chain. Enabling this, while ensuring the integrity of all on-premises data, manufacturers should look at the hybrid network model that includes dual Subscriber Identity Module (SIM) solutions to allow devices to access the dedicated network while on premises and securely roam onto the or public network while in transit.

Figure 4: Manufacturers’ Guide to Different Deployment Models

(Source: ABI Research)

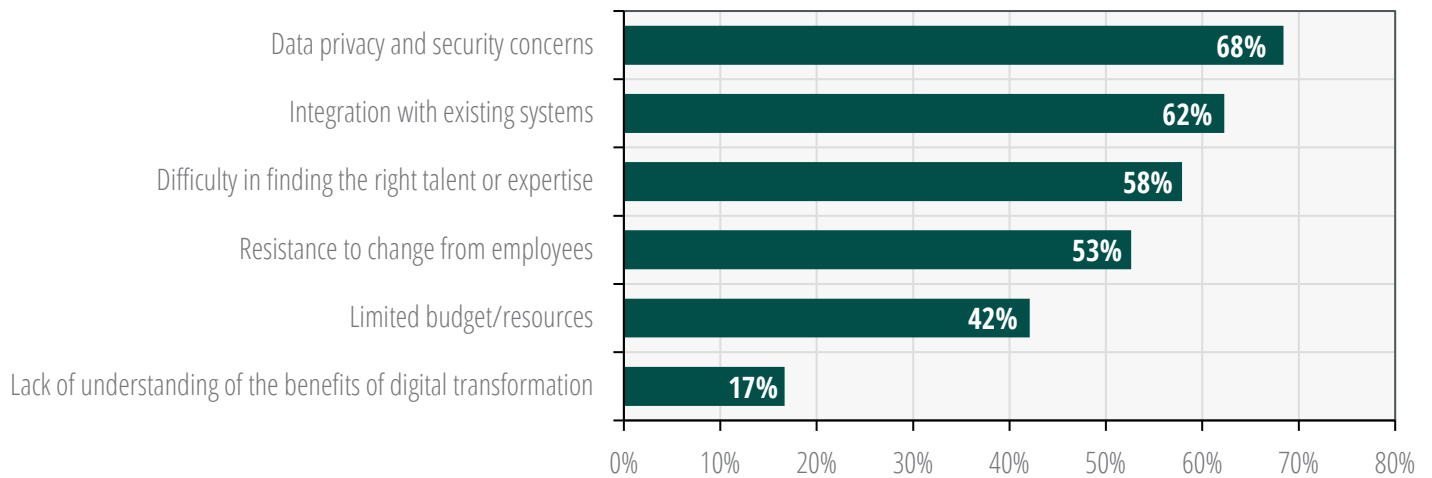


MANAGING INDUSTRIAL TRANSFORMATION: FROM WIRED TO WIRELESS CONNECTIVITY

In developing a durable strategy to manage industrial transformation processes, looking at the experience of early adopters can help mitigate risks. The most prominent issues for successful manufacturing transformation projects are around data security and guaranteeing business continuity throughout the transformation process. Furthermore, building up the necessary talent pool to manage and accompany transformation processes is seen as a main challenge for manufacturers’ transformation, as responses to the survey by MxD, Betacom, and ABI Research show (Chart 5).

Chart 5: Main Challenges for Enterprise Digitalization, N=114

(Source: ABI Research)



Let us look at each of these challenges and outline how deploying a private cellular network can help manufacturers mitigate them.

SAFEGUARDING DATA AND SECURING WIRELESS CONNECTIVITY NETWORKS

The main challenge for manufacturing transformation projects is guaranteeing data safety and networking integrity throughout the process. This becomes more important as use cases within an industry are increasingly business critical. After all, the number of production lines, data on their condition, or position of movable machines and workstations are critical for every operation and, therefore, need to be protected from unauthorized access, as this would allow competitors to gain vital insights into the production conditions. In addition, a hacking or ransomware attack has the potential to cripple operations, resulting in significant costs from downtime and security mitigation.

