White Paper
December 2024

IT@Intel: Delivering Operational Efficiencies Using a 5G Private Network

Intel IT is helping Intel Corporate Services to digitally transform its infrastructure to support Intel's factories, driving a USD 35M 5-year net present value

Authors

Balakrishna Anumolu
Director of Industrial Automation, Intel Corporate Services

Rob Colby
Principal Engineer, IT Architecture and Infrastructure Services

Ram Patel
Senior Staff Network Engineer, Intel IT

Joe Robison
Automation Architect, Intel Corporate Services

Table of Contents

Executive Summary

Minimizing factory downtime and improving operational efficiency have always been the driving forces behind Intel IT's push to digitize equipment in both factory and subfab environments. Now, we're expanding these efforts by working with Intel's Corporate Services (CS) team to connect critical factory-support infrastructure, including surveillance systems in guardhouses, electrical supply equipment, water systems, and more.

Connecting equipment in remote outdoor areas to the corporate network has always been a challenge. Wi-Fi coverage is limited; hard wiring is costly and time-intensive; and relying on public networks introduces concerns with cost, performance, and security. After reviewing the options, we chose to roll out 5G private networks at Intel factories to extend wireless connectivity for key use cases in Internet of Things (IoT), robotics, operations, and security. This deployment, combined with 5G-enabled IoT Gateways and an array of sensors, lets us reach further and deliver more robust connectivity where it's needed.

With our 5G private network in place, CS technicians can tap into sensor data to gain deeper visibility into equipment health, enabling predictive and preventative maintenance. This enhanced connectivity also allows technicians to connect field devices, like tablets, directly to the corporate network to increase efficiency. Currently, our 5G private program supports only 13 use cases—a fraction of the potential applications. Our 5G deployment spans five factories and is projected to generate a net present value of USD 35M over the next five years.

We hope that by sharing our 5G private network journey, we can inspire other IT departments to explore using this technology to continue the digital transformation of their previously unconnected environments.

Contributors

Joe Sartini, Global Domain Lead, Industry 4.0
Ryan Kovalchick, Engineering Manager and Architect, Industrial Automation

Acronyms

AP	access point
CS	Corporate Services
IoT	Internet of Things
LAN	local area network
PoC	proof of concept
POR	proof of record
RFP	request for proposal
ROC	Remote Operations Center
WLAN	wireless local area network

Business Challenge

Intel factories are highly complex environments, integrating thousands of interconnected systems that manage precise manufacturing processes with minimal tolerance for error. Each factory operates on a vast scale, coordinating advanced machinery, robotics, and real-time data flows to achieve rigorous performance and quality standards that are essential for semiconductor production. To support this ecosystem, the factories rely on many supporting services that are crucial to factory operation, such as water, power facilities, and security infrastructure like guardhouses, turnstiles, and surveillance cameras. Intel IT's long-term vision is to achieve full automation of services like water purification and power; but to get there, we need a reliable connectivity solution to link up these currently unconnected spaces.

In many outdoor areas, such as a guardhouse or a power feed installation, connecting to the corporate network over the local area network (LAN) or even the wireless local area network (WLAN) is nearly impossible. Connecting the LAN to outdoor or remote buildings is costly because it typically requires extensive cabling over long distances, which demands both high-grade materials and significant installation labor. Additionally, these setups often need specialized equipment to handle environmental factors like weather exposure, which drives up both the initial investment and ongoing maintenance costs. Even inside our factories we have spaces with sparse or non-existent LAN and WLAN connectivity due to the cost and complexity of running conduit to these locations. Most of the use cases discussed in this paper require some type of connectivity, such as when a technician carries a tablet around while inspecting equipment and performing preventative maintenance of their assets in the field.

