

WHITE PAPER

How does 5G private cellular network work?

March 2026

Summary

The acceleration of industrial digitalization and rapid increase of IoT (Internet of Things) connected devices directly creates an increasing need for 5G private cellular network (5G PCN).

5G PCN is particularly beneficial for organizations and industries where reliable, secure, and high-performing wireless connectivity is essential. This network enables the use of advanced applications and adapts well with the increasing demand for industrial automation.

A 5G PCN, compared to Wi-Fi®, offers a better outdoor coverage, has better capacity, and can handle more devices than traditional mobile networks (3G/4G). Also, it affords users the ability to own and design their systems to meet their specific workflow. A 5G PCN is a large investment but at the same time, when compared to a wired installation, it saves costs by eliminating the need for trenching and improving operational efficiency.

Cellular networks have developed over the years and moved from one generation to another with each generation experiencing rapid changes in capacity and connectivity of mobile devices.

Table of Contents

1	Introduction	4
2	Benefits of 5G private cellular network	6
3	Use cases and applications of a 5G private cellular network	7
4	Differences between private and public cellular networks	8
5	Security and privacy considerations in 5G private cellular network	9
6	5G and video surveillance	9

1 Introduction

This whitepaper refers to a private cellular network as a network that has its own core and uses cellular technology to provide connectivity within a specific location. The core network acts as the intelligent control center of the PCN and is, for example, responsible for managing data traffic, authentication, user sessions, security, and service provisioning.

Unlike public cellular networks that are operated by mobile network operators (MNOs) and meant for the public, private cellular networks are designed exclusively to meet an organization's specific needs. Only authorized users can access private cellular networks.

Radio Access Network (RAN) uses radio signals to connect user devices to 5G private cellular network.

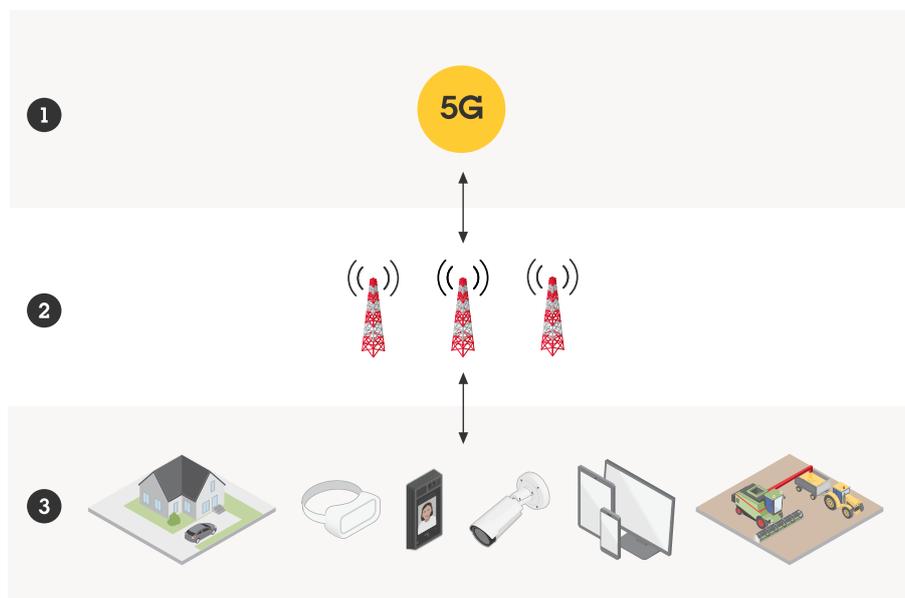


Figure 1.1 1: 5G core network 2: Radio Access Network (RAN) 3: User Equipment (UE)

5G supports a broader frequency spectrum than its predecessor. It supports frequencies in three bands: high-band, mid-band, and low-band.

