5G challenges and opportunities

Empowering Trust®

Executive summary

Driven by trends such as high-quality communication and the Internet of Things (IoT), the number of connected devices is expected to grow by more than 10 times than what existed in 2019. In order to keep up with this need for more connected devices as well as demands for increased data speeds and reliability, technology standards for cellular networks are expanding into their fifth generation, called 5G. This new generation will enhance the capabilities of mobile broadband, massive machine type communications and ultra-reliable, low-latency communications. It will enable the development and adoption of new applications that have been pursued for a long time, such as augmented reality (AR) and virtual reality (VR), self-driving cars, smart medical services, and smart buildings. However, these opportunities come with challenges. 5G requires large infrastructure investments to realize its full benefits. Also, the technology requirements for hardware, software, raw materials, communication architectures and applications are radically different than what was required for previous cellular generations. The expanded connectivity and high-risk applications of 5G, such as autonomous vehicles, also increase security challenges. This white paper outlines the evolution of 5G, its technological requirements, industrial opportunities and security challenges.

Focuses of this White Paper

- **Evolution and key technologies from 1G to 5G**
- **Three major application scenarios and key technological breakthroughs of 5G**
- **Promising industries accelerated by 5G**
- **Full 5G Ecosystem Standards**

Demand boosts development of mobile communication.

The smartphones developed in the 3G/4G era have changed people's lifestyles. As mobile phones featured more and more functions, they replaced many devices, including telephones, fax machines, scanners, recorders, cameras, video cameras, televisions, stereos and remote controls. As lifestyles changed, new needs were created. The digital generation's desire for online self-branding on social media increased the demand for data volume and transmission speed. Real-time cloud storage and computing services were developed to accommodate the need for a large amount of video and audio information exceeding the capacity of a mobile phone's memory and processor. In order to make the connection between mobile phones and the cloud operate more smoothly, the requirements increased for network transmission rates and audio and video quality.

5G, compared to 4G, has three main improvements — greater bandwidth, ultra-high network speed and low latency reliability. These advances in technology will enable the realization of IoT, which includes smart healthcare, smart buildings, smart home appliances, self-driving cars, and VR and AR devices.

Consumer demand	Use cases	Market
Low latency	Gaming, AR/VR, telepresence, industrial and medical automation, autonomous cars	Consumer, healthcare, industrial, automotive, municipalities
Massive connectivity	Smart cities, vehicle to everything (V2X), entertainment venues, smart homes	Consumer, auto, municipalities
High reliability	V2X, autonomous vehicles, smart cities, industrial and medical automation, two-mission critical communications for uses such as (V2X, emergency response location positioning	Automotive, municipalities, healthcare, industrial
High-traffic density	Malls, stadiums, public events, e-commerce	Consumer, retail
Large-data volumes	AR/VR/mixed reality (MR), ultra-high definition TV, smart cities infrastructure systems, machine learning and artificial intelligence	Consumer, government, research, industrial, municipalities, retail

Evolution and key technologies from 1G to 5G

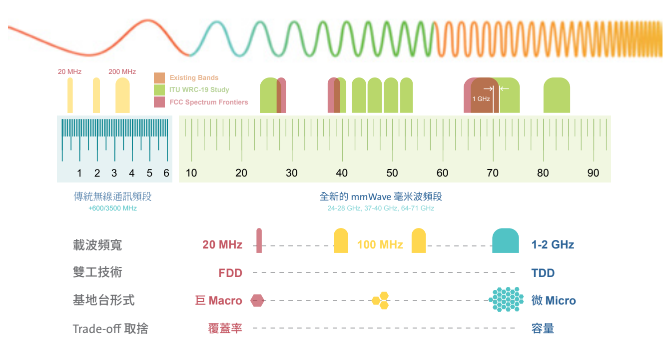
The evolution of each cellular generation is mainly recognized by the difference in transmission rates. But, in addition to quantified improvements, consumers are looking forward to qualitative progress, i.e., technologies that drive innovative applications and solve application issues. Table 1 shows that from 1G to 4G, in addition to the increase of available frequency bands, there are also differences in capabilities and network connections.

