Military-Grade 5G: Use Cases and Challenges

5G will boost capabilities ranging from critical communications to autonomous vehicles and robotic surgery
Communications systems for military and government applications have evolved from analog to digital, include high-resolution imagery, and allow for rapid adoption by multiple new users. Today’s critical communications networks serve military, government, and public safety personnel with ad hoc communications to boost networks in emergencies and fill coverage holes. Fifth-generation (5G) cellular extends the capabilities of critical communications, allowing 5G network deployment on bases, in emergency scenarios, and on the battlefield.

Beyond tactical communications, 5G enables a broad variety of applications in military and government realms. Planes, ships, Humvees, and other vehicles will integrate 5G connectivity. 5G robotics allows for smart warehousing and telesurgery. Self-driving military vehicles will create new opportunities and use cases. 5G will seek to secure communications and discover security gaps. Evolving 5G non-terrestrial networks (NTNs) stand to make all of these new applications a reality.

To assure performance, however, these different applications require unique approaches to design and test. By taking a multistep approach, you can ensure your product seamlessly integrates into the final design. You also confirm that your design meets 5G’s promise for military and government applications.

---

**Key points covered in this white paper:**

- 5G enables new use cases for military and government
- Satellites will enable new capabilities
- Do not compromise on performance or security
5G in Space

5G NTN holds the promise of ubiquitous, or greater, cellular coverage. Using space-borne or airborne assets, 5G can enable service in areas otherwise without coverage. Tactical military users might use this feature to establish communications over new lands, air, or seas. First responders who tend to emergencies in forests, mountains, or other areas with low communications coverage also can use 5G NTN.

An evolving standard

The Third Generation Partnership Project (3GPP) develops the standards for 5G, with the 5G New Radio (NR) standard continuously evolving. Until now, base stations have been ground-based or terrestrial, but 3GPP ratified NTN as a feature in Release 17. The round-trip time in NTN can be much larger than in the terrestrial case. You compensate for propagation delay by making certain assumptions about the delay range.

One enabling technology for NTN is the global navigation satellite system (GNSS). Through GNSS, the user equipment (UE) can establish its own position, frequency, and time reference (see Figure 1). It can compute the time and frequency difference from the satellite signal and apply timing advance and frequency adjustments for the UE. The timing advance helps ensure coordination or time synchronization of UE signals from multiple UEs, so they do not collide with one another.

Figure 1. The first focus of NTN is on UEs with GNSS capabilities, supporting FR1 with power class 3 (which is max power +23 dBm within FR1 bands). 3GPP may consider additional enhancements to support smartphones connecting to LEO satellites.
The specific architectures will be finalized as the standard develops. No matter the final choice, the architecture will start with a UE block. Until 5G, UE comprised mobile phones. Now, UE includes vehicles, sensors, and watches. The UE typically communicates with the base station, which in 5G is known as the gNodeB. You can refer to the 5G Core Network as the Next Generation Core (NGC).

Developing under uncertainty

Researchers and developers face several challenges with NTN. The standard remains in development, so commercial equipment and prototypes are not available. That means finding other ways to research, prototype, or develop. Unfortunately, available commercial-off-the-shelf (COTS) UEs and gNodeBs will not work with the amounts of Doppler and delay found in space-borne communications links.

To develop NTN, take a crawl-walk-run approach that starts with basic software modeling. The software tool should model the following:

- downlink and uplink transmit and receive chains of the UE
- the gNodeB
- the signal propagations to and from the satellite
- the satellite’s motion
- the antennas
- the delay and Doppler throughout the system

The UE will pre-frequency shift its transmission to counter the Doppler shift of the satellite. The gNodeB must also do this, but in a way that is common to all served UEs, no matter their location. When a UE attaches to the network and looks for a base station, it must assume a greater range of frequency offsets than it would in the terrestrial case. Although COTS prototypes are not yet available, you can simulate NTN links in software and prototype them with emulators. Use hardware emulators that are more easily customizable for mimicking NTN links. You can perform this prototyping in a lab or a chamber on a small-scale basis.

When NTN equipment becomes available, you should prototype this with real equipment in the lab or chamber on a small-scale basis. Follow that step with a full-scale implementation, deploying with actual equipment on the target platform. Then engage in periodic maintenance testing.
Tactical Communications

5G NTN promises transformative improvements for military and government agencies worldwide. They want to leverage private 5G networks on military bases, in government buildings, on the battlefield, and in emergency scenarios. By adopting 5G, military, first-responder, and other agencies can accelerate the integration of multiformat radios and transition to custom digital modulation formats (see Figure 2). These capabilities pave the way to heightened communications capabilities and enhanced security.