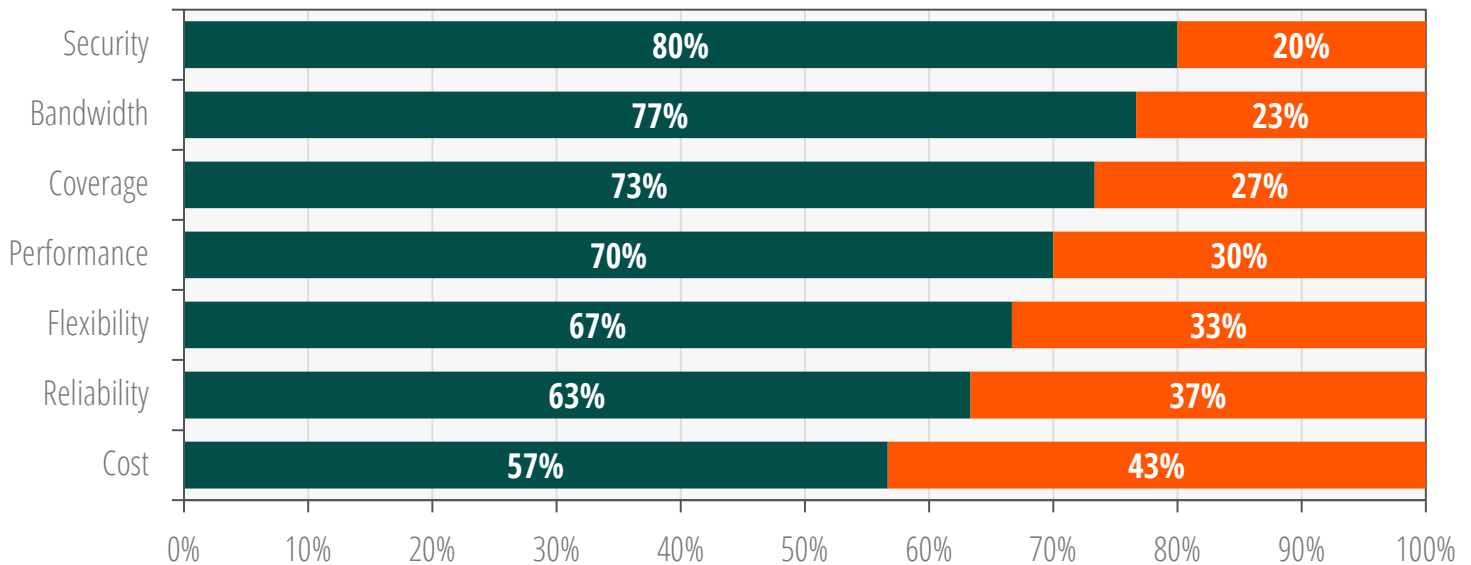
Deploying private 5G for manufacturing use cases will mean that critical manufacturing data will be digitized. Consequently, a profound security strategy needs to include cybersecurity considerations as well. 5G networks represent greater device connectivity, increased software usage, more cloud functionality, and, therefore, an increased attack surface for new threat vectors. 5G requires security implementation across various parts: user equipment, radio access, Multi-access Edge Computing (MEC), core network, and cloud, as well as for the data generated, communicated, and stored across the network. Overall, the most important security requirements to be delivered center around resilience, communication and data security, identity management, and privacy.

As Chart 6 illustrates, manufacturers that are early adopters are particularly happy with the security guarantee of a private 5G network. This is due to the additional security characteristics that private cellular networks offer—apart from security software solutions. First, a private network requires specifically designated 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 within 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, The 3rd Generation Partnership Project (3GPP) tunneling, encryption, and granular access controls.

Chart 6: Satisfaction with Enterprise Cellular, N=86

(Source: ABI Research)



GUARANTEEING BUSINESS CONTINUITY DURING THE CHANGE PROCESS

Understandably, manufacturers are particularly concerned with guaranteeing the continuity of their operations during an upgrade to their communication and production infrastructure. Most importantly, this will need to be underpinned with a reliable time frame for digital transformation projects, as unplanned downtime is detrimental to productivity. Business continuity, however, is also important beyond the borders of an individual manufacturer’s premises. Supply chains have become a lot more globally interconnected, which means that a sudden, unplanned stop of production within one manufacturing site can have wider consequences for manufacturers globally. These considerations have become more important since the global outbreak of the COVID-19 pandemic and subsequent measures to curb its spread highlighted the vulnerabilities of global supply and value chains.