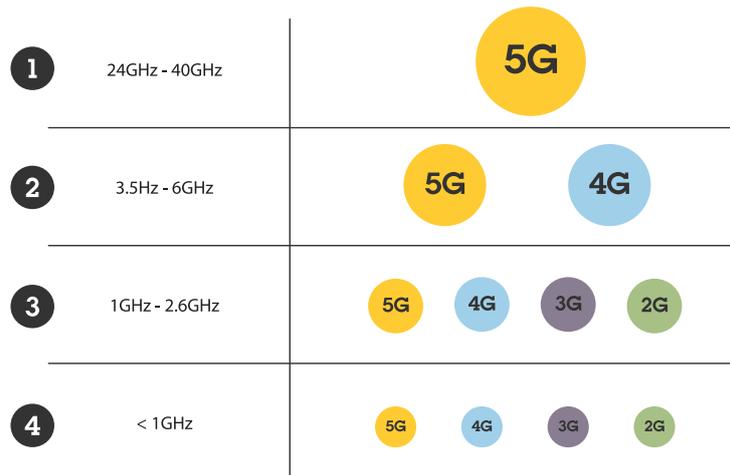


Figure 1.2 1: High-band 2 and 3: Mid-band 4: Low-band

- High-band delivers ultra-fast speeds with an ultra-low latency of about 1 millisecond.
- Mid-band's fast speed and low latency for mobile devices enable high-definition video streaming, virtual and augmented reality, and cloud gaming with high reliability and massive connectivity.
- Low-band offers broad coverage and better indoor penetration.

These 5G bands are also referred to as 5G sub-6G hz and 5G millimeter waves (24GHz - 40 GHz) and they impact the network's coverage, capacity, and speed.

5G is the fifth generation of cellular network technology, designed to provide faster data speeds, lower latency, and greater capacity compared to previous generations. Theoretically, it offers a maximum download speed of 20 Gbps and peak upload speed of 10 Gbps. Real-world, user-experienced speeds are typically lower, often exceeding 100 Mbps. These peak rates, primarily achieved through millimeter waves spectrum, are designed to support 100 times higher traffic capacity than 4G LTE. With this data rate, streaming, downloading, and uploading high data content is smoother and faster.

2 Benefits of 5G private cellular network

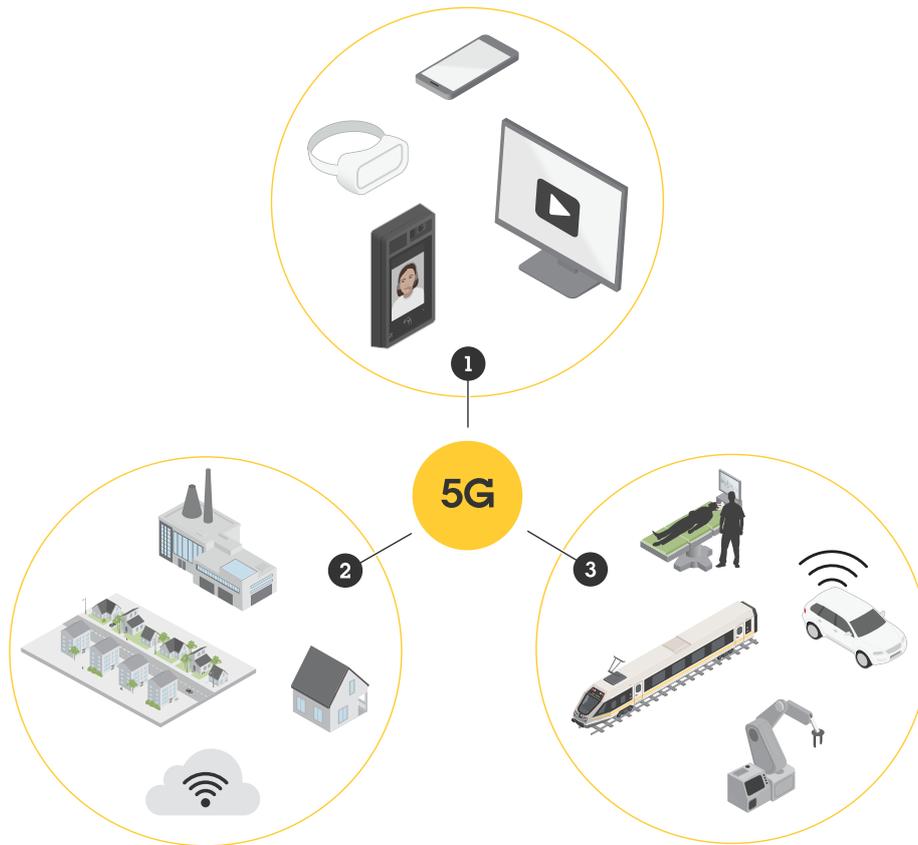


Figure 2.1 1: High-performance mobile broadband 2: Huge machine type communication 3: Reliable low latency communication