Figure 2. 5G offers many advances to critical communications, such as ad hoc military networks on the battlefield or for first responder applications via satellite connectivity.

With the adoption of more advanced digital capabilities, for example, military, public safety, and government agencies gain access to higher-speed downloads and the sharing of data-intensive tools such as maps and video. Sharing more detailed intelligence more quickly enables heightened situational awareness — ideally, in real time.

5G provides increased flexibility for tactical communications spanning use cases from enhanced mobile broadband to ultra-reliable low-latency and massive machine-type communications, as well as increased security. Tactical networks could provide augmented / virtual reality in combat and combat training, battlefield telesurgery, tactical self-driving vehicles, ad hoc secure communications, and connected battlefield assets such as planes, ships, and missiles.
Proving military 5G performance

For these agencies and organizations, however, 5G adoption is not simply a lift and repurposing of existing technology. Military and public safety environments differ significantly from commercial 5G environments. Gauging performance proves difficult, as testing in battlefield terrains, in crisis scenarios, or with planes and ships is not easy or accessible. You probably want to characterize the network and limits of service for specific use cases, such as over temperature, under jamming or interference, and under different terrain. You may also value some key performance indicators more than others, such as sensitivity, battery life, or robustness to temperature. In other cases, the network could be self-deployed, meaning you will need to test, deploy, optimize, and maintain the system.

Four 5G elements require testing in tactical networks:

- The UE could be a subscriber’s mobile device, such as a cell phone, tablet, or modem, or it could be a vehicle or a sensor.
- The gNodeB is a 5G wireless base station that transmits and receives communications between the UE and the mobile network.
- The channel tests the link between gNodeB and the UEs.
- The core network encompasses everything supporting the network.

To test a UE, emulate the system that communicates with it, the gNodeB (see Figure 3). Using an emulator rather than a real gNodeB gives you a greater level of control and flexibility. It also lets you observe metrics from the UE, which a real gNodeB would not provide. You’ll be able to perform tests repeatably. You should do this in nonstandalone or standalone mode and in frequency range 1 (FR1) or FR2.

Figure 3. To test a UE, you emulate the gNodeB, which is the system that communicates with it. Metrics of concern include a UE’s battery life, battery aging, or battery life against temperature. You also want to observe quality of service, such as block error rate or sensitivity.
A military / government 5G network usually takes one of two forms. If a service provider offers a public or private or standalone network, the service provider should deliver the limits of the service. You may need to characterize or verify the network and limits of service. Alternatively, a self-deployed private or standalone network could look like a smaller version of a commercial network or backpack system. The network will have its specifications, but deployment could impact service.

Once you have deployed the 5G NR network, you must field test the base stations and the entire network. One way to do this is with a special test UE, which will have dedicated capabilities to report detailed metrics. Driving or walking around with the test UE lets you test the network and report on base-station signal strength. It provides random access channel information, transmit power, the amount of multiple-input / multiple-output and modulation the channel can support, block error rate, quality metrics of the single sideband beams, and throughput and latency.

5G coverage in the air for crewless aerial vehicles and other airborne assets with 5G communication links will be available soon. A test UE mounted on a drone can record data of the coverage and metrics. This is a simple extension of what the UE already does on the ground.

**Vehicles: 5G on the Move**

We categorize 5G devices as user equipment because the vision is for 5G to go beyond cell phones. Anything can be a UE now, including aircraft, ships, Humvees, and other vehicles. Outfitted with 5G for long-haul communications, these vehicles can use 5G to enable communications, high-data-rate video conferencing, and Internet of Things sensors. Eventually, these capabilities will evolve into self-driving or autonomous vehicles. The goal is to eliminate service members from some missions, although a hybrid approach will require someone on board to oversee vehicle performance.

Use cases range from base-contained vehicles, which would improve energy efficiency, to field and combat vehicles. The development projects spurring this progress focus largely on advancing methods for vehicles to identify and understand their surroundings. Primary examples include radar, lidar, and sensing techniques. Artificial intelligence and machine learning will sort through, process, and act on this information. Connecting all this information is critical to success, shouldering 5G with succeeding at this task in a very crowded, complex signal environment.
Complex signals in motion

Ships, planes, and ground vehicles have different transmitters and receivers, including telemetry devices, communications transceivers, radar and satellite communications, and surveillance systems (see Figure 4). They must all operate simultaneously without compromising the performance of other systems or damaging them. For example, improperly designed high-powered radar could damage sensitive satellite receivers. Planes, ships, and other vehicles with 5G make the RF environment more complicated.