Without network connectivity, it is difficult to monitor, troubleshoot, and perform preventative maintenance efficiently. For example, consider a technician performing routine rounds and readings outdoors, where previously there was no wireless connectivity. The technician may notice that a motor is emitting a loud whining sound. Without connectivity, the technician does not have visibility into how long the motor has been making this noise and whether it has been getting worse over time. However, with connectivity provided by a 5G private network, the technician can use a tablet to access real-time trend data about the asset to help identify possible issues. If needed, the technician can make immediate adjustments to the asset or access its operating procedures directly from the tablet. Technicians can also use the 5G private network to access virtual training such as task steps or videos.

Seeking to improve network connectivity and increase efficiency, CS requested that Intel IT help them digitally transform their infrastructure.

Solution

To solve our connectivity challenge and deliver customer value, we evaluated several potential solutions:

- Adding additional access points (APs) for the WLAN at all locations where service is required
- Adding cabling for the wired LAN
- Using existing public 4G and 5G networks
- Deploying a 5G private network

Our full market evaluation determined that a 5G private network could best meet our cost and quality goals for the following reasons:

- Adding Wi-Fi connections in the remote spaces is not a truly cost-scalable solution (we still must run landlines and introduce switch infrastructure). In addition, we saw that WLAN latency was higher compared to private 5G latency.
- Running new cabling directly to all unconnected equipment, like security cameras, would be very cost-prohibitive for multiple reasons, considering how expansive our factory spaces are. In addition, guardhouses and turnstiles change location often, so hard wiring would create multiple instances of zero-value cost compared to wireless options.
- Public network scale and cost analysis showed that using a public network was cost-prohibitive at a certain inflection point of the number of connected devices (see Figure 1; data presented is for example only).

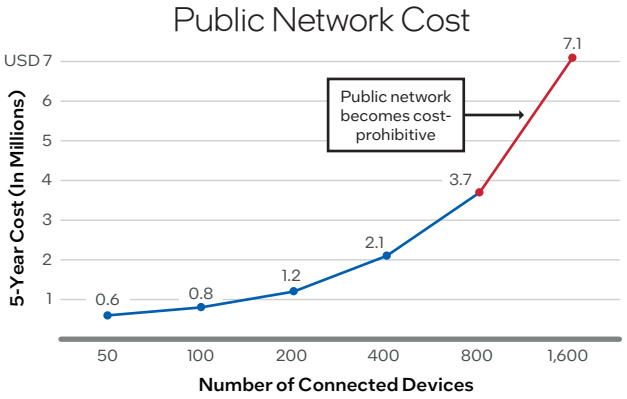

Figure 1. Our scale and cost analysis revealed that public network costs escalate as the number of connected devices increases (data is for example only).

Intel Corporate Services (CS) Digital Strategy

CS seeks to improve efficiency through connected automation in the following ways:

- Modernizing and extending the life of obsolete assets by retrofitting them with connected smart sensors.
- Improving equipment-to-staff efficiency through IoT and robotics.
- Using analytics and AI to enable proactive fault detection.
- Building a solid foundation to enable a fully connected CS environment for the entire campus.

Beyond cost concerns, public networks introduce risks to intellectual property and data security. Surveillance data, for instance, requires strict protection, and data stored in the public cloud can be vulnerable to malicious actors. While a virtual private network (VPN) could mitigate these risks, 94% of CS-maintained equipment—excluding tablets and smartphones—lacks VPN capability because it cannot run the necessary software. This lack of VPN support not only increases security risks but also creates an inconsistent user experience across devices. To address these issues, managing our own data plane helps to ensure secure and uniform access to Intel's network without relying on public infrastructure, which could potentially be exposed.

After deciding that a 5G private network was the best approach for transforming CS's network connectivity, we laid out a project timeline (see Figure 2). This timeline includes a proof of concept (PoC), a request for proposal (RFP) to select our network equipment provider, and a phased rollout of 5G private networks across all Intel factories worldwide.

Conducting the PoC

Intel IT is always careful in validating the business value of the approach used to solve a business challenge. In 2023, we ran a PoC to dive deeper into assessing the cost and effectiveness of a 5G private network. The PoC ran for three months at one factory campus across 13 use cases, which included using business tools in the field (such as tablets), collecting data via Internet of Things (IoT) sensors, collecting data via autonomous robots, and guardhouse connectivity for surveillance.