1 High-performance mobile broadband: With a 5G private cellular network, you can allocate, control, and disperse network bandwidth within a building or location based on your connection needs. It allows network slicing, which means you can create multiple virtual networks with different performance characteristics, within a physical infrastructure. This allows organizations to tailor the network to specific use cases. For example, an airport running a PCN can offer an airline their own private network as a slice of their PCN in a more secure way than a traditional Wi-Fi or public network.

5G is less susceptible to interference and provides better security than Wi-Fi. Since the network is private, it offers enhanced security and control over data traffic. This is important for organizations that handle sensitive information. It also works independently from public networks and doesn't have the problem of network congestion from public users or outages caused by malfunctions in systems, outside the organization's control.

2 Huge machine type communication: It supports IoT and machine-to-machine (M2M) communications, which are essential for modern industrial and enterprise applications. It has a larger coverage capability and can support more connected devices than 4G. The growing number of devices that use IoT and M2M shows the increasing need for 5G.

3 Reliable low latency communication: 5G networks have lower latency, which is the time a packet takes to travel from a source to a destination. Applications that require real-time responsiveness, such as online gaming, self-driving vehicles, and telesurgery require a cellular network with lower latency.

A private 5G network is a large investment, however, it also has the potential to save cost. Cost-saving can be in the form of direct installation cost and operational efficiency. For example, in an airport, PCN helps save cost in the following ways:

- **Cost-effective perimeter installation:** Trenching around large fences can be very costly. PCN doesn't need trenching as long as there is power.
- **Faster and more flexible installations:** You can mount cameras without requiring new connectivity infrastructures. Trenching and cables can have unwanted impact on various parts of an airport, including buildings. Also, these wired installations rarely have a positive aesthetic effect on the environment. Trenching, drilling, and cable drawing among other needed construction activities takes time, creates noise, and road blockages which may disturb or obstruct daily work in organizations
- **PCN complements old infrastructure:** Rather than replace old, wired infrastructure with a new one to increase capacity, PCN can complement and offload the network. It also allows you to add new devices.
- **Temporary connectivity:** PCN has the advantage of mobility since it is difficult to manage a moving vehicle connected to a wired network. It comes in handy on many occasions where you temporarily need connectivity, for example, on an airfield, in a trade fair with customers, on a construction site on your campus, or at an indoor or outdoor event.

