White Paper

5G Device
Networking

Navigating the 5G Device Landscape

A study on the benefits and challenges of the 5G device (UE) ecosystem and strategies to accelerate its adoption.

Authors:

Swapnil Srivastava
Practice Manager,
5G & Telecom Network,
Wipro Limited

Ashish Khare
General Manager & Practice Head,
IoT & 5G,
Wipro Limited

Vijay S Kesavan
Systems Solution Architect,
Network & Edge Group,
Intel Corporation

Bhupesh Agrawal
General Manager,
Networks & Edge Group,
Intel Corporation

Table of Contents

Executive summary

The rise of Industry 4.0 and the Internet of Things (IoT) has presented enterprises with new and demanding communication requirements that were not previously encountered. The data-driven decision-making processes and the growing need for substantial cloud computing have continuously increased the demand for higher bandwidth. The combination of higher bandwidth requirements and the need for mobility has led to a growing demand for a high-bandwidth mobile network like 5G. While the need for 5G is substantial, its adoption has not been entirely smooth. Several hurdles need to be addressed, including the availability of spectrum, the allocation policies for spectrum, and the development of the device ecosystem and supporting equipment.

5G communication technology has been developed with a focus on data communication. It offers various application scenarios, including enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication uRLLC, and Massive Machine Type Communication (mMTC), which enable high bandwidth, ultra-reliability, and support for a massive number of devices. The uRLLC feature not only provides very low latency but also ensures an exceptionally high availability of up to 99.9999%. In addition to these services, 5G offers better security mechanisms, such as Subscriber Concealed Identifier (SUCI), Subscriber Permanent Identifier (SUPI), and Temporary International Mobile Subscriber Identity (TIMSI), among others. Furthermore, Private or Enterprise 5G networks can be made even more secure through various other means.

Despite these benefits and features, one of the major hurdles in 5G adoption is the device ecosystem. The availability of end devices or User Equipment (UE) that support 5G is much lower compared to what is available for 4G and Wi-Fi. Additionally, the broad operating frequency band of 5G poses a challenge for many manufacturers to support the entire range.

Secure and dedicated connectivity for critical applications

Critical applications often require low-latency and highly reliable connections. Traditional network architectures that operate in a collision domain are not suitable for these types of applications, as they can introduce unpredictable latencies and packet jitter. In applications that control manufacturing line robots, most of the UEs are e-bonded with the SIMs to prevent any intrusion from the UE side. This e-bonding mechanism prevents the use of unauthorized UEs or the swapping of SIMs, offering a secure and robust network for enterprise devices.

Additionally, 5G's network slicing capability allows Private 5G networks to be divided into multiple virtual networks, each with its own dedicated resources and performance guarantees. This can be used to isolate different applications and traffic types, ensuring that even critical applications always have access to the resources they need.

Typical device requirement in Enterprise 5G

In the enterprise environment, the most common applications are manufacturing robots, Automated Guided Vehicles (AGVs), Programmable Logic Controllers (PLCs), and Supervisory Control and Data Acquisition (SCADA) systems. Many of these devices offer Ethernet connectivity or wireless connectivity through Wi-Fi, using protocols such as Profibus, ControlNet, and CANOpen.

In a multi-robot scenario, communication becomes even more critical. While 5G offers advantages like uRLLC which is crucial for the proper functioning of robots, many of these devices currently lack 5G connectivity.

Broadly speaking, devices (UEs) deployed in a manufacturing environment and connected to a Private 5G network can be categorized into three groups:

a. **Fully Supported:** Devices that have a built-in 5G modem and can connect directly to the 5G network. This includes many mobile devices like smartphones, tablets, and laptops, as well as some specialized devices like cameras with native 5G modems.

b. **Not Supported:** Devices that may never have an integrated 5G modem, due to factors like legacy design, cost, lack of mobility, power/size constraints, or a combination of these.

c. **Selectively Supported:** Devices like sensors that run on battery and report data infrequently, which can justify the use of a low-power, narrow-band 5G modem, referred to as Reduced Capability (RedCap) in 3GPP Release 17. While RedCap modems are still under development, devices supporting RedCap are anticipated in the future.

Devices from categories B and C that do not have a native 5G modem are typically bridged to the 5G network using an industrial gateway or router. The gateway supports a native 5G modem and multiple other connectivity modes, including Wi-Fi, Bluetooth/Bluetooth Low Energy (BLE) and wired connections.

It's important to note that even devices with a native 5G modem (category A) may not work out of the box in a Private 5G network, as the network might use a Mobile Country Code (MCC) and Mobile Network Code (MNC) that is not whitelisted. To overcome this, the firmware of the modem may need to be upgraded or modified to ensure that the MCC/MNC is permitted.

Challenges faced due to unavailability of devices supporting 5G

Modern enterprises, particularly in the manufacturing and mining sectors, often require the operation of complex multi-robot systems. These robots have various control mechanisms, including centralized, decentralized, and hybrid approaches.

When these robots are connected using conventional wireless mediums, the primary challenge is ensuring low latency and high quality of service (QoS). This requirement often necessitates the use of wired communication between the robots, as wired connections can provide the necessary low latency.

However, the use of wired communication restricts the mobility of robots, which is a critical requirement, especially in the case of Automated Guided Vehicles (AGVs). The need for both low latency and mobility poses a significant challenge for enterprises operating these complex multi-robot systems.

Comparison with Wi-Fi as a contemporary technology

Wi-Fi 6 (IEEE 802.11AX) and Enterprise 5G are two modern technologies that both offer high spectrum efficiency. This similarity might lead to the impression that these two technologies are competitors. However, analysis shows that they are not competing but rather complementary technologies. Each plays a unique role in industry settings by supporting different use cases. In certain scenarios where 5G UEs are not available, Wi-Fi devices can also leverage 5G connectivity.