The results of the PoC confirmed that for Intel's factory environment, a 5G private network was an optimal solution for helping CS connect their unconnected and high-cost connected devices. It showed we could enable all CS-maintained devices to connect to the corporate network—which was not possible with a public network—and our overall cost analysis showed we could drive a five-year net present value of USD 35M.

USD 35 Million
5-Year Net Present Value

Choosing a 5G Private Network Equipment Provider

When our PoC was complete, we conducted an RFP. We rigorously evaluated three private network providers from two perspectives:

- IT perspective for overall scalability, support, and infrastructure management
- Platform perspective for ensuring that the products used met customer requirements

We needed a solution that would work worldwide (Intel is a global company), with enhanced security, excellent performance, and superior monitoring and support. We scored each provider on various criteria, weighting the scores depending on overall program priority. For example, we weighted cost efficiency more heavily than scalability. The most critical evaluation criteria included network and security, provisioning, and monitoring and support (see Table 1 on the next page). Criteria also covered other aspects, such as supported bandwidth for upload and download, and resiliency (of both radio and core network).

Table 2 provides an example of the type of evaluation we performed. In this table, the numbers are not the actual numbers we used, but they do provide a high-level view of the evaluation methodology.

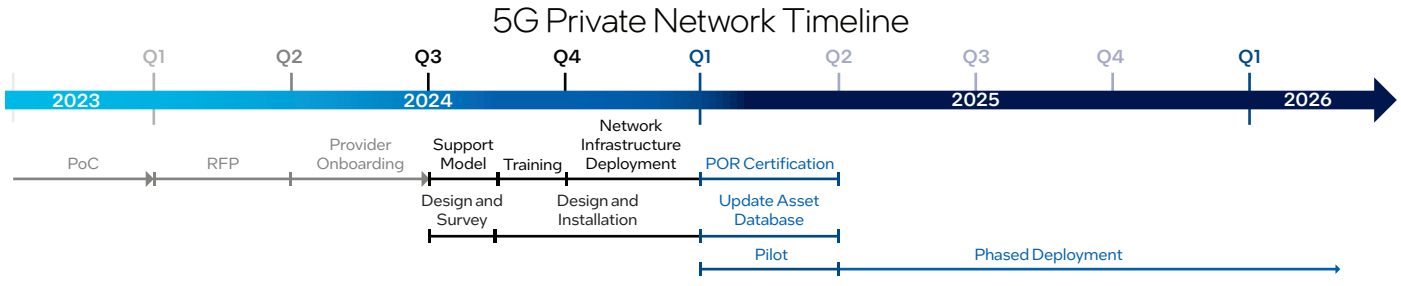

Figure 2. We took a phased approach to deploying 5G private networks for Intel's factories.