Parameter	1G	2G	3G	4G
Year	1980	1993	2001	2009
Technology	AMPS (Advanced Mobile Phone System), NMT, TACS	IS-95, GSM	IMT2000, WCDMA	LTE, WiMAX
Network Protocol/ Architecture	FDMA	TDMA, CDMA	CDMA	CDMA
Information Exchange	Line Switching	Audio: Line Switching Material: Packet Switching	Packet Switching (Except over the air)	Packet Switching
Speed (data rates)	2.4 Kbps to 14.4 kbps	14.4 Kbps	3.1 Mbps	100 Mbps
Function	Only Audio	Audio and Data Material	Audio and Data Material	Audio and Data Material
Internet functions	None	Narrowband	Broadband	Ultra-broadband
Bandwidth	Analog	25 MHz	25 MHz	100 MHz
Operating Frequency	800 MHz	GSM: 900MHZ, 1800MHz CDMA: 800MHz	2100 MHz	850 MHz, 1800 MHz
Sub-bandwidth	30 KHZ	200 KHz	5 MHz	15 MHz

Table 1: Evolution of mobile communications[1]

In order to realize the potential of 5G, including achieving faster transmission, longer transmission distance, and more connected and simultaneous users, Figure 1 shows that the following key new technologies are required:

- More powerful mobile phones/base station infrastructure planning
- Higher frequency bands/larger bandwidth to increase data transmission
- More efficient communication architecture/protocol to improve spectrum utilization



圖一：頻譜與技術[2]

- Better key materials/components/assembly technology: antennas, wafer manufacturing, wafer materials, circuit boards, oscillators, and shielding materials to reduce millimeter wave (mmWave) high frequency loss and suppress noise

These technologies are currently distributed as follows:

- Countries/regions possessing core technologies: Europe (system and application), United States (system and application), mainland China (application), South Korea (application, component and device), Taiwan (component, device, material and application) and Japan (component and material)
- Long-distance cellular IoT communication protocol: Cat-M1 and NB-IOT
- Base station manufacturers, such as Huawei, Ericsson and Nokia
- Major mobile phone manufacturers, like Apple, Google, Samsung, Huawei, etc.
- Chipset designers including Qualcomm, Broadcom, MediaTek, Samsung, Huawei
- Virtualization technology, such as Red Hat, Inc. and Altiostar

Similar to how 4G has different frequency bands, 5G will utilize the frequency groups: low band, mid band and high band, as shown in Figure 2:

- The low band is being used mainly in the U.S., Korea and Europe.
- The mid band is expected to be used by most countries planning to deploy 5G.

The high band, above 24.25 GHz, requires new components and materials to withstand high frequency stressors. This is currently being built out in the U.S., China, Taiwan and Japan. Many countries have plans to develop in this band in the coming years

5G requires higher bandwidth, better equipment and more intelligent communication technology to meet diverse needs.

