Microwave Journal
eBook
July 2022

Innovations in 5G FR2 Measurement

SPONSORED BY

ROHDE&SCHWARZ
Make ideas real

Table of Contents

Introduction

Innovations in 5G FR2 Measurement

The adoption of mmWave frequencies to provide the bandwidth for the high data rates envisioned for 5G — "enhanced mobile broadband" or eMBB — unveiled a stream of measurement challenges. They begin with the greater sensitivity of the cable assemblies interconnecting mmWave components and extend to the need for over the air (OTA) measurements where there are no wired connections. To address the challenges making accurate and repeatable measurements, from the semiconductor to the system, this eBook collates several Rohde & Schwarz articles and focuses on the mmWave frequencies in the FR2 (frequency range) bands.

We begin with "5G Evolution — On the Path to 6G," a thorough discussion of 5G and its continuing evolution through 5G-Advanced, with a few conjectures about the next generation (6G). Building on this overview, the article "Mobile Network Testing of 5G NR FR1 and FR2 Networks: Challenges and Solutions" describes an approach for drive testing fielded mobile networks using a passive scanner measuring the synchronization signal/physical broadcast channel blocks from the base station. This technique is usable for 5G base stations operating in either the FR1 or FR2 bands.

Addressing OTA measurements, the application note "Antenna Beam Characterization of 5G Mobile Devices and Base Stations Using the R&SNRPM OTA Power Measurement Solution" covers the theoretical basis for OTA power and pattern measurements, then describes an approach to verify the power level and radiation pattern of an antenna, including the accuracy of the antenna's beam steering. The approach compares measurements of the antenna being tested to a known "golden" standard.

For OTA test scenarios where signal fading must be emulated — such as radio resource management conformance and demodulation — the methodology must include virtual cable calibration (VCC). The article "VirtualCable Calibration for OTA Testing of 5G mmWave Devices" discuss the concept of VCC and how it is used to make 3GPP compliance measurements.

"Choosing The Right Signal Source for Reliable Measurements" is a salient reminder of the adverse effects the signal source can have on measurement accuracy, such as harmonics, compression and phase noise. A key step when setting up a measurement system is estimating the overall measurement uncertainty and the contribution from the signal source. If the latter is too high, a better source may be warranted.

The eBook concludes with an example of a test system for characterizing and testing a Sivers Semiconductors transceiver and antenna module that operate over the 57 to 71 GHz unlicensed band. The RFIC was developed to support the IEEE 802.11ad/ay standard with 64-QAM modulation and is used in various fixed wireless access links. The article outlines a Rohde & Schwarz equipment setup used to drive and test the transmitter and receiver portions of the transceiver, including a compact antenna test range for OTA measurements.