Table 1. Critical Platform Evaluation Criteria

Criteria Category	Specific Requirements
Network and Security	▪ Multifactor Authentication ▪ In addition to the SIM, additional attribute(s) ensure a device is not rouge, such as MAC address or IMEI number ▪ Device category segmentation (such as camera versus IoT device versus tablet) ▪ Micro-segmentation within device categories (such as one camera versus another camera) ▪ End-to-end secure communication via encryption ▪ Guarantees that data remains within the private network ▪ Granular QoS configuration per use case or traffic type (such as real-time streaming versus voice versus data) and support for SIM-based prioritization ▪ Integration with the existing enterprise network ▪ Resilient and reliable end-to-end infrastructure (from radio to AP to core) ▪ Zero-downtime maintenance, with minimal additional infrastructure ▪ Mature lifecycle process (including provisioning, replacement, and decommission) ▪ Meets hardware longevity expectations (core/backbone, 7-10 years; radio, 5 years) ▪ Supports relevant network protocols (including TCP/IP, UDP/IP, Jumbo Frames/PDU)
Provisioning	▪ Onboarding/registration capability through a SIM application ▪ Onboarding lifecycle capability (First-Day office, Last-Day office) ▪ Secure onboarding portal or application ▪ Integrates with Intel IT's asset management tools ▪ Supports authentication via the SIM
Monitoring and Support	▪ Escalation support with a service level agreement (SLA) ▪ Global bug fixes and software upgrades, along with vulnerability support per SLA ▪ Application support and customer training ▪ Infrastructure performance monitoring (service, radio, AP, and core) along with streaming telemetry with API and dashboard ▪ Infrastructure fault monitoring and alerting (service, radio, AP, and core), endpoint monitoring (onboarding, traffic/bandwidth, type of traffic), and reporting capabilities via webhook, APIs, or email, along with integration with existing enterprise network management tools ▪ Anomaly detection and machine-learning-based monitoring ▪ Pay-per-view (PPV) capabilities via a dashboard and APIs (such as setting up PPV for a specific use case)

Table 2. Summary of the 5G Private Network RFP Results (Data Presented Is For Example Only)

Evaluation Category	Sample Criteria	Score Weight	Provider A Score Raw	Provider A Score Weighted	Provider B Score Raw	Provider B Score Weighted	Provider C Score Raw	Provider C Score Weighted
Commercial	▪ Cost ▪ TCO ▪ Contract	5%	75%	3.75%	55%	2.75%	100%	5%
General Technical	▪ Solution ▪ Capability ▪ Scale ▪ Global Market Presence ▪ Products Powered by Intel® Processors	5%	80%	4%	60%	3%	65%	3.25%
Network and Security	▪ Multifactor Authentication ▪ Segmentation ▪ QoS ▪ Integration ▪ Resiliency	40%	60%	24%	60%	24%	63%	25.2%
Provisioning	▪ Onboarding ▪ SIM Provisioning	10%	50%	5%	45%	4.5%	55%	5.5%
Monitoring and Support	▪ Fault, Configuration, Accounting, Performance, and Security ▪ Escalation ▪ Monitoring ▪ Software Upgrades and Fixes	40%	70%	28%	50%	20%	60%	24%
Total				**64.75%**		**54.25%**		**62.95%**

Deploying the 5G Private Network

When the RFP was completed and we scored the three providers, we chose the provider with the best overall score (Provider A in Table 2). In early 2024, with the decision made about which product we were going forward with, we started designing and building a 5G private network at one campus based on our 5G private network connectivity reference design (see Figure 3).

Our primary goal is to establish connectivity over a 5G private network to the enterprise network, comparable to traditional wired or Wi-Fi connections, while meeting business objectives, ensuring a positive user experience, and maintaining stringent security standards. The following list describes our approach to each 5G private network component at a high level.

- **IoT Gateway installation:** Install the IoT Gateway within the facility's operational environment. The gateway will serve as the conduit for data collected from IoT sensors attached to machinery and other equipment.
- **5G private network connection:** Connect the IoT Gateway to the 5G private network. This connection requires the IoT Gateway to be equipped with a 5G modem and a specific SIM card that is whitelisted for use exclusively for this use case.
- **Network segmentation:** Integrate the IoT Gateway into a network segment that is specifically designed for IoT devices. This strategic segmentation is essential because it isolates IoT traffic from the broader enterprise network, thereby reducing the risk of security threats spreading across the network.
- **Data routing to a secure internal zone (SIZ):** Route data from the IoT Gateway to a SIZ, which is a protected network layer where data is subjected to thorough inspection and analysis to help ensure it is free of malware or anomalies before being allowed onto the enterprise network.
- **Secure external connections:** Establish secure, encrypted communication channels for the IoT Gateway to interact with external resources. These channels must be continuously monitored to verify compliance with the enterprise's security policies.

By following these steps, we can securely integrate the IoT Gateway into the 5G private infrastructure. This integration not only provides the necessary security and user experience but also complies with the enterprise's security policies and meets business requirements.