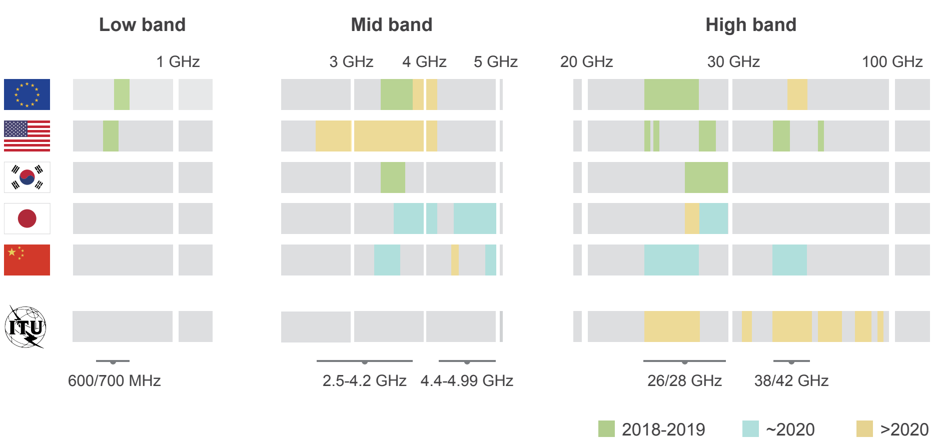
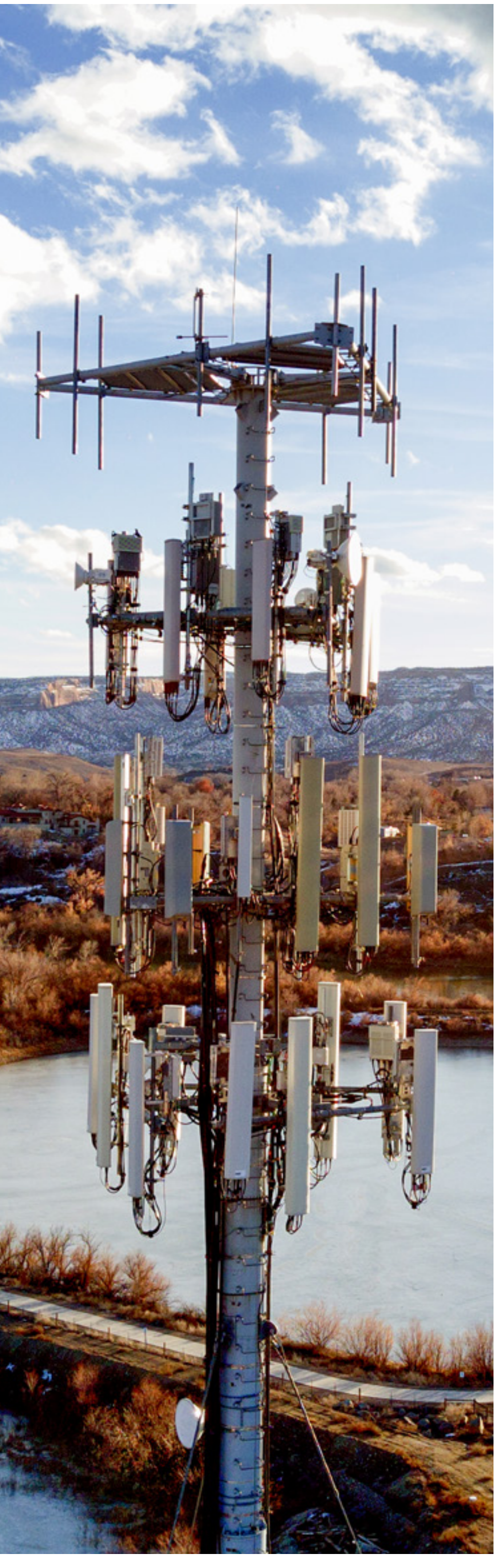


Figure 2: Global 5G frequency band distribution[3]



Three major application scenarios and key technological breakthroughs of 5G

The 3rd Generation Partnership Project (3GPP), which formulated the communication standard, has developed three major capability use cases for 5G technology: enhanced mobile broadband (eMBB), massive machine type communication (mMTC), and ultra-reliable and low latency communication (URLLC).

In order to achieve these three major capability use cases of 5G, we must achieve breakthroughs in three areas of technology: higher-frequency semiconductor technology, denser base station communications, and more efficient network protocols and architectures.

Broadband capabilities depend on high-frequency semiconductor technology.

Broadband capability comes from the higher frequency and higher power of third-generation semiconductor technology. The current working voltage and frequency range of various high-frequency semiconductors are shown in Figure 3. In addition, market development affects availability for low band, mid band and high band.

- Low band and mid band: The oscillation frequency of silicon crystal (less than 9 GHz) can be used, and the technology is mature with low cost.
- High band and high-power area: Newer technology semiconductors such as gallium nitride (GaN) and gallium arsenide (GaAs) must be used. Few global manufacturers exist for such components. The United States and Japan have been leading in these key technologies, while Taiwan has the best capability for mass production.