Figure 4. New ships should go through these phases to properly deploy the bevy of transceivers involved in their operation. To develop 5G systems on vehicles, we recommend a crawl-walk-run approach that starts with basic software modeling. The software modeling tool should model the UE downlink and uplink transmit and receive chains, the gNodeB, and the signal propagation of other communications systems on the vehicle.

Vehicles with communications equipment, radar, surveillance systems, and other equipment pose potential electromagnetic compatibility issues. Careful planning must take place so that all of the systems can operate simultaneously and safely. Software modeling can help you discover potential issues. The software modeling tool should model the downlink and uplink transmit and receive chains of the UE, the gNodeB, and the signal propagations of other communications systems on the vehicle.

In the planning phase, simulating signals in software determines electromagnetic compatibility using a 3D model of the deployment platform. The finite-difference time-domain (FDTD) method is based on volumetric sampling of the electric and magnetic fields throughout the complete space. This method updates the field values while stepping through time, following the electromagnetic waves propagating throughout the structure. As a result, a single FDTD simulation can provide data over an ultra-wide frequency range.
You can also boost confidence by prototyping signals in the lab on a small scale to gauge performance in the field. In place of COTS equipment, use hardware emulators, which are easy to customize and adapt. The prototyping is conducted in a lab or chamber on a small-scale basis. Once you are satisfied, follow up with full-scale implementation, deploying with actual equipment on the target platform. Following that is periodic maintenance testing.

In the prototype phase, simulate signals with signal generators and other emulation equipment. You can adjust signal levels to simulate the real-world environment on a much smaller scale inside a chamber. Measurements determine electromagnetic compatibility.

Robotic Surgery

In addition to autonomous vehicles, the military landscape will evolve with the greater integration of robotics and exoskeletons, all employing an increasing level of artificial intelligence. These advances will help ease the workload and physical burdens of service members while improving situational awareness. 5G enables a new application that promises to transform medical care for military personnel: robotic surgery.

Figure 5. Robotic surgery will save lives on the battlefield and in emergency scenarios such as natural disasters. For this application to succeed, 5G will have to enable very low-latency connections that allow a doctor to remotely direct the surgery.
In a conflict, medical response time often determines survival. Extensive injuries and resulting blood loss mean the window for lifesaving procedures is small. With robotic surgery, military doctors could quickly perform operations from a distance using robotic arms and cameras (see Figure 5). Housing such equipment on medical vehicles would eliminate the need to transport patients to begin treatment.

For such systems to succeed, however, these highly intelligent systems must work under various environmental conditions with no downtime. The goal is for these systems to become so intelligent that they perform some procedures with minimal or no oversight. The growing adoption of 5G networks paves the way for such connectivity by supporting high data transfer, approaching rates closer to real time. To enable doctors to perform robotic surgery remotely, however, 5G networks must eliminate the latency incurred in the relay of information.

**URLCC is key**

3GPP, which oversees 5G standards development, includes ultra-reliable low-latency communications (URLLC) for critical networks. URLLC applies to the end-to-end connection between the client and the server, with low latency typically lasting only 2 to 3 milliseconds. It can range down to 1 ms for end-to-end latency. The result is an ultra-reliable connection between the device and the network.

By promising URLLC from space, 5G NTN can provide this level of reliability on a widespread, accessible basis. While it targets remote applications like robotic surgery, URLLC could eventually provide an alternative to terrestrial connectivity for essential services such as hospitals and emergency responders. Enabled by 5G, doctors can provide better care remotely anytime and anywhere.

URLLC’s potential, however, comes at a cost. Harnessing the components required to make it work presents significant challenges across the wireless communications spectrum. Chipset and device vendors will face new design and test challenges. Network equipment manufacturers and mobile network operators will confront new network latency and reliability demands. Designers must harness and implement the components of URLLC in chipsets, devices, networking equipment, and mobile networks to successfully deliver on the promise of 5G for applications such as robotic surgery.
The Coexistence Challenge

For radar and satellite applications in particular, 5G raises another challenge: coexistence. Because these applications may use the same spectrum as 5G, they can impact one another, leading to service disruption or performance degradation. Coexisting signals have the right to operate in the same frequency range, but one signal usually takes priority. For example, radar signals typically take priority over 5G signals. As a result, 5G needs to shut off or move to another frequency.

Satellite signals can also coexist with 5G signals. For example, 5G NR FR2 overlaps with fixed-satellite services (FSS) Earth station uplinks at 27.5 to 29.5 GHz and FSS downlinks at 37.5 to 40 GHz. This overlap creates questions around how interfering waveforms interact and how much in-band and out-of-band suppression is needed. You also need to determine how much guard band is necessary and what metrics to consider in assessing impact.