3 Use cases and applications of a 5G private cellular network

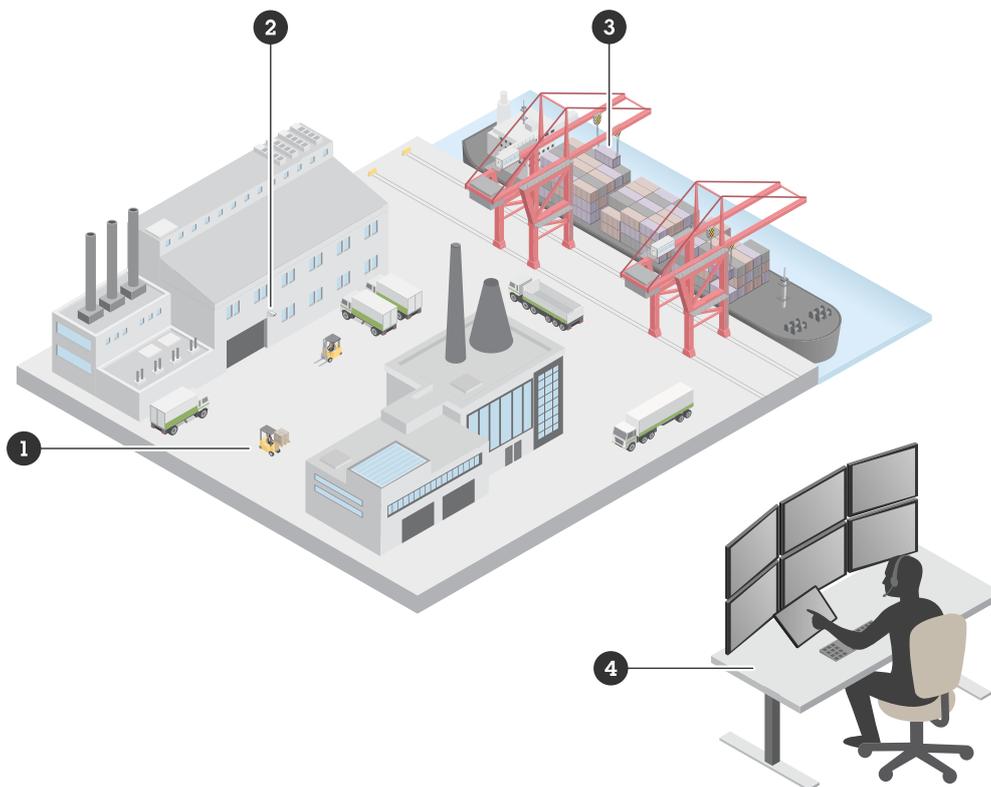


Figure 3.1 1: Real-time workload tracking 2: Video surveillance 3: Telemetry on machines 4: Surveillance monitoring and remote operations

5G private cellular network is most suitable for organizations that operate in large, complex, and dynamic environments and require secure and reliable mobile connection.

1 Real-time workload tracking: 5G PCN enables real-time tracking. For example, manufacturing and industrial factories might need to track their assets in real-time to know their precise location and status. To do this, they need ultra-low latency and reliable connection which 5G provides. Hospitals can also use private 5G for reliable connectivity of life-critical medical devices, low-latency telehealth consultations, telesurgery, and

tracking of mobile equipment like IV pumps and wheelchairs throughout a large campus, ensuring data security and network performance.

2 Video surveillance: Dynamic environments such as a port with cranes, trucks, and workers, need seamless video surveillance over outdoor and indoor areas. 5G PCN provides wide coverage and seamless handoffs a port needs to track assets, manage autonomous vehicles, and keep operations running smoothly.

3 Telemetry on machines: To predict a machine's maintenance need, operational analytics and be able to control it remotely, you need a constant flow of data from it. Such data can include spreader position, load weight, and motor temperature. For example, a massive ship-to-shore crane can become a fully connected digital asset. A private 5G connection replaces fragile and maintenance-heavy fiber optic cable reels and wirelessly transmits critical information electronically. Simultaneously, the same connection can stream video feeds from cameras mounted on the crane itself, giving operators a clear view of the container and its surroundings.

4 Surveillance monitoring and remote operations: Critical infrastructures (energy, utility, mining) and large venues (airports, stadiums) often need to monitor the venue and remotely operate their machines. A utility company, as an example, needs to monitor their grid sensors. A private 5G connection can handle both, that is, monitoring locations and operating machines, while guaranteeing an efficient performance for critical operational traffic.

4 Differences between private and public cellular networks

While a private cellular network is dedicated to a specific organization, a public cellular network is shared and used by the general public. Though they both provide network connections, there are certain differences between them. These include:

Feature	Private network	Public network
Ownership	<p>A dedicated private network is separated from any publicly operated mobile network. It is operated exclusively for an organization.</p> <p>It provides the organization with full control of the network, devices, and security policies.</p>	<p>It is owned and operated by mobile network operators (MNOs) and end users have limited control.</p>
Configurability	<p>A PCN provides the organization with full control of the network, devices, and security policies.</p> <p>The organization can configure the uplink and downlink radio resources as well as set QoS levels, configure network slices, and extend the network as they see fit.</p>	<p>You have less possibilities of specific network configurations for your subscription.</p> <p>All configurations will need to go through the MNO's administration. It is however possible to create a virtual subnetwork (network slice) of a MNO's network which behaves like a private network and thus utilizing the MNO's core and network nodes instead of owning your own network equipment.</p>
Cost model	<p>It requires a significant investment to buy and deploy its hardware and to maintain the network. However, it is a</p>	<p>MNOs are licensed by government and must follow certain regulations. You need to</p>