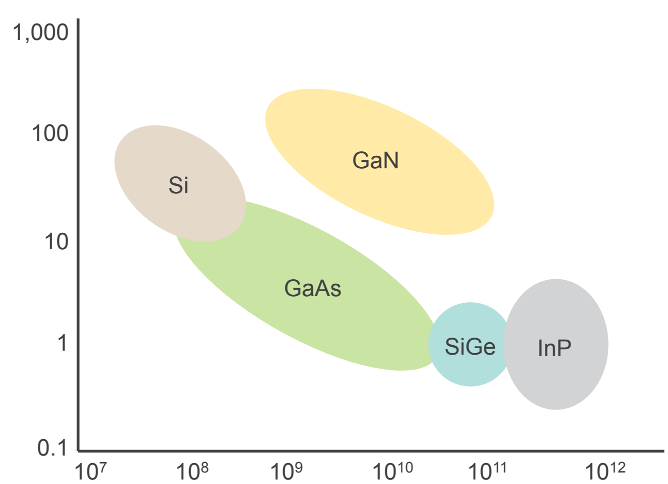


Figure 3: Working frequencies and power of various high-frequency semiconductor technologies[4]

On the other hand, in order to reduce the interference and loss of high-frequency signals, the application of appropriate insulating materials and radio frequency (RF) transparent materials is necessary. The insulating and RF transparent materials used in high band are called millimeter-wave (mmWave) materials because the wavelengths of the tens of GHz and even hundreds of GHz bands have reached the millimeter level. As such, they have higher requirements for insulation and RF transparency. At present, only a few countries such as the United States and Japan possess such technologies. The three major technologies of high-frequency oscillators, wave-transmitting materials and insulating materials, as well as printed circuit boards, have not yet fully matured. Therefore, the unit price for high band is about 10 times higher than that of low band. This limits the development of high band technology. For the mid band range, the challenge in power exists, but no such problem exists in the low band range.

Massive IoT communication and ultra-reliable low-latency rely on smart network architecture.

Massive IoT communication and ultra-reliable low-latency communication must rely on the intelligent network architecture. The reason for this is traditional mobile communication is subject to data supervision and payment management, and most use star topology or mesh topology, as shown in Figure 4.

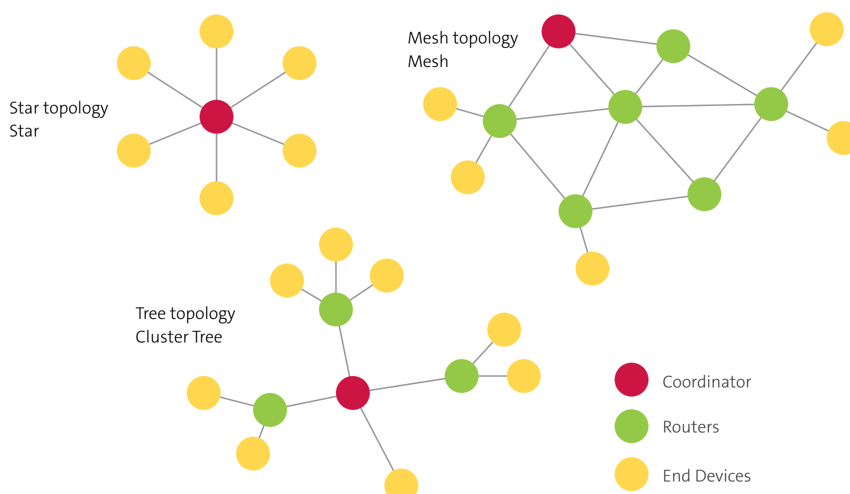


Figure 4: Network topology for mobile communications[5]

In this architecture, the increase of users or data to be transmitted must be achieved by adding node devices. However, all signals must be returned to the base station for exchange. Even the simplest local area network or automated production line must upload data first instead of direct interconnection. This increases the risk of unnecessary and unwanted data flow, slowness and network instability, and investment in the installation site and maintenance. Once the base station is compromised, the communication will be down.

Conversely, if applying the peer-to-peer (P2P) communication protocol and architecture concept, as shown in Figure 4, each device can become a base station that can send, receive and relay. The denser the user area, the higher the transmission rates. However, because it involves dividing, comparing, merging, transmitting, receiving and calculating available resources, a better data processor and special algorithms are needed. The billing, information monitoring and security will also be regulated by national surveillance systems.

Low-Earth orbit communication satellite achieves ultra-long-range low-latency communication.