In anticipation, manufacturers will need to factor this in when deciding on a digitalization path. In other words, how can they upgrade infrastructure in a way that does not affect their ability to produce? Manufacturers will need to put this on their checklist for potential digitalization partners. At the same time, this is a call for any suppliers of private cellular networking solutions to include solutions in their portfolio that safeguard manufacturers’ business continuity throughout the transformation process.

BUILDING UP INTERNAL CAPABILITIES TO MANAGE DIGITALIZATION PROJECTS

Manufacturers report challenges in recruiting the necessary personnel capability and know-how for digitalization projects, which again highlights the importance of fruitful partnerships for successful transformation projects. Manufacturers should choose their partners based on a careful analysis of their own capabilities. First, they need to identify gaps within their own expertise and identify the necessary skillset that is required from partners. Second, the skillset of potential partners should be examined in several different ways. Manufacturers should look at the partner's track record. What other projects did they work on? Have they assisted manufacturers with similar requirements in the past? Manufacturers should also use trial periods and Proof of Concept (PoC) projects to find out whether a potential partner has the required skills and if the potential partner speaks the same language as the respective manufacturer. Both checks are important to ensure a smooth transition. Manufacturers should bear in mind that this transition—and the digitalization of manufacturing processes in general—is a fundamental change that a dedicated team needs to carefully manage.

At the same, new technologies themselves can ease the demand for personnel know-how in managing transformation projects. Using AR and VR allows external partners to assist and train on-site staff, expanding their capabilities or instructing them on a case-by-case basis.