Showcasing the Value of Private 5G for Operational Technologies

Currently, our 5G private network manufacturing environment use cases fall into three categories:

- **Enhancing security:** cameras, turnstiles, and guardhouses
- **Enabling mobility:** CS mobile technicians
- **Connecting the unconnected:** real-time monitoring of assets

The following sections describe several specific use cases; we intend to expand the number of use cases over time to deliver additional business value.

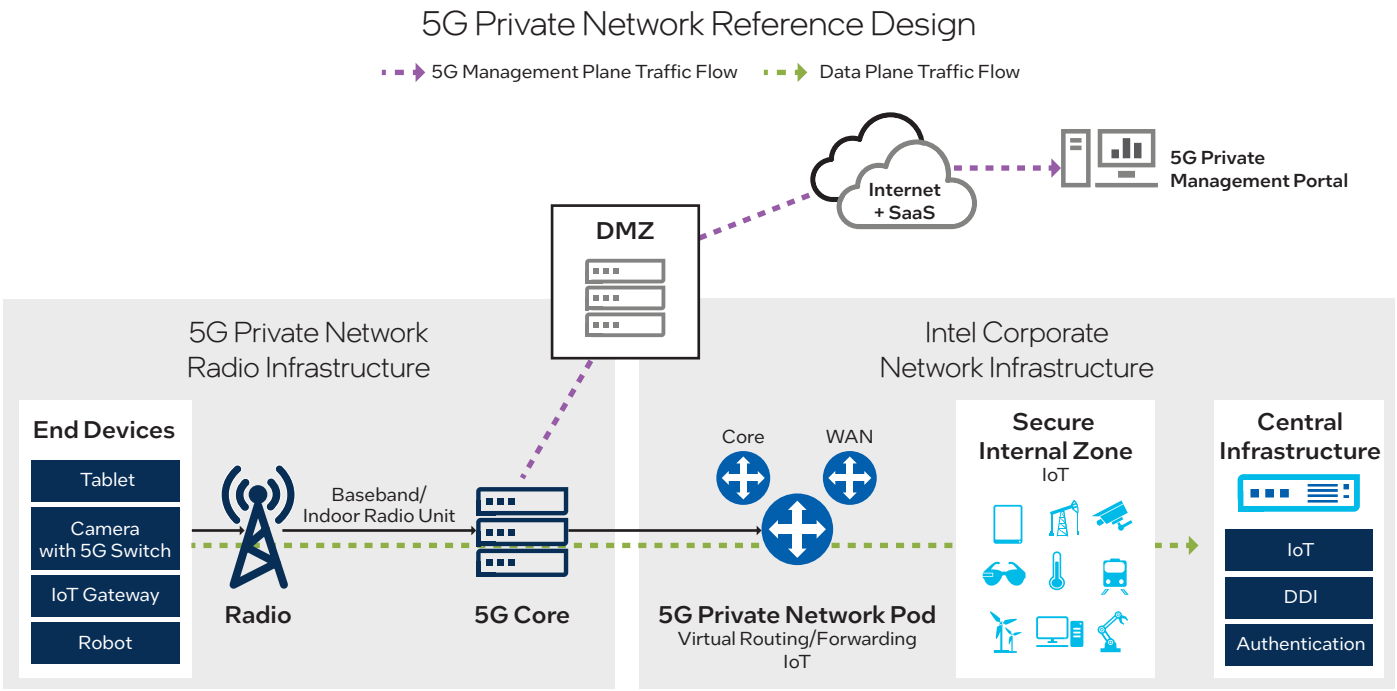

Figure 3. Intel IT's 5G private network connectivity reference design.

Enhancing Security

Keeping a factory's people, products, and intellectual property safe is paramount. Most factories have one or more guardhouses equipped with surveillance cameras. Prior to the deployment of a 5G private network, it was difficult, or even impossible, to connect these cameras to the Intel corporate network, which raised security concerns since real-time monitoring data from the cameras wasn't readily available.