Gary Lerude, Microwave Journal *Editor*

5G EVOLUTION – ON THE PATH TO 6G

Expanding the frontiers of wireless communications

White paper | Version 01.00 | Dr. Nishith D. Tripathi, Dr. Jeffrey H. Reed

ROHDE&SCHWARZ

Make ideas real

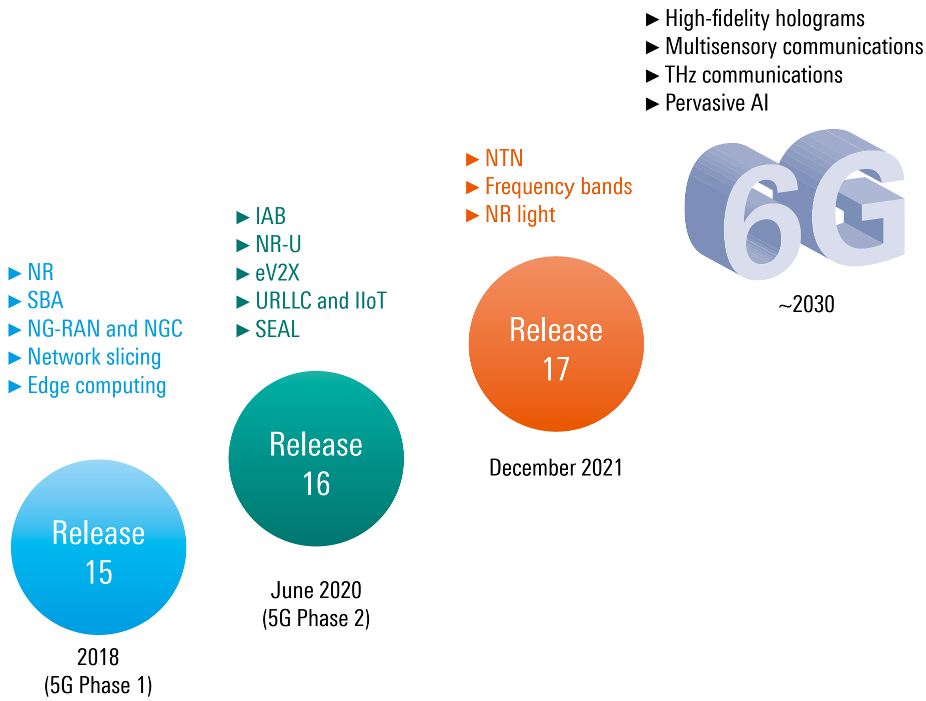
CONTENTS

1 5G PHASE 1 AND EVOLUTION TOWARD 6G

3GPP[1] defined the fifth generation (5G) cellular technology in Release 15 to meet ITU's IMT-2020[2] performance requirements and to enable a variety of services associated with usage scenarios such as enhanced mobile broadband (eMBB), ultra-reliable low latency communications (URLLC) and massive machine type communications (mMTC). Example 5G performance requirements are 20 Gbps peak data rate, 1 ms radio network latency, 10 Mbps/m^2 area throughput and 1 million (low-rate) IoT devices per square kilometer. Key building blocks for 5G are the New Radio (NR) air interface, new radio and core network architectures, virtualization and automation technologies and new types of devices [1]. These building blocks enable 5G to offer targeted 5G services.

While Release 15 provides a solid framework for enhanced network performance and mass offering of amazing services, 3GPP is actively working on further enhancing the framework as shown in Fig. 1.1.

Fig. 1.1: Evolution path from 5G to 6G



- **Release 15.** 3GPP defined 5G Phase 1 in Release 15 (R15). Example features of R15 include the New Radio (NR) air interface, new radio network architecture called next generation radio access network (NG-RAN), new core network architecture called next generation core (NGC) or 5G core (5GC), service based architecture (SBA), network slicing and edge computing.

[1] 3GPP stands for Third Generation Partnership Project. 3GPP has previously defined specifications for third generation Universal Mobile Telecommunication System (UMTS) and fourth generation long term evolution (LTE).

[2] ITU is the International Telecommunication Union. A network is said to be a 5G network if it can meet International Mobile Telecommunications (IMT)-2020 performance requirements.

- **Release 16.** Planned features for Release 16 (R16), also called 5G Phase 2, include NR unlicensed (NR-U), integrated access and backhaul (IAB), enhanced vehicle-to-everything (eV2X), URLLC and industrial IoT (IIoT) enhancements and service enabler architecture layer (SEAL) for verticals.

- **Release 17.** Potential Release 17 (R17) features include non-terrestrial networks (NTN) (i.e. those using satellites), new frequency bands (e.g. 7 GHz to 24 GHz and > 53 GHz), enhancements to NR sidelink and NR light.

- **6G.** 5G Phase 1 deployments have started only recently, and releases beyond R15 will continue to tap into the tremendous potential of 5G. However, since a new generation of cellular technology typically appears every 10 years, 6G can be expected around 2030. 6G could offer high-fidelity holograms, multisensory communications (e.g. touch, taste and/or smell!), terahertz (THz) communications and pervasive artificial intelligence (AI).

Some features may initially be introduced in one release, but defined in an elaborated fashion in a future release. In this white paper, the 3GPP work in R16 and R17 is classified into the following categories: (i) service expansions, (ii) NR enhancements, (iii) network architecture enhancements and (iv) miscellaneous enhancements. Sections 2 to 5 contain an overview of the 3GPP work based on these categories. Our crystal ball view of 6G is given in section 6. Finally, section 7 summarizes the paper's key findings.

Before diving into R16 and beyond, here is a quick look at key features of 5G R15 [1].