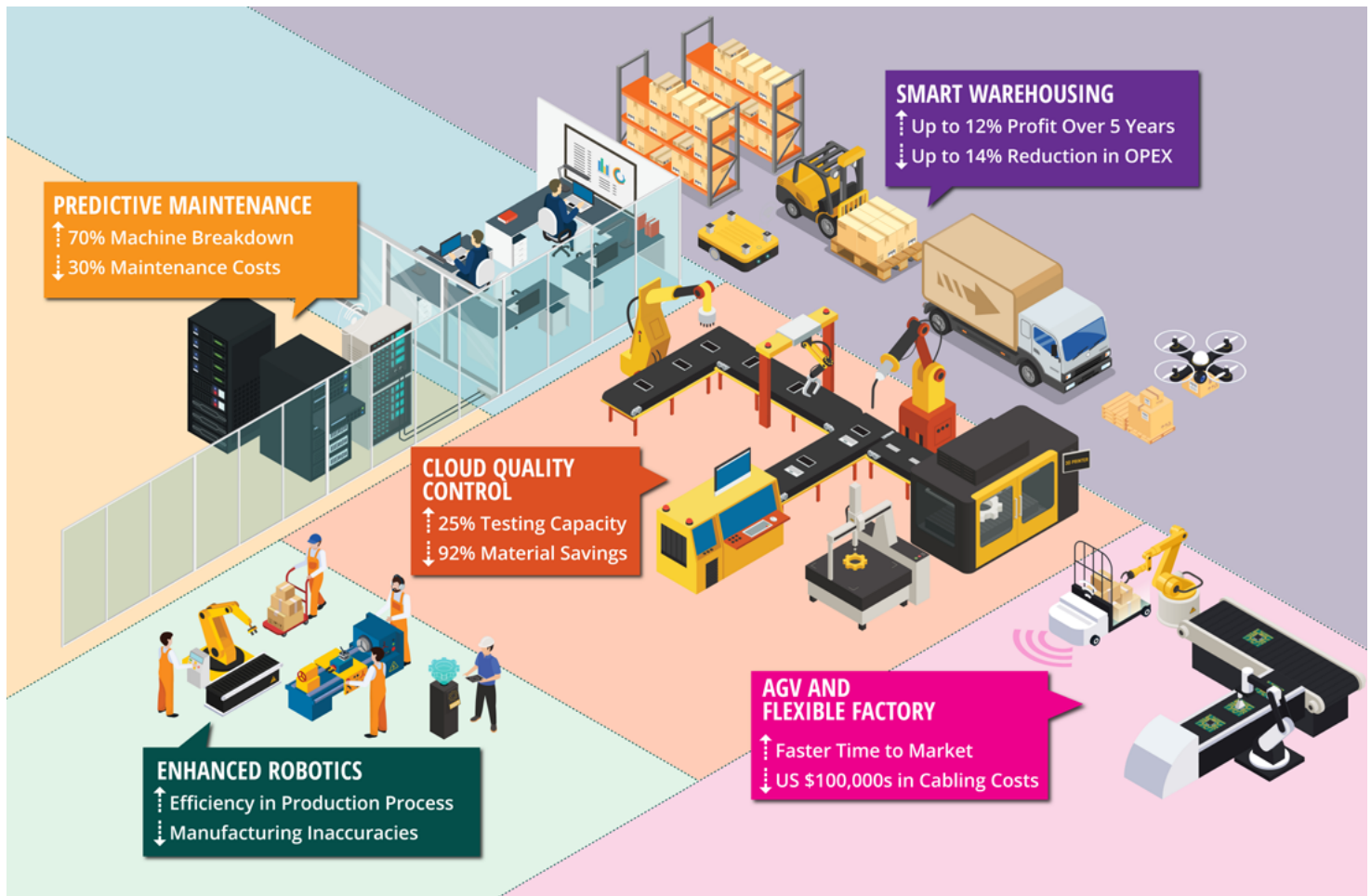
UNDERSTANDING THE BENEFITS OF DIGITALIZATION PROJECTS AND FINDING THE MONEY

There is no question that cellular connectivity deployment is a considerable investment that needs to be well thought through, especially in times of harsh macroeconomic conditions. To justify the investment, manufacturers should consider the quantifiable benefits of deploying 5G connectivity, as well as the opportunity cost of not deploying 5G. Informed by extensive discussions with the manufacturing industry, ABI Research has been working on a model to quantify both benefits and the Cost of Inaction (COI). As Figure 5 shows, these efficiency enhancements, quality improvements, and production increases are considerable and, therefore, need to be factored into any kind of investment planning :

- **Overall, ABI Research forecasts that**—by streamlining processes and operations—private 5G can yield a potential US\$1 billion for a Tier One factory in the United States over a 5-year period.
- **Assuming a cost per cable drop of US\$225**, an average factory will save several thousands of dollars in cabling costs per year.
- **Early deployment data show** that an AGV on 5G can be operated at a 30% higher speed, due to robust signal handover.
- **Early deployments of private 5G** around the world have shown that cloud quality control increases testing capacity by 25%. The higher accuracy reduces waste material and translates into significant materials savings.

Figure 5: Enterprise Cellular Use Cases on the Factory Floor

(Source: ABI Research)



Furthermore, manufacturers can choose between different models of private 5G to exactly fit their financial capabilities. Most importantly, they can look at deploying a private 5G network on their premises in a managed service model. In addition to benefits around network management and ownership, it also allows manufacturers to minimize their upfront Capital Expenditure (CAPEX) investment and focus on monthly recurring managed service fees. How these managed service fees are determined varies from provider to provider.

A GUIDE TO DEPLOYING PRIVATE CELLULAR NETWORKS

As the previous sections of this guide have shown, the drive for manufacturers to modernize their connectivity infrastructure is clear, as are the capabilities that wireless connectivity can bring to particularly harsh environments. At the same time, however, the extensive survey among manufacturers in the United States has shown that manufacturers currently face important difficulties in managing their transformation journey, which can be mitigated by choosing to deploy a private 5G network in the right way. To support manufacturers in deciding on the optimal private

cellular model and ensuring a safe and smooth transition, digitalization partners need to cater to these requirements and develop solutions to address them.

