www.pipelinepub.com
Volume 20, Issue 9

The Industrial IoT Digital Divide

By: Rajeev Shah

Let's start with the definition of Industrial IoT (IIoT). It is an ecosystem of devices, sensors, applications, and networking equipment that work together to collect, monitor, and analyze data from industrial operations to increase visibility and enhance troubleshooting and maintenance capabilities. The overall goal is to improve productivity and increase operational efficiency.

The market is flooded with smart devices for Industrial IoT, including sensors, connected PLC machines, scanners, ruggedized tablets, automated forklifts (AFLs), automated guided vehicles (AGVs), and autonomous mobile robots (AMRs). The problem is that this modern technology is rendered useless without robust connectivity to ensure that the tools always work, no matter where they travel in the plant, the warehouse, the yard, or the remote reaches of the field.

Industrial environments have traditionally relied heavily on wired connectivity protocols such as PROFIBUS, PROFINET, Modbus, and EtherCAT to connect their IIoT devices. With the cost of wired connectivity coming in at $8-$18 per square foot, connecting all remote IIoT devices with cables becomes economically unfeasible. For example, consider a pressure sensor monitoring pipeline at a remote location in an oil refinery, or a security camera monitoring a remote gate at the periphery of the facility.

When it comes to wireless solutions, we are constantly having discussions with customers who ask if their Wi-Fi is "good enough," and it is increasingly not! It is certainly not good enough for mission-critical applications. Any mine, refinery, warehouse, or manufacturing plant that is trying to add automation to their operation, both indoors and out, is quickly running into the limitations of Wi-Fi. As an example, handover challenges mean that you cannot reliably and safely run AGVs and AFLs on Wi-Fi. Another common experience we hear from customers is that even if you can run reliably in a small section of the warehouse where Wi-Fi coverage is not impeded by racks of goods, you cannot run that AGV down an aisle or into a corner, and network performance plummets as you try to add more devices onto the network.

Here are just some environments where Wi-Fi is simply not good enough:

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

Two other connectivity options in use today, Low Power Wide Area Network (LPWAN) and public cellular, are also insufficient to meet modern automation needs. While LPWAN technologies work well for low bandwidth IoT sensing, they will not work for applications like computer vision and robotics that require high bandwidth, low latency connectivity. IoT devices connecting using public cellular service also face coverage and QoS challenges, and the standard business model of metering and charging for data quickly becomes cost prohibitive. Needlessly transporting sensitive business data over a public cellular network causes deep security concerns as well.Two other connectivity options in use today, Low Power Wide Area Network (LPWAN) and public cellular, are also insufficient to meet modern automation needs.
While LPWAN technologies work well for low bandwidth IoT sensing, they will not work for applications like computer vision and robotics that require high bandwidth, low latency connectivity. IoT devices connecting using public cellular service also face coverage and QoS challenges, and the standard business model of metering and charging for data quickly becomes cost prohibitive. Needlessly transporting sensitive business data over a public cellular network causes deep security concerns as well.

As described in the definition of Industrial IoT, gaining an ROI from an IIoT project relies on gathering high quality data from every device deployed so the data can be analyzed for continuous improvement. This is especially true as AI can increasingly be applied to monitor, troubleshoot, and apply new rules to any areas of operational inefficiency. Yet today, **roughly 90 percent of all data generated in the field** is classified as stranded data because it cannot be accessed by core process control applications. Innovations in predictive maintenance and digital twins are not possible without reliable access to large amounts of data.

There is a new type of wireless connectivity that has only become available to enterprises over the last few years that many are not fully aware of — private 5G. Due to a change in spectrum policies across the globe, enterprises now have a choice to deploy their own private 5G networks. These are networks that they own and control. The data stays on their premises with the added benefit of robust security. Businesses have been deploying these networks since 2020 and the **trend is growing across industries**.

Let's take a look at some of the IIoT cases customers are deploying today, and how private 5G is providing connectivity for measurable improvements in productivity and efficiency.

Connected worker: Workers on the factory floor, in the warehouse, and in storage yards are equipped with devices like tablets, scanners, smart helmets, gas detectors and push-to-talk. These devices need to work reliably anywhere on premises or in the field and require ubiquitous connectivity for operational efficiencies and worker safety.

Remote equipment monitoring and predictive maintenance: One of the biggest IoT use cases in industrial environments is to remotely monitor equipment and predict maintenance needs before

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

anything breaks down. Connectivity to the equipment needs to be highly reliable and always available to keep things running smoothly.

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

IoT sensing in mobile robots: The last few years have seen incredible advances in automating industrial operations. This includes AGVs, AMRs, and robotics solutions for multiple workflows, which use a host of IoT sensors for video analytics, collision avoidance and navigation. The need for IoT sensors to maintain connectivity while moving presents yet another dimension to the problem since the robots traverse large areas, typically requiring a switch from one wireless access point to another along the way.