How it impacts you

To test the impact of radar or satellite on a 5G network, you can use a 5G test UE in the field. This approach provides a detailed view of the quality and throughput metrics of the 5G network. To test the impact of 5G on a coexisting signal, you can use a signal analyzer (see Figure 6). The signal analyzer can run analysis software measuring many signal types, including radar, satellite, and 5G.

You can simulate radar signals in several ways, depending on the fidelity and emitter parameters required. By leveraging software, you can generate single radar emitters or high-density emitter environments. These simulations create threat environments that let you specify parameters such as amplitude, frequency, pulse width, modulation-on-pulse, pulse repetition interval, coherent processing intervals, and antenna scan modulation.

Creating satcom simulated signals is as easy as using a vector signal generator with digital video broadcast (DVB) software. Today’s software can generate a number of DVB signal standards. The signal-creation process allows you to simply enter the signal parameters, including pseudo-noise (PN) sequencing and user-defined data patterns.

For scenarios in which it is difficult to generate realistic conditions with signal generators and software, use a record and playback system. Here, a system records the signals live on a platform and brings the recording back into the prototyping platform lab. It replays them with a vector signal generator.
Figure 6. 5G-radar coexistence studies the impact of radar on 5G and vice versa. This issue grows increasingly prevalent on bases, planes, or ships. 5G spectrum monitoring helps detect signals that may interfere with the 5G network or ensure that the 5G network is operating at specified levels.

With your 5G network, you face unknown coexistence vulnerabilities. But 24/7 monitoring can help you secure the network from coexistence conditions. By prototyping coexistence conditions for research, you can expose those conditions and make sure they will not negatively impact your 5G system.

The Security Threat

For military and government applications, reliability reigns supreme. Service cannot go down in life-and-death scenarios. As cybersecurity risks increase, data reliability also becomes critical. Compromised data transmissions put devices, patients, and whole operations at risk. Cybercriminals can change information, status, and other aspects so that individuals and agencies are responding to incorrect information. Cyberthreats include finding the location of forces or their equipment. Suppose foes attack the Global Positioning System signal in the base station. In that case, they can potentially overwhelm the base station by using a UE simulator to mimic multitudes of UE.

Remember that an exploit that successfully enters a device can spread to the whole network. To measure cybersecurity defenses, you must rigorously test for network vulnerabilities. You want to test your system for its resilience, not just its ability to detect a threat and respond appropriately.
Hone your skills

Solutions now present opportunities to engage hands-on with attacks that simulate real-world threats (see Figure 7). Security professionals working in controlled environments gain cybersecurity skills and test their organization’s security posture. They train in use cases that include security operations, analysis, forensic specialists, “situational operations” testing for new products, software releases, and restructuring. To ensure a realistic training environment, such solutions simulate real-world legitimate traffic as well as malicious attacks. Sending threats into your system as a “bad guy” lets you gauge what your system can withstand.

Figure 7. 5G security is critical. Although the standard improves some security elements, attack surfaces have multiplied. You can use a wireless test platform to prototype pseudo-base station attacks. Research the attack beforehand to determine usage conditions and constraints.

When choosing a cybersecurity solution for a military or government 5G network, you want a rich library of predefined threat scenarios. For an optimized learning experience, you also want access to instructional and reference materials, as well as lab exercises. A scalable and flexible learning environment should offer services such as the development of custom threat scenarios integrating an organization’s security controls.
The 5G Future Is Now

In the United States and globally, 5G installations in military and government locations are improving communications, streamlining supply chain logistics, and enabling technology firsts that offload burdens from warfighters and workers. These use cases will quickly expand as support for their development continues to grow.

Because these advancements do not yet exist, you may want to use software to simulate their features. Examples of such features include NTNs, where the 5G satellite link is simulated; UE-to-UE communication; and connected vehicle to anything. 6G technology will also necessitate a software simulation feature as hardware development becomes defined. Once the concept is investigated in software, you can use hardware-in-the-loop to prototype the new feature with off-the-shelf solutions.

Next, development and integration testing offers control, observe, and repeat functionality. You then move on to performance characterization of the complete 5G system. In the final use case, you test and assess the security of the finished solution.

Military and government applications demand the highest levels of reliability and security. You need not take big leaps. You can rely on gradual steps to ensure performance through validation and emulation. Find out how Keysight can support the development of these use cases today and as the standards and technology evolve.
Reference

New Services and Applications with 5G Ultra-Reliable Low Latency Communications (2018):


Please explore our resources on 5G including the following:

- The Essential Guide for Understanding O-RAN
- Satellites Bolster 5G Through Non-Terrestrial Networks
- How 5G Will Influence Autonomous Driving Vehicles
- How 5G and IoT are Shaping the Automotive Industry
- The Challenges of 5G C-V2X Testing