OBTAINING SPECTRUM

Obtaining mobile network spectrum is the backbone of private cellular networks, especially because of the unique security features of private cellular over Wi-Fi connectivity—increased security and network integrity, in particular—due to the fact that private cellular uses licensed spectrum that cannot be simply accessed by anyone. This will ultimately benefit manufacturers, but it creates additional considerations around choosing the best possible spectrum asset.

DIFFERENT TYPES OF MOBILE NETWORK SPECTRUM

Broadly speaking, there are three different types of spectrum assets. Each has its distinct advantages and disadvantages for manufacturers.

- **Low Band Spectrum (<1 Gigahertz (GHz)):** Radio waves operating at this spectrum can travel particularly far and propagate walls. Therefore, they are optimal for wide-area coverage. However, waves using a low frequency range can carry less data, therefore offering lower bandwidth.
- **Mid Band Spectrum (1 GHz – 6 GHz):** Radio waves operating in the so called “mid band” spectrum offer a compromise between the high range of low band spectrum and the high-capacity features of high band spectrum. Therefore, they are widely regarded as the “gold standard” for 5G deployments. Manufacturers can use this spectrum either through private 5G deployments using the Citizen Broadband Radio Service (CBRS) (see section 5.1.2 for details) or through leasing spectrum from a public network operator.
- **High Band Spectrum (>6 GHz):** Radio waves operating in high band spectrum can carry particularly high amounts of data, and therefore are ideal for high-capacity use cases. At the same time, however, they suffer from poor propagation characteristics, as they can be blocked off even by thin walls. Therefore, network infrastructure would need to be deployed a lot more densely, which would create additional costs for network deployments.

THE CITIZEN BROADBAND RADIO SERVICE

In the United States, the Federal Communication Commission (FCC) decided in 2019 to open 150 Megahertz (MHz) on the Citizen Broadband Radio Service (CBRS), which operates between 3.55 GHz and 3.7 GHz, i.e., mid band spectrum, for spectrum sharing between enterprises and (incumbent) government users. To avoid interference with incumbent government users, access is granted on a tier-based approach. This model makes it easier for enterprises to deploy a private cellular network using their own spectrum and allows digitization partners to bring new end-to-end automation solutions to the table. The CBRS is widely seen as the spectrum that is used for innovation within enterprises and provides optimal spectrum for private 5G deployments.

To be able to operate a private cellular network using CBRS spectrum, manufacturers will need to follow a set procedure that ensures proper frequency coordination.

- 1) Obtain an FCC Part 96 Certification:** In the United States, the FCC regulates the use of the CBRS spectrum. Manufacturers need to obtain an FCC Part 96 certification for their wireless equipment, such as access points and user devices, to operate in the CBRS band.
- 2) Register with the Spectrum Access System:** The CBRS spectrum is managed dynamically through a Spectrum Access System (SAS). Manufacturers must register their CBRS devices with an authorized SAS provider. The SAS provider coordinates the spectrum usage to prevent interference with incumbent users and other CBRS devices.
- 3) Obtain a Grant from the SAS:** Once registered, the SAS will grant the manufacturer access to a portion of the CBRS spectrum based on the availability and demand in the specific geographical area where the private network is to be deployed.
- 4) Deploy the CBRS Network:** After obtaining the spectrum grant, the manufacturer can deploy their private wireless network using CBRS-compliant equipment and follow the guidelines provided by the FCC and the SAS provider.

INVESTING IN EQUIPMENT FOR PRIVATE NETWORKS

While determining which spectrum solution is right for your operations, you also need to consider the equipment ecosystem that supports it. For example, you need to find the RAN, End-User Device (EUD), wireless gateways and routers, and Customer Premises Equipment (CPE) that support the spectrum you selected. To find a list of certified equipment for CBRS spectrum, visit the [On Go Alliance](#).

Hardware and software needed for an end-to-end private wireless network includes RAN automation, element management system, SIMs, 5G core, grandmaster (important for network timing), switch, router, firewall/security gateway, Uninterrupted Power Supply (UPS), and Wireless Wide Area Network (WWAN) backup solutions. If you choose to Do It Yourself (DIY), you will need to research and integrate all these components. Alternatively, you can select a service provider who can plan, design, install, and operate the end-to-end solution.