	one time investment and with it, you can use unlimited data.	pay a subscription fee to the MNO.
Security	It is highly secure because you can directly manage security, keep data on-premise, and traverse the public internet or MNOs' network securely. Private SIM cards also add an extra level of security through SIM PIN, if configured.	You have to entrust your data to third party data security and policies. Also, data travels over MNOs' shared infrastructure.
Access and coverage	It has low latency and wide area coverage because connection and access is restricted to only authorized devices and deployed where the organization needs it. You can control every single device regarding how much data a device can use and its quality of service.	It has limited coverage and there is a possibility of network congestion. This is because your device, alongside many other devices, compete for shared resources and you don't have control over who uses the data and how much data they use.

In summary, a public network has a simple, subscription-based model and comes in handy when a good-enough performance is acceptable. A private network is needed when performance, security, and reliability are critical to an organization's operations and cannot be compromised.

5 Security and privacy considerations in 5G private cellular network

A private cellular network provides organizations with a secure and private connection. Also, with a private cellular network, organizations have ownership and control of their data.

In addition to protecting network access through SIM cards, an end-to-end encryption helps to protect both operational and personal data. Only authorized users, devices, applications, and systems should be allowed on the network.

Physical access to the on-premises core server or radio unit should be limited and controlled. This is to ensure that only people with authorized access can get to the physical components of your network security.

Below are some security risks in a 5G PCN:

- **Misconfiguration:** A misconfigured network slice can bypass shared controls. This can create a security gap that's hard to detect and easy to exploit.
- **Side-channel attacks:** It could be possible to extract information from indirect signals like timing, power, or memory usage.
- **Denial-of-service (DoS):** Attackers may jam radio access channels, overload APIs, or flood a network slice.
- **Eavesdropping and traffic analysis:** Data in a 5G network is encrypted but not always metadata. Attackers who observe traffic patterns can infer user behavior, location, or application type.
- **Meddler-in-the-middle (MITM) attacks:** A device can simulate a 5G base station and compromise both confidentiality and integrity.

6 5G and video surveillance

Although a 5G network utilizes an IP based architecture, it differs significantly at Layer 2 (Data Link Layer). This makes a 5G network behave differently than a wired or Wi-Fi network.

The default behavior of an IP camera is that it is passive and waits for a client to connect to it. Through a VMS (Video Management System), the cameras are often discovered by protocols like mDNS (Multicast DNS) or UPnP (Universal Plug and Play). These protocols rely heavily on the link layer and are not supported by a 5G network. In order to onboard a camera on a 5G PCN to a legacy VMS such as Genetec, Milestone or AXIS Camera Station, the camera should have a known static IP address. It is also possible to scan an IP range from the VMS, however, the camera still needs to have a static IP address within a known IP address range.

By using, for example, WebRTC or a VPN solution, you are not dependent on having a known static IP address as the client and server connects through a common known server. However, this is not natively supported by an Axis camera or any legacy VMS.

5G PCN operating in the mid band (sub 6 GHz) supports a max bandwidth of 100 MHz which limits the available bitrate. In addition, the signal quality can change for a moving device. A stationary device can also experience changes in the radio environment affecting the signal quality and thus the available bitrate on the channel. Compared to a wired network, a 5G PCN has a more limited and unpredictable bitrate and thus more susceptible to congestion.

A classic video stream profile is often very spiky. An I-frame generates a large chunk of data that needs to be transmitted over a short time period. In case of insufficient bandwidth, this may cause broken buffers, latency, dropped frames and poor video quality.

Compared to a wired network, a 5G PCN, operating the sub 6 GHz band, has additional latency of ~10 ms. This is irrelevant for surveillance use cases such as live view and Pan-Tilt-Zoom (PTZ) control but essential for other use cases such as autonomous vehicles. Network congestion can cause latency to increase significantly.

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.