Ultra-long-range low-latency communication requires the use of increasingly dense low-orbit communication satellite systems (low-Earth orbits (LEOs)). Compared with the existing communication satellites located in the 36,000 km area, those in the orbit of 500 km to 1,200 km are called low-orbit communication satellites. Due to the short communication distance, the delay is about 100 milliseconds, which is closer to the wireless communication delay in the atmosphere, and the launch cost is lower. This helps to reduce the manufacturing cost, but, currently, the communication frequency band at this location needs to use Ku (10.7–14.5 GHz) or Ka (17.3–30 GHz) frequency band to avoid atmospheric interference.

At present, the development of low-orbit satellites is advancing rapidly for American manufacturers. Emerging satellite operators include Space X, OneWeb, Telesat, and technology behemoths such as Amazon, SoftBank, Facebook, and Google. According to the survey, the number of currently commercialized satellites is between1,700–1,800, and it is estimated that it will reach 17,000 in the next 10 years. These satellites will be mainly used for communications. The demand for very-small aperture terminals (VSAT) and ground-receiving equipment have also increased.

In addition to the above technologies, the existing distributed architectures are getting cumbersome in the present network environment. In order to improve the efficiency, simplify management and save space, a new generation of software-defined networks (SDN), network function virtualization (NFV) and edge computing that allow real-time processing and analysis of data near the data aggregation source. It is not required to directly upload data to the cloud or a centralized data processing system. Both are highly anticipated technologies in 5G.

High-frequency and high-power semiconductors, material technology, new telecommunications architecture and LEO satellite communications are key technologies of 5G.

Industries that will benefit from 5G

5G will improve high-quality audio and video for media and entertainment, as well as accelerate construction of industrial automation for IoT and digital finance to power a smart city of the future. The following industries are expected to benefit from 5G technology:

- Automated and smart applications across domains of food, clothing, travel and entertainment, such as unmanned vehicle delivery, smart laundry, smart appliances, smart homes, self-driving cars, drones, etc.
- Industrial automation applications, such as smart robots, unmanned factories, smart grids, digital manufacturing, etc.
- Medical applications, such as remote and digital medical and healthcare empowered by big data analysis and virtual and augmented reality technologies, etc.

Twelve health, safety and security risks to be considered

Most of the smart technologies enabled by 5G focus on high-speed data transmission so less attention has been paid to the development at the application layer. However, designers also need to consider various security vulnerabilities at the application level. Imagine the following possible risk scenarios:

1. Would the harmless low-power and frequency bands increase its electromagnetic power in order to achieve higher speed and efficiency, and coverage, adversely affect living organs, such as disturbing nervous systems and even the brains?
2. Would the increasing electromagnetic power or the additive emission energy from more transmitting devices interfere with the operating signals of the electronic equipment at the transmitting or receiving antennas, leading to incorrect commands and causing danger?
3. Would the data be intercepted during the transmission, leading to the disclosure of sensitive information such as personal data or trade secrets?
4. Would the data transmission or device settings be remotely altered, resulting in unexpected actuations?
5. Would a sudden power outage/interruption/recovery, traffic or electrical overload damage the device itself or peripheral hardware or software affecting how its functional safety system works?
6. Would different communication protocols interfere with each other and lead to wrong commands?
7. Would the electromagnetic waves induce excessive eddy current on metals and cause overheating?
8. Would the telecommunications network equipment that was intended for ordinary office environments or personal use be misused in high reliability applications, harsh industrial environments or hazardous locations?
9. Would skin burn injuries happen if you contact or wear these communication devices containing high temperature chips for a prolonged time? Or corrode various materials of the device due to sweating?
10. Has a proper and comprehensive upward or downward compatibility assessment been performed on the network subject to frequent upgrades?
11. Do the sensors used to enable smart controls, such as temperature, humidity, pressure, infrared, and even image recognition lenses or light sources, remain stable constantly and emit only correct signals in every expected use environment?
12. Could a highly automated process be interrupted manually in case of emergency, e.g., out of control or failure?

Products with such risks that are not tested and mitigated in a laboratory setting can end up in the marketplace and cause injury, loss of consumer confidence and costly recalls. Such incidents have increased as the complexity of technology has evolved. Recent media stories have highlighted technology risks including a robot violating some biometric information privacy laws, self-driving accidents, flight sensor failures, lithium-ion battery fires, etc. Whether it is the privacy compromised by artificial intelligence (AI), algorithm failure, commercial considerations overriding safety, etc., all are safety and security issues arising from losing control of smart technology. To help ensure the market acceptance of any innovative technology, UL recommends that safety and security always come first when considering product development.