Wireless gateways and wireless routers are used for connecting equipment that does not have 5G already embedded, such as Programmable Logic Controllers (PLCs) and cameras. There are two major categories of 5G wireless gateways and wireless routers: Ethernet gateways and IIoT gateways.

Ethernet gateways can physically connect with manufacturing equipment via Ethernet ports. IIoT gateways offer a wider variety of port interfaces for connecting with existing manufacturing equipment, including Ethernet, Wi-Fi, Universal Serial Bus (USB), Input/Output (I/O) ports, serial ports, Modbus, and MQTT. Two examples of industrial-grade IIoT gateway/wireless routers are the Siemens SCALANCE MUM856-1 (RoW) and AMIT IOG880-0G1B1.

Another aspect of integration with OT equipment is that the solution needs to interface with the protocols used on the factory floor. Protocols include PROFINET RT/IRT, Ethernet/IP, and Modbus TCP. Table 2 provides additional context for when each is used.

Table 2: Different Protocols in Manufacturing and Their Use Cases

(Source: Betacom)

	Non-Real Time	Real Time	Time Critical
Examples	Data services, IT, etc.	Factory Automation	Motion Control
			
Latency	+100 milliseconds	20-100 milliseconds	≤10 milliseconds
Protocols	Ethernet/IP	Ethernet/IP, Modbus TCP, Profinet RT	Ethernet/IP, EtherCat, Ethernet Powerlink, Sercos, Profinet IRT

Real Time

FINDING THE IDEAL PARTNER FOR PRIVATE CELLULAR NETWORK DEPLOYMENTS

Much of the success of digital transformation projects depends on selecting capable partners. Manufacturers will need to decide carefully who to partner with when it comes to introducing new connectivity technologies to the factory floor. As the manufacturing environment is characterized by particularly harsh environments and highly critical use cases, any transition needs to be carefully managed to ensure a smooth transition and business continuity throughout the process.

Therefore, manufacturers should carefully assess the capabilities of different digitalization partners. In doing so, they should not only focus on the technological capabilities of potential partners, but also “soft skills” that include a company’s ability to guide manufacturers through transformation processes. The checklist on the left lists the capabilities that manufacturers should be looking for in their digitalization partner based on our recent survey.

Because private wireless networks are relatively new to the market, manufacturers might not have a team of cellular experts on-site to plan, design, install, and operate them effectively, which was one of the perceived barriers to adoption identified in our survey. To mitigate these barriers, manufacturers should look at partners that can offer a managed service package that includes network monitoring, security monitoring, patches and upgrades management, network optimization for new use cases, and break-fix repair, with a Service-Level Agreement (SLA) that meets their expectations. It is important to note that there are a number of private network providers in the United States, including Betacom, that can offer Private Wireless-as-a-Service, offering net-

work design and installation, and then securely managing network operation to meet the manufacturers' performance requirements.

VENDOR SELECTION CRITERIA	
✓ Security and data privacy capabilities	✓ Financial stability of digitization partner
✓ Customization and flexibility capabilities	✓ Integration capabilities with other solutions/vendors
✓ Customer service/support	✓ Cultural fit
✓ Reliability and scalability of solutions	✓ Industry knowledge and understanding
✓ Communication and collaboration	✓ Experience and expertise
✓ Cost-effectiveness	✓ Reputation and track record

As touched upon in Section 4.4, manufacturers should also consider different approaches to determining the managed service fee in choosing the right partner. The number of connected devices or data usage amounts are among the most prominent determinants. In addition, certain providers are looking at the coverage area, or the operating time of the network. There is no right or wrong in this, so it ultimately comes down to each manufacturer's individual financial capabilities and their preference of predictable recurring fees versus usage-based pricing.

Table 3 provides an overview of how network operators, telco infrastructure vendors, system integrators/managed service providers, and hyperscalers approach the most important partnership selection criteria.