Owning and operating a private wireless network comes with several advantages for these emerging use cases:

Speed of deployment: A well-designed private 5G solution can be installed and deployed in hours, not weeks or months. The best systems are turnkey solutions that map into the enterprise IT infrastructure.

Wide coverage area: Because private 5G access points can efficiently transmit signal and antenna gains at higher levels than Wi-Fi, far fewer APs are required to cover the same area. Not only is this less infrastructure to manage, but it also dramatically reduces the cabling requirements for bringing wireless connectivity to these environments.

Deterministic connectivity: Applications that require real-time response from the network infrastructure — and associated data flows that require low packet loss, very little delay, and predictable bandwidth — need a transport medium that can identify these flows and prioritize them using strict service level objectives. Deterministic network capabilities that offer this type of functionality are a key component of private 5G.

Data security: Private 5G gives enterprises complete control and visibility over the network that transports sensitive business data, and the data can remain on premises. Given data privacy and compliance requirements within an enterprise organization, this is a must-have. For others, it lessens the risk of data loss or theft.

Granular quality of service (QoS) for critical applications: Private 5G can provide granular performance controls all the way down to the application and workload level. This means that mission-critical applications can be given connectivity preference within the private 5G network to ensure they are always on.

Simplified administration: The device onboarding process is far easier with private 5G since access control and authorization is built directly into cellular SIM cards, deployed as physical SIMs and eSIMs. Administrators can reduce the time it takes to provision devices and onboard users.

Cost savings: Private 5G can be delivered at a cost much lower than public cellular or wired solutions. In fact, they are being offered today at a cost that rivals Wi-Fi.

Here are some real-world results from one 1,260,000 square foot distribution center wherein a private mobile network solution was recently deployed. Using only 17 percent of the Wi-Fi indoor access points and 6 percent of the outdoor access points, the solution was quick to install and offered these measurable improvements immediately:

Coverage: Indoor coverage increased from 78 to 99 percent throughout the 700,000 sq. ft. facility. Outdoor coverage increased from 59 to 95 percent throughout the 560,000 sq. ft. yard. This lit up the entire facility with high-performance wireless connectivity.

Latency: Measurements taken after the deployment showed average latency became consistent and

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

was reduced by as much as 80 percent when compared to the Wi-Fi, especially when the network was under load or when devices are in motion. This means that scanners and AGVs perform as designed and react in real-time to any changes in the environment. (See Figure 1)

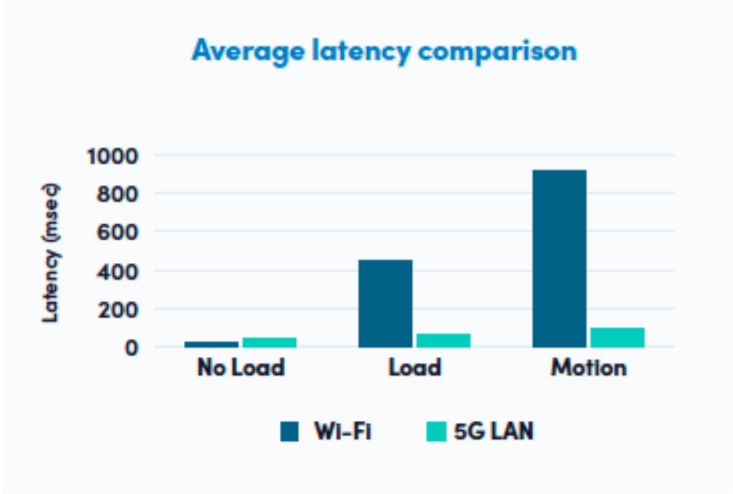

Figure 1. Average latency comparison

Total Cost of Ownership: The customer was pleased to find that the private wireless solution proved to be 47 percent the cost of Wi-Fi gear and 9 percent the installation cost, providing a TCO (Total Cost of Ownership) that is 32 percent of Wi-Fi.

Summary

The industry is at the very beginning of the move towards private 5G, but there is a real shift underway. I see three major drivers that will cause the market to take off in the coming years.

The first is the maturation of the private 5G device ecosystem. Every day more and more private 5G devices are coming onto the market, and as the more advanced 5G features are delivered — like ultra-low latency and 5G positioning — more sophisticated use cases like digital twins and machine vision can be supported.

The second driver is increased availability for spectrum globally. In June, the FCC announced that the areas in the US where shared CBRS (Citizens Broadband Radio Services) spectrum can be deployed is being increased, positively impacting thousands of businesses and millions of people. Globally we also are seeing an increase in countries setting aside mid-band spectrum for local licensing directly by enterprises. There is increasing government recognition of the positive economic impact of making spectrum directly available for enterprises to deploy private cellular networks.

The third factor is the growth of a neutral host model built on private 5G. As telcos start to abandon subsidizing DAS deployments for all but the largest enterprises, neutral host networks based on private 5G networks will increasingly be recognized as a solution that allows staff and guests to access to access the public cellular network from a private cellular network.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

© Pipeline Publishing, L.L.C. All Rights Reserved.