A few major comparisons are given below:

Feature	Wi-Fi	5G
Operational spectrum	2.4 GHz, 5 GHz & 6 GHz unlicensed spectrum	Vast range of licensed spectrum in FR1 (410 MHz – 7125 MHz), FR2 (24250 MHz – 52600 MHz)
Coverage	Shorter coverage	Comparatively broader coverage
Architecture	Decentralized architecture	Centralized cellular architecture
QoS	Comparatively less predictable	Highly predictable
Connecting user	Very simple	Requires SIM/eSIM

Key strategy for device planning in the enterprise

When planning a 5G network and selecting UE devices, several critical factors need to be taken into account to ensure optimal performance and compatibility. Few of the important considerations are as follows:

Spectrum

Devices connecting to the network must support the specific operational bands planned for the 5G network. Since different countries utilize different frequency bands, it is essential to select UEs that are compatible with the local bands. In many countries, multiple bands are available, so network and use case planners must carefully choose the most suitable frequency band based on availability and the number of compatible UEs for their applications. In some countries, enterprises can directly acquire spectrum, while in others, they must obtain it through spectrum sharing agreements with Communication Service Providers (CSPs).

A list of major countries with frequency band is given below:

Country	Private 5G Spectrum
Argentina	700 MHz, 2600 MHz, 3500 MHz
Australia	2100 MHz, 1800 MHz, 700 MHz, 2300 MHz, 3575-3700 MHz, 25.1 GHz-27.5GHz
Brazil	700 MHz, 2.3 GHz, 3.5 GHz, 26 GHz
Canada	600 MHz, 1.7 GHz/2.1 GHz, 3.5 GHz, 2.3 GHz, 26 & 28 GHz, 3.8 GHz
China	2.5 GHz, 3.5 GHz, 4.8-5.0 GHz, 6 GHz, mmWave
France	700 MHz, 2.1 GHz, 3.5 GHz
Germany	3.5 GHz, 2.1 GHz, 700 MHz, 1.8 GHz
Japan	3.7 GHz, 4.5 GHz, 28 GHz
Netherlands	2100 MHz, 1800 MHz, 700 MHz
South Africa	700 MHz, 2.5 GHz, 3.5 GHz, mmWave
UAE	3.5 GHz
United Kingdom	2100 MHz, 1800 MHz, 2300 MHz, 3500 MHz, 24.25 GHz-25.25 GHz
USA	3.5 GHz, 3.55-3.75 GHz

Figure 1. Countries with Regulatory Provided Spectrum

Country	Private 5G Spectrum
India	700 MHz, 800 MHZ, 900 MHz, 1800 MHz, 2100 MHz, 2300 MHz, 2500 MHz
Kenya	2600 MHz
Malaysia	700 MHz, 3.5 GHz, 26/28 GHz
Mexico	700 MHz, 2.5 GHz
Saudi Arabia	3.5 GHz, 26 GHz
Singapore	2300 MHz, 3500 MHz, 2100 MHz, 26000 MHz
Switzerland	2.1 GHz, 700 MHz, 3.5 GHz

Figure 2. Countries with Operator Provided Spectrum

Device Planning

The selection of devices should be based on the licensed frequency band and the device category required for the specific application. Since Frequency Range 2 (FR2) is less popular, has fewer compatible devices, and offers a shorter range, it is generally advisable to choose bands within Frequency Range 1 (FR1) and select devices accordingly. In cases where 5G-compatible UEs are not available but the application requires the low latency and high bandwidth benefits of 5G, connectivity can be achieved by establishing a 5G network and creating a Wi-Fi network using 5G–Wi-Fi gateways.

Security

5G employs robust encryption algorithms like Advanced Encryption Standard (AES) and SNOW-V, among others. The security key is distributed across core network segments, mitigating the risk of International Mobile Subscriber Identity (IMSI)/Temporary Mobile Subscriber Identity (TMSI) catchers.

Mobile operators can utilize the elliptic curve integrated encryption scheme to regularly conceal and update a subscriber's TMSI Authentication and authorization in 5G are based on the Authentication and Key Agreement (AKA) method.

Furthermore, the use of SUPI and SUCI enhances security. SUPI, replacing the Globally Unique Temporary Identifier (GUTI)/TMSI/IMSI, is used for all plaintext transactions over the air, significantly bolstering the security of 5G communications.

Conclusion

While the 5G device (UE) ecosystem is currently not as rich as the Wi-Fi and 4G device ecosystems, the distinct advantages offered by 5G technology are driving its increasing adoption and maturation of the supporting device ecosystem. The superior security protocols, improved spectral efficiency, and the ability to support diverse use cases such as eMBB, uRLLC, and mMTC are making 5G an attractive choice for customers. As a result, a steady growth in the demand for 5G-enabled end devices is being observed, although there is still a long way to go before it reaches the level of maturity seen in other wireless technologies.

Regulatory bodies across different geographies are working on policies for the allocation of Private and Enterprise 5G spectrum, which is acting as an accelerator for the demand of 5G network deployment in various industry domains. This, in turn, is incentivizing Original Equipment Manufacturers (OEMs) to develop a wider range of 5G-compatible UEs to cater to the growing market needs. As the regulatory landscape evolves and the 5G device ecosystem continues to mature, we can expect to see a more diverse and robust selection of 5G-enabled devices becoming available, further driving the adoption and utilization of 5G technology in enterprise and industrial applications.

No product or component can be absolutely secure. Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy. Intel technologies may require enabled hardware, software or service activation.