Table 3: Competitive Assessment of Private Cellular Providers

(Source: ABI Research)

	Network Operators	Telco Infrastructure Vendors	System Integrators/ Managed Service Providers	Hyperscalers
Security Provision	No dedicated enterprise security features apart from what cellular connectivity offers.	Few additional enterprise-grade security features available.	Rich portfolio of additional security solutions available.	Ties to app developers allow hyperscalers to offer dedicated security applications.
Customizability	"Build it and they will come" offer from the consumer market, limited customizability.	Standard connectivity elements available that can be customized to a certain extent.	Everything-as-a-Service: Solution can be customized based on manufacturers' KPIs.	Limited room for customizability; hyperscalers sell their public infrastructure.
Enterprise Support	Enterprise support channels for IT solutions would need to be improved.	Direct to-enterprise sales are fairly new, so support channels need to be developed.	Dedicated support during planning, design, commissioning and monitoring phases.	Enterprise support channels for IT solutions would need to be improved.
Cost-Efficiency	Business model relies on Connectivity-as-a-Service; no way to ensure cost efficiency.	Network solution is fairly CAPEX intensive, so no direct way to ensure cost efficiency.	Monthly service fee means manufacturers can ensure that their investment is efficient.	Monthly Service Fee: Manufacturers can ensure that their investment is efficient.
Integration Capabilities	Network operator provides connectivity, integration will fall back to manufacturers.	Telco infra vendors are not experts when it comes to adjacent connectivity technology.	Highly experienced, as integration is their everyday job.	Unless explicitly specified, hyperscalers are not in charge of integration.

STRATEGIC RECOMMENDATIONS FOR MANUFACTURERS

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 as to how manufacturers should plan this journey to ensure it leads to the desired outcome.

PRE-DEPLOYMENT



Define Use Cases and Technology Capabilities

Manufacturers should begin thinking about updating their communication infrastructure by identifying specific use cases and IIoT applications that could benefit from a private 5G network. To do this, manufacturers should engage in a detailed cost-benefit analysis. Manufacturers will need to gather offers from different providers and quantify the effect of automation on different use cases. When determining pain points, they should also develop a profound understanding of how to quantify the effect of the bottlenecks: How much revenue they lose from unplanned machine downtime, how many faulty products need to be corrected after they leave the factory floor, or how much money and time it takes to (re-) cable a factory floor could be aspects to determine the most pressing use cases. This could include areas like real-time monitoring, asset tracking, autonomous vehicles, or remote-controlled machinery. Understanding the use cases will help with designing and optimizing the network accordingly.

To benchmark the financial benefits of a cellular network, manufacturers will also need to define their own financial capabilities, which will influence the network deployment considerably and have effects on the amount of connectivity infrastructure, coverage area, and even the partnership strategy. A manufacturer choosing to manage the entire deployment on their own will have to invest significantly more CAPEX in purchasing necessary equipment. Siding with a managed service provider, on the other hand, allows manufacturers to finance most of these deployments through recurring fees.



Plan the Network and Partnership Strategy

Based on these use case-specific considerations, manufacturers should then start to plan the network deployment. At the heart of this, manufacturers should define the intended coverage area that is necessary to address the identified use cases. Furthermore, a specific time horizon for the entire network deployment project should be internally formulated to increase accountability. Furthermore, at this stage, manufacturers should decide whether they want to deploy, manage, and operate the network on their own (in a DIY model) or partner with a managed service provider, which can provide a full turnkey solution to manufacturers so they do not have to spend valuable production time planning any of the networking aspects that will follow.



Design the Network

Based on the initial planning steps, manufacturers should then start to design the cellular network. This entails several steps. First, manufacturers will need to decide on the type of cellular network spectrum that shall be used. As discussed in previous sections of this guide, several types of mobile network spectrum offer different (dis-) advantages to manufacturers that should be carefully assessed.

- Low band spectrum provides coverage for a wide area.
- High band (Millimeter Wave (mmWave)) spectrum offers exceptionally high data rates with low propagation, especially in harsh environments with a high degree of metal infrastructure.
- Mid band spectrum is emerging as the perfect compromise, as it offers the optimal combination of propagation characteristics (and therefore, a large enough coverage area) and throughput. Manufacturers can use the CBRS in the United States to gain access.