- **NR air interface.** Like LTE, NR uses orthogonal frequency division multiplexing but makes it highly flexible. For example, variable subcarrier spacing, flexible radio frame structure including a self-contained slot, and carrier bandwidth parts are introduced. Both sub 7 GHz spectrum (called frequency range 1 or FR1) and millimeterwave spectrum (called frequency range 2 or FR2) are supported. The new high performance channel coding techniques of low density parity check coding and polar coding are defined. Spatial multiplexing techniques used in LTE, SU-MIMO and MU-MIMO[3] are enhanced in 5G. NR is a beamformed air interface with fewer beams at low frequency bands and more beams at high frequency bands. 5G supports hybrid beamforming where both digital beamforming (available in LTE) and analog beamforming are combined. Massive MIMO (mMIMO) in 5G enables enhanced combining of beamforming methods with spatial multiplexing.

- While NR provides a flexible air interface, it is advantageous in transitioning from 4G to 5G to use dynamic spectrum sharing (DSS) to dynamically allocate 4G and 5G subcarriers in the same channel. With DSS, mobile operators can simultaneously support 4G LTE, 5G NSA and 5G SA devices. DSS was introduced in R15, further refined in R16 and R17 and will probably continue to be refined in future releases, especially to improve the scheduling of resources between and within 4G and 5G subcarriers and across multiple cells. While the transition from one wireless generation to another in a specific band has been a painful experience in the past, it will be much easier with 5G thanks to DSS.

3) SU-MIMO and MU-MIMO refer to single user multiple input multiple output and multi-user multiple input multiple output, respectively.

- **NG-RAN, NGC and SBA.** NG-RAN includes NR based 5G base stations called next generation node Bs or gNBs. A gNB can be decomposed or disaggregated into a central unit and a distributed unit. Such a gNB architecture reduces infrastructure and transport costs and provides scalability. While LTE uses a limited number of nodes in the evolved packet core (EPC), 5G defines more network functions (NF) that have fewer responsibilities. The overall 5G system is based on SBA, where NFs communicate with each other using service based interfaces. SBA facilitates the design and deployment of the 5G system using virtualization and automation technologies such as network functions virtualization (NFV), software defined networking (SDN), OpenStack and Orchestration.

- **Deployment options.** R15 fully defines two deployment options for the network architecture: non-standalone (NSA) NR and standalone (SA) NR. Non-standalone NR with the EPC uses the LTE eNB as the master node and makes use of a gNB's additional NR radio resources when possible. Standalone NR with the NGC does not rely on the LTE eNB at all and allows direct communications between the UE and the gNB.

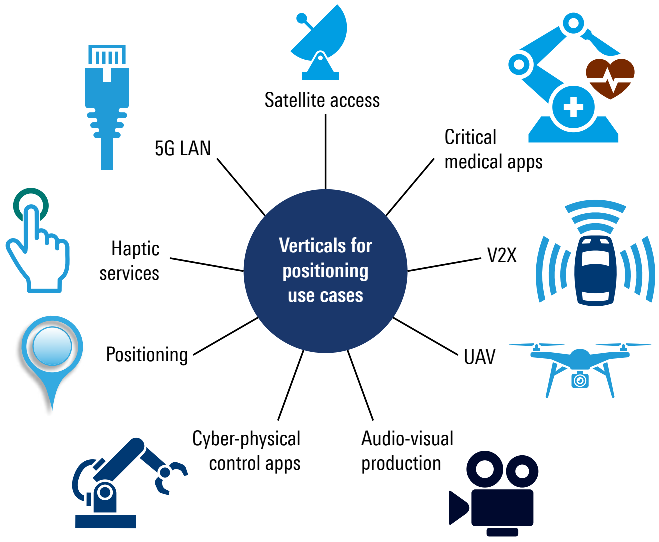
- **Network slicing.** 3GPP introduces the concept of network slicing, where different logical networks are created using the same physical network to cater to different services and different customer requirements for a given service. Three standard slices for eMBB, URLLC and massive IoT are defined with support for numerous operator-defined network slices.

- **Edge computing.** 3GPP supports edge computing where the applications are located close to the UE. More specifically, 3GPP allows the selection of a gateway that is close to the gNB. Since user traffic passes through a local gateway instead of a remote gateway located deep inside the core network, both the end-to-end latency and transport requirements are reduced.

2 SERVICE EXPANSION BEYOND RELEASE 15

Although the work accomplished in R15 is useful for URLLC and mMTC usage scenarios, 3GPP focused more on the eMBB usage scenario in R15. Fig. 2.1 shows how 3GPP expands services beyond eMBB-related services in R16. Since 3GPP focuses on different verticals (i.e. industries), many of these services are related to verticals. Note that these services are not necessarily distinct from each other; there could be overlap among some services. These services are described in sections 2.1 to 2.10.