To resolve this problem, we developed a new camera setup that allows three cameras to connect over a LAN to a single switch equipped with a 5G radio for backhaul to the Intel corporate network. This setup successfully integrated the cameras and the associated security panel onto our 5G private network, achieving seamless connectivity with zero downtime and no bandwidth issues, such as buffering. This 5G private network solution provides CS security teams to have more confidence in maintaining secure and reliable monitoring against potential threats.

Enabling Mobility

Intel's factories can cover several acres, so mobility is crucial to increasing operational efficiency. We are using the 5G private network to enable two mobility use cases:

- CS technicians continuously inspect equipment for current or imminent problems. This task is often called "rounds and reads." Each technician can only cover so much ground during a shift, and if a problem isn't caught soon enough, it can negatively impact factory operation. A 5G private network can support robotic rounds and reads, increasing round-and-read efficiency while freeing technicians' time to work on other important or highly skilled tasks.
- While they are working, technicians carry tablets that can help them with their jobs—such as providing step-by-step videos of repair tasks, interfacing with the asset management database, or going online to order parts. However, the usefulness of the tablets is diminished by Wi-Fi coverage gaps or a lack of connectivity entirely. A 5G private network can enable tablets to connect anywhere, anytime.

Connecting the Unconnected

In our previous papers, we have described how we use sensors and IoT Gateways to gather data from equipment and, in some cases, send commands back to the equipment. The data is sent using Wi-Fi or hard-wired cabling in these cases. However, not every factory device can be covered by the WLAN or LAN, so they cannot connect to the Intel corporate network. In our never-ending quest for more data from the factory floor, we wanted to increase the consumption of data from the factory floor from stand-alone devices by leveraging low-cost Intel IoT Gateways in remote locations where traditional Intel network connectivity is not available.

Mobility Use Cases

Robotic Rounds and Reads

We deployed an autonomous robotic solution equipped with onboard Internet of Things (IoT) sensors to record the rounds and reads, eliminating the need for technicians to perform this task. The robotic solution also serves as the "eyes and ears" for the Remote Operations Center (ROC) for any potential issues found in the field. We experienced 100% device connectivity to the Intel corporate network (via private 5G), with a latency of less than 200ms between a robot and the on-premises server. The video feed to the ROC has no jitter, and we experienced no data drops. The ROC can remotely control and manage the robots, such as locating the robot or sending software patches to a robot.

Mobile Technicians

CS technicians can use the 5G private network to perform preventative maintenance, rounds and reads, and on-the-spot troubleshooting using a connected tablet (or another mobile device, such as a laptop or 2-in-1). In our experience, all devices have excellent coverage and can use private 5G to connect to the Intel corporate network to access internal and external productivity applications.

Several applications are possible, including the following:

- **Monitoring the vibration and temperature of critical rotating equipment.** Historically, this type of monitoring was performed by a third-party technician, who manually visited each piece of equipment with a hand-held analyzer. We installed vibration and temperature sensors onto critical industrial fans and pumps connected to a 5G-enabled gateway. Now, analysis can be done in-house with more frequent and higher-quality data points, and we can use our internally developed AI and machine-learning models to predict maintenance needs and failure potential.
- **Monitoring the temperature of electrical switchgear.** Reliable, consistent electrical power is vital to factory operation. We installed temperature analyzers onto critical electrical switchgear infrastructure, typically located in remote outdoor locations, and connected the analyzers to a 5G-enabled gateway. The connected sensors enable predictive equipment maintenance that protects the factory from damage to the main power feed.
- **Data collection.** We installed 5G-enabled gateways to collect data from various equipment that have never previously been connected. For example, data from

process analyzers in the manufacturing environment provides the ability to pair data with industrial control systems process data to enable real-time analytics of manufacturing processes. Extracting data from stand-alone variable frequency drives (VFDs) in the manufacturing environment enables predictive maintenance on critical rotating equipment (motors/pumps/fans) and the VFD itself. Collecting data from stand-alone uninterrupted power systems (UPS) units in an outdoor remote location provides valuable operational and maintenance information to help technicians understand the health of UPS assets in real time.