In connection with this, manufacturers will need to make a detailed Radio Frequency (RF) design to ensure that the network uses the right amount of infrastructure equipment to cover the intended areas and use cases. Second, manufacturers will need to define the network infrastructure that is required (including end devices, cloud components, security gateways, the cellular core network, the RAN, spectrum access management solutions, and SIM cards).

Third, manufacturers will need to agree on an operating model for network monitoring, security monitoring, patches and updates, and break-fix repairs. As part of this, SLAs regarding network uptime and other performance indicators will need to be discussed with each component vendor.

DEPLOYMENT AND COMMISSIONING



Install Cellular Connectivity Infrastructure

As the first step of deployment and commissioning, manufacturers will need to mount, install, and integrate the connectivity infrastructure. This includes pulling power and fiber cables, mounting small cells, installing the necessary IT infrastructure, as well as the cellular core network. As all network equipment will be provided by different vendors, integration can vary in complexity and take several days. In addition, SIM cards and other industrial end devices will need to be provided for the intended use cases and be properly integrated into the overall network infrastructure.



Initial Post-Deployment Tests and Commissioning of the Network

Once all infrastructure is mounted, installed, and integrated, the full networking solution will need to be tested to ensure proper functionality. This should include a test of all networking components individually, but also test interoperability of the different components. Certain software solutions may help—specifically to provide appealing and easy-to-use interfaces. Once all interoperability tests have been completed, the network can be handed over to the different production units for use in a real-time commercial environment.



Create the Right Structures to Operate the Network

After successful commissioning of the network, manufacturers will need to ensure that appropriate structures are in place to manage and operate the network as effortlessly as possible. This includes staffing a team for Tier One support (for immediate support in case of problems with the network) with cellular and cybersecurity experts, as well as break-fix repair resources. As manufacturers generally do not have this expertise in-house already, a DIY approach commonly will have to include new hires and significant investments in staffing.

As part of this, manufacturers will need to define and measure necessary SLAs in accordance with what has been defined earlier in the process. Software solutions in the form of Software-as-a-Service (SaaS) or readily available test kits that some of the leading manufacturers of test and measurement equipment provide can be of help to ease monitoring.



Ensure Warranty and Support Arrangements

Apart from creating the appropriate structures internally to manage and operate the cellular network, manufacturers will also need to ensure that warranty arrangements with the individual component vendors are in place for level-2 support and beyond. Once again, careful selection of partners can mitigate the workload for manufacturers, as managed service providers, for example, can include all installation and commissioning work into their offering.

POST NETWORK DEPLOYMENT



Continuously Monitor Network Performance and Adjust

Once the private 5G network is deployed, manufacturers will need to establish a monitoring and optimization framework. This includes analyzing network performance in accordance with the pre-defined Key Performance Indicators (KPIs). Most commonly, this will include measuring availability and reliability, average and peak data rates, and end-to-end latency. By now, a number of globally-leading test and measurement providers have dedicated software and hardware solutions in place, so manufacturers do not have to build such a system from scratch. Furthermore, to design a future-proof networking solution, manufacturers will have to identify areas for improvement, and proactively address any issues or bottlenecks. Again, software solutions—using AI algorithms—can help simulate network extension. Designing a digital twin of the private network, for example, can enable manufacturers to test how extensions might affect the network performance without having to test it out in the real-time commercial environment.

Private 5G offers manufacturers immense opportunities to digitalize their operations and provide a much-needed upgrade to their communication infrastructure. The deployment, however, should only be the last building block in a much wider digital transformation strategy. In all of this, manufacturers should bear in mind that innovation in cellular connectivity will not stand still. Instead, it will gradually advance its features and, therefore, use cases and application scenarios. To manage this change from wired to wireless connectivity on the factory floor, manufacturers will need partners with links to the telecoms industry that will design, manage, and operate an easily upgradable, future-proof private 5G network together with manufacturers.



Published October 2023

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.

© 2023 ABI Research. Used by permission. ABI Research is an independent producer of market analysis and insight and this ABI Research product is the result of objective research by ABI Research staff at the time of data collection. The opinions of ABI Research or its analysts on any subject are continually revised based on the most current data available. The information contained herein has been obtained from sources believed to be reliable. ABI Research disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.