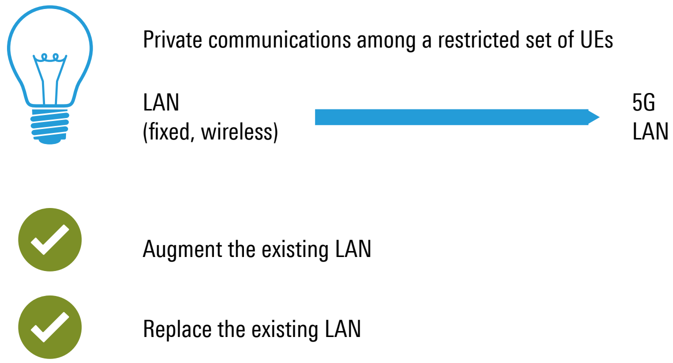
Fig. 2.1: New or enhanced services beyond 5G Phase 1



2.1 5G LAN

Fig. 2.2 shows the key concepts related to 5G local area network (LAN) services [TR 22.821].

Fig. 2.2: 5G LAN



Scope
Residential, enterprise, industrial

Benefits
Performance, long-distance access, mobility, security

Similar to a fixed or wireless LAN, a 5G LAN provides private communications among a restricted set of UEs in a residential, enterprise or industrial setting. A 5G system can either augment or supplement an existing fixed or wireless LAN or completely replace such a LAN. A private virtual network (PVN) can be created using a 5G system. Compared to a traditional LAN, a 5G based PVN offers benefits such as superior performance, long-distance access, mobility support and enhanced security.

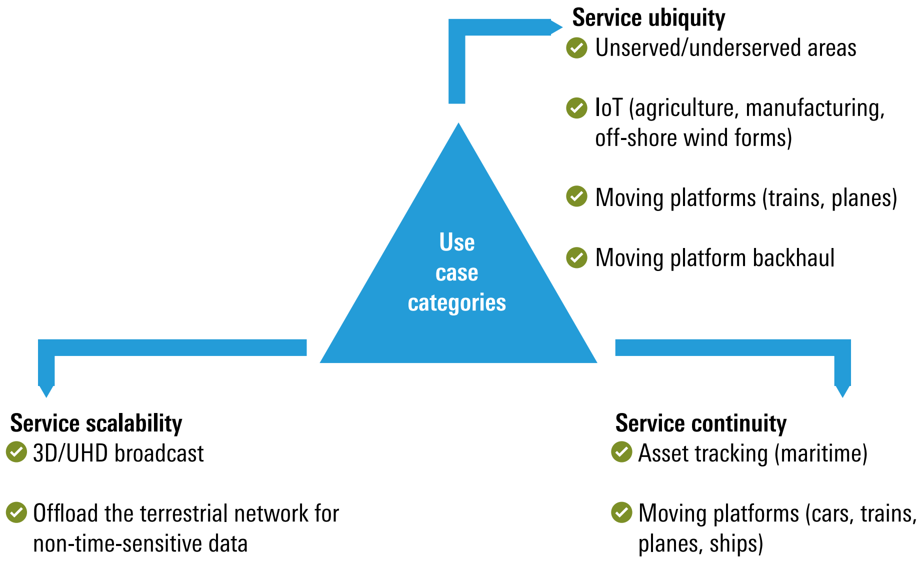
In the residential setting, different devices in a single home or different users in an apartment complex can obtain enhanced 5G QoS and maintain privacy and isolation of communications where needed. In the enterprise setting, 5G LAN helps connect computers, printers, scanners and servers, and facilitates access to private and secure settings across a large area or even across distant sites. In the industrial environment, controllers, actuators and sensors can be connected without the need for wires and with low latency communications. Reliable 5G wireless connectivity eliminates the need for Ethernet cables in a hazardous environment or in moving or rotating parts, and facilitates factory reconfiguration to increase productivity. In the case of IoT devices, two communications endpoints can even span countries, for instance a pipeline sensor in one country and a pipeline valve in another country.

When a network offers private communications services, such a network is referred to as a non-public network (NPN) or simply a private network. Only selected devices that are members of the NPN can obtain the network's services. Devices that are not members of the NPN obtain services from the regular "public" network. Furthermore, the network resources (e.g. radio and core networks) are dedicated to the private entity that controls the NPN. The NPN may be fully independent of the regular public cellular network or may work in conjunction with the regular public cellular network.