We have experienced excellent 5G private network coverage for these 5G-enabled gateways. Latency is less than 500ms between the edge device and the MQTT server, with zero data drops. With this low latency, the gateways can stream data every second, which enables a high level of fault detection and classification. In addition, the gateway can be managed remotely.

Solution Architecture

The architecture for connecting sensors and 5G-enabled gateways to our 5G private network is similar to the architecture we use for WLAN- and LAN-connected devices, with one exception—the gateway uses a 5G-enabled modem instead of an Ethernet switch (see Figure 4).

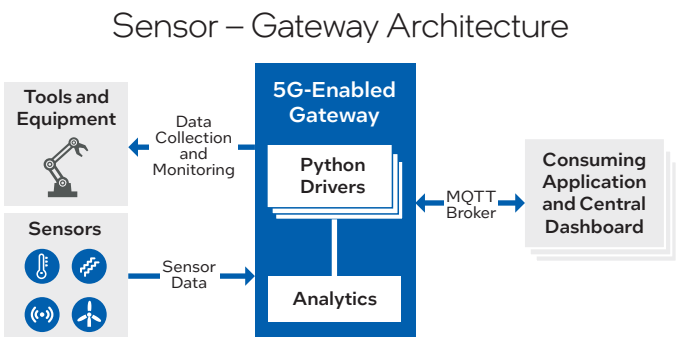

Figure 4. Sensors and 5G-enabled IoT Gateways enhance security, enable better mobility, and help connect the unconnected.

Results

We estimate that deploying a 5G private network for the 13 use cases across five factory sites will create a USD 35M NPV over five years. In addition to cost savings, we also found that the average latency of the 5G connections was far lower than WLAN connections—driving additional potential for quick equipment problem discovery and intervention.

Lessons Learned

Some key takeaways from our 5G private network journey include the following:

- Rigorous testing and validation are necessary to help ensure that all user endpoints can connect to the 5G private network. The market is still growing in this space, and not all devices can connect to private 5G.
- To enable efficient ongoing support, we must keep detailed documentation about radio status, location, and coverage.
- A platform powered by Intel® Xeon® processors best meets our quality and scalability objectives.
- Our success with a 5G private network in the manufacturing environment challenges the current plan of record (POR) as we continue to reimagine factory floor connectivity.

Conclusion

Our 5G private network PoC results are very promising, both from the perspective of financial value and factory efficiency and reliability. We are moving forward with a pilot project in the first quarter of 2025. During the first half of 2025, we will establish our indoor 5G private network strategy, which includes collaborating with connectivity industry players to explore the technology that is necessary to enable a seamless transition from indoor to outdoor networks. This smooth transition will enable always-on connectivity as CS technicians move about their job sites.

Our 5G journey has just begun; through 2027 we will be working with product suppliers to expand direct vendor connectivity. For example, we will work with equipment vendors to embed 5G private radios in their products and establish an onboarding process. Also, based on the pilot project results, we will pursue plan of record (POR) certification and roll the 5G private network solution out to additional factories worldwide. We encourage other manufacturers—and other industries—to explore the potential of 5G private networks and we would be glad to share our experience and learnings.

Related Content

If you liked this paper, you may also be interested in these related stories:

- Reliability Engineering Helps Intel Cut IT Manufacturing Systems Downtime in Half
- Expanding Low-Cost IIoT Manufacturing Use Cases
- Intel Cuts Downtime and Costs with Fault Detection Systems for Factory Equipment
- Transforming Industrial Manufacturing with Software-Defined Networking

For more information on Intel IT best practices, visit intel.com/IT.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation on **X** or **LinkedIn**. Visit us today at **intel.com/IT** if you would like to learn more.

1224/WWES/KC/PDF