Wireless communication IoT security risks are more complicated and harder to evaluate

5G full ecosystem standards

5G will need the support of the entire technology and development ecosystem to achieve the desired connectivity and quality consumers want. Safety standards are required to prevent technology from losing control. With more than 125 years of experience in safety science, UL helps develops standards across the ecosystem from raw materials to the wireless network to the product security requirements for 5G applications.

Based on electric safety and fire safety

Since the era of telecommunications, Underwriters Laboratories has continued to develop various safety standards, such as UL 1950, which has since evolved into IEC 60950-1 and UL 62368, the Standard for Audio/Video, Information and Communication Technology Equipment. It is the safety standard for the new generation of communication products based on hazard-based safety engineering (HBSE) principles. It can be used in personal communication equipment, base stations and equipment in the data centers.

In order to maintain the battery safety of mobile devices Underwriters Laboratories was first to develop the safety standard for lithium cells (UL 1642, the Standard for Lithium Batteries) and assisted in the development of the international standard IEC 62133. For the safety of portable chargers, UL 2056, the Outline of Investigation for Safety of Power Banks, has been established. UL 1973, the Standard for Batteries for Use in Stationary, Vehicle Auxiliary Power and Light Electric Rail (LER) Applications, was developed for small energy storage system. Large-scale computer room or container-level energy storage systems are evaluated for system safety in accordance with UL 9540, the Standard for Energy Storage Systems and Equipment.

For cloud-based data centers, UL uses UL 2755, the Outline of Investigation for Modular Data Centers, to evaluate the electrical safety of modular data centers and uses UL 3223, the Outline of Investigation for Data Center Certification, as the basis for UL Data Center Certification Program.

For product use, environment and electromagnetic interference exert a big impact.

UL also has electromagnetic compatibility testing capabilities at various test severities and fields, including IEC 61000, CISPR, also known as the International Special Committee on Radio Interference. Other universal electromagnetic compatibility testing specifications range from electromagnetic interference (EMI) to anti-electromagnetic interference (EMS, greater than 20 V/m). Tests include standards for the military, automotive industries and industrial IoT environments.

Through long-term accelerated stress testing, UL 746B, the Standard for Polymeric Materials – Long-Term Property Evaluations, can evaluate the long-term heat resistance of polymer materials. ISO 16750 can also be used to perform accelerated stress testing of the secondary system under temperature and humidity cycling impact.

Not only should efficiency and telecommunication quality, be taken into account, but also electrical safety and connectivity safety

Improved performance and more secure connections.

IoT-based appliances and industrial controls require the reliability assessment of hardware and software security controls. UL supports the assessment and testing of IEC 60335 (home appliances), IEC 60730 (controllers), IEC 61508/ UL 991, the Standard for Tests for Safety-Related Controls Employing Solid-State Devices,/UL 1998, the Standard for Software in Programmable Components (software and hardware architecture), UL 1740, the Standard for Robots and Robotic Equipment/ISO 10218 (industrial robot) and ISO 13849 (industrial robot control), so as to help ensure the security control algorithm of the connected smart devices.

To prevent the IoT and the connection from being damaged or invaded, the U.S. federal government announced a national security plan called the Cybersecurity National Action Plan in February 2016, which uses the UL 2900 Series of Standards. This provides network security testing guidelines for connected products and systems to assess software vulnerabilities and weaknesses, reduce the risk of intrusion, dispose of known malware, review security control items and improve public safety awareness. For other countries or regions, UL also provides IEC 62443 series of IoT information security services consistent with UL 2900, the Standard for Software Cybersecurity of Network-Connectable Products, including industrial control systems, medical equipment, automobiles, heating, ventilation and air conditioning (HVAC) and refrigeration equipment, lighting products, smart homes, appliances, alarm systems, fire alarms systems, building automation, smart meters, network equipment, and consumer electronics.