2.2 Satellite access

5G aims to support satellite access in addition to terrestrial access. Fig. 2.3 summarizes three main use case categories where a satellite network using 5G can be used.

Fig. 2.3: Satellite access



The three use case categories are service ubiquity, service continuity and service scalability. These categories are not mutually exclusive; a given use case may belong to more than one category.

- **Service ubiquity.** This category corresponds to the scenario where a terrestrial 5G network is not providing coverage but a satellite network is. For example, some rural or hard-to-reach areas may be unserved or underserved by a terrestrial network. Some IoT use cases such as smart agriculture, remote area manufacturing and offshore wind farms may not be economically viable for a terrestrial network but feasible for satellite access. If a terrestrial 5G base station (i.e. gNB) cannot connect to the 5GC using a typical fiber backhaul due to the lack of backhaul facilities, satellite access can come to the rescue. Since a satellite is helping with the implementation of backhaul, such a scenario is called moving platform backhaul.

- **Service continuity.** In some cases, the UE initiates communications with a terrestrial 5G network but moves out of the terrestrial system's coverage area. In such a case, service continuity can be ensured by using satellite access. Example use cases include asset tracking for IoT devices and people embarking on trains, planes and ships.

- **Service scalability.** Since a satellite covers a large geographic area (e.g. an area corresponding to hundreds or even thousands of terrestrial base stations), some broadcast content such as ultra high definition content or three-dimensional content can be efficiently and economically transmitted to many users simultaneously. The transmission of any non-time-sensitive data can also be offloaded from a terrestrial network to a satellite network.

2.3 Critical medical applications

5G can significantly influence healthcare by enhancing preventive care, reducing time-to-treatment and reducing overall costs [TR 22.826].

In one category of critical medical applications, the patient and the medical specialists are collocated. This category can be further classified into "static – local" or "moving – local" depending upon whether the devices or people are moving while the care is being delivered. Since the care delivery for this category occurs inside a facility, indoor communications services are provided in a private 5G network.

In another category of critical medical applications, the patient and the medical specialists are located at different places. This category can be further classified into "static – remote" or "moving – remote" depending upon whether the devices or people are moving while the care is being delivered. Since the care delivery for this category occurs over a large area, communications services are delivered using 5G PLMNs.

- **Private 5G network use cases.** In an operating room (OR), a teleoperation system can be configured where a surgeon uses a console and a robotic system operates on the patient under the surgeon's guidance[4)]. URLLC and MEC are essential when the surgeon is working on a 3D model of the patient's body. The MEC application processes the patient measurements to bridge the robotic system and the surgeon's commands. In another use case of image-guided surgery, real-time video is wirelessly duplicated on multiple monitors. An operator controls the imaging equipment using a video monitor in one part of the OR, and the surgeon observes the video on a separate monitor. In augmented reality assisted surgery, a surgeon uses a head-mounted display (HMD) to perform the surgery. With the help of a MEC application, a combined

4) In some types of robotic surgery, the robotic system can carry out more precise surgery through suitable instrumentation (e.g. within very small areas), and tremors in a surgeon's hand movements can be smoothed out by a suitable multi-access edge computing (MEC) application.

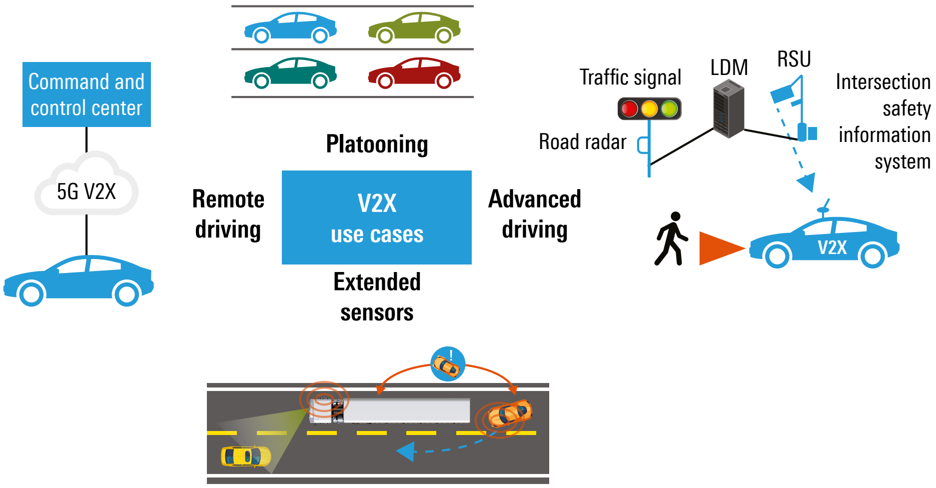
real-time video stream and reference medical image are displayed on the HMD to facilitate surgery.