Evaluating the effectiveness of the ecosystem is essential UL can conduct benchmarking performance evaluations to help consumers choose hardware and software that meet their needs from an objective third-party perspective. UL has multiple benchmark suites to evaluate the performance of devices such as laptops, tablets and smartphones, and discover problems concerning setup and stability. Comparing the scores of similar systems is helpful to choose right upgrade for systems and components to help ensure the continuous improvement in performance during the transition of 5G.

UL continuously helps develop standards related to the 5G full ecosystem and collaborates with industry to improve safety and security

UL continuously helps develop standards related to the 5G full ecosystem and collaborates with industry to improve safety and security

When 5G is fully implemented, smarter, fully automated buildings will become possible. The five aspects of energy, maintenance, comfort, efficiency and safety will exert a great influence on users and house values. In February 2019, UL and the Telecommunications Industry Association (TIA) announced that they will jointly help develop and promote smart building standards and formulate various test standards for smart buildings.

UL experts sit on more than 500 international committees and, in many cases, more than 100 regional committees to help develop safety standards. An example of standards that apply to products likely to utilize 5G is the UL 4600, the Standard for the Evaluation of Autonomous Products.UL cooperated with MITRE and ECR on the UL 4600 unmanned device safety standard to establish a safety standard framework for unmanned devices. This innovative method of product safety self-reporting is expected to allow manufacturers to consider product safety issues more carefully and comprehensively. In addition, UL is also actively cooperating with industry, government and academia to help develop innovative product standards, including UL 3300 service robot standards, smart building standards, and UL 8400 AR/VR/MR spatial computing sandards. Future safety standards likely will focus on AI and machine learning, both enabled by 5G technology.

With regard to communication technology, UL has long been involved in the formulation of mmWave related tests, while also actively participating in the development of 3GPP wireless communication testing. UL is also a senior member of such committees as PTCRB and Global Certification Forum (GCF). Preparations have been made for each element of the 5G ecosystem, including function and performance requirements, compliance testing, and telecommunications industry acceptance testing. UL has more than 20 years of experience in mmWave testing services for various applications, including automotive radars, wireless HD and 802.11ad, e-band, P2P, etc..... UL has leveraged this experience to provide testing in the new 5G bands. As of mid-2020, UL offers testing for 5G in the low-and mid-band frequency in the U.S., the U.K., China, South Korea, Japan and Singapore. Testing in the high-band mmWave frequency is available in the U.S. and South Korea. Additional testing locations will continue to open over time.

Using science and technology, UL hopes to collaborate with industry, government, academia and other stakeholders. By doing so, UL will introduce correct, appropriate and proven approaches to safety and security testing, and help with the consensus-based development of safety standards related to products that use 5G. In turn, helping future-focused companies have more opportunities to prove their innovations’ safety in a secure laboratory environment.

More security and safety issues about 5G application

Question: 5G enables smart technologies such as VR, self-driving cars, smart buildings ... What safety concerns must be considered?

Answer: Similar to other high-power wireless solutions, there are a number of concerns to be considered. For example, the interference of strong electromagnetic waves on organisms and the operation of electronic equipment, the biological safety of long-term wearing and low temperature burns or corrosion, the security risks of intercepted or tampered data, the interference of different communication protocols, and the heating of equipment, hardware risks, or system compatibility caused by software and hardware updates, etc., must be considered.

Question: Are there any international standards to follow when considering 5G connected devices?

Answer: You should consider the various standards that affect safety and user experience. These include: performance, communication quality, electrical safety, and interoperability.

To learn more about 5G testing, visit https://www.ul.com/offerings/5g-compliance-testing

Notes: References

1. http://www.zseries.in/telecom%20lab/telecom%20generations/#.XXcIMigzbBU
2. http://www.techplayon.com/wp-content/uploads/2017/05/5g_sptectr.png https://img.technews.tw/wp-content/uploads/2018/07/06163153/5G-Characteristics-of-Different-Bands.png
3. https://www.zdnet.com/article/5g-new-radio-the-technical-background/
4. https://www.eetimes.com/document.asp?doc_id=1276329#
5. https://www.datarespons.com/wp-content/uploads/2015/06/Network-Topologies-1024x684.png

UL.com

Distribution Number (e.g. MMYY)