- **5G PLMN use cases.** Distance is often a critical factor in emergency situations. 5G helps overcome such distance limitations when providing critical care to a patient. In one emergency care use case, an ambulance nurse can carry out an ultrasound examination at the incident location and perform suitable actions (e.g. applying pressure on a specific body part to prevent bleeding or damage) under the guidance of a remote medical specialist. The most suitable medical facility for the patient's situation (e.g. a heart hospital) can be selected. A variety of sensors can be placed on the patient's body and the emergency room (ER) can be prepared even before the patient has been transported to the ER. Remote surgery or telesurgery where a special surgeon does not need to be physically present is also possible, significantly expanding the reach of medical care to remote areas. In another use case, a connected ambulance can transmit important patient data to the ER from the instant the ambulance arrives at the incident scene to the point when the patient is brought to the operating table in an ER that has been prepared to meet the patient's needs. In yet another use case, a patient recently discharged from the hospital has sensors on their body that track vital measurements and keep the appropriate medical facility informed. Prompt medical assistance is provided to the patient if the need arises.

2.4 5G V2X

While LTE can address some vehicle-to-anything (V2X) use cases, 5G V2X significantly expands the types of supportable use cases thanks to the high data rate, ultra-low latency and high reliability of 5G. Note that NR based V2X complements, and is not intended to replace, LTE based V2X. For example, basic safety messages can be sent using LTE based V2X, and scenarios that demand more stringent QoS requirements (e.g. latency, reliability and data rates) can benefit from NR based V2X. V2X, a subcategory of sidelink communications, supports not only vehicles but public safety with UE to UE communications. R17 will address the V2X issues that have been not been resolved in R15 and R16 and introduce study items to further extend the capabilities and applications of NR sidelink communications. R17 is expected to contribute enhancements in power savings, reliability and latency. Fig. 2.4 summarizes the use case groups targeted by 3GPP for 5G V2X [TR 22.886].

Fig. 2.4: 5G V2X use case groups



- **Platooning.** Platooning is operating a group of vehicles in a tightly-coupled manner. Such operation resembles a train with virtual cables between the vehicles. To maintain distance between the vehicles, the vehicles participating in platooning share their status information such as speed, heading and intention (e.g. braking or acceleration). Information about the platoon needs to be shared with vehicles that are not part of the platoon so as not to disturb the platoon. Platooning enhances safety by maintaining a safe distance while reducing the required distance between vehicles. Platooning reduces the overall fuel consumption and results in smoother traffic flow. The number of drivers needed to operate a given number of vehicles can also be reduced.

- **Advanced driving.** Vehicles can share a wide variety of information with each other to enhance safety and avoid or prevent accidents. For example, cooperative collision avoidance involves evaluating the probability of an accident and coordinated maneuvers using safety messages (cooperative awareness message or CAM and decentralized environmental notification message or DENM), sensor data, and commands for braking and accelerating. In the case of emergency trajectory alignment, when a vehicle learns about road obstacles through onboard sensors, it calculates a maneuver to avoid an accident and informs other nearby vehicles. These vehicles can then align their trajectories to cooperatively perform the emergency reaction. Similarly, at an intersection, a local dynamic map (LDM) server can monitor the road using a road radar and a traffic signal, generate LDM information and deliver that information to the vehicle via a roadside unit (RSU).

- **Extended sensors.** A vehicle can share its raw or processed sensor data with other vehicles and RSUs to create situational awareness. Such information sharing enables a vehicle to make tactical or maneuver decisions. For example, sharing of sensor data including high resolution videos can be used to detect objects that are not directly visible to the local sensors (e.g. behind other vehicles, on curves or behind the corners of buildings).

- **Remote driving.** In remote driving, a vehicle is controlled remotely by a human operator or a cloud server. For example, buses are driven on predetermined routes. A human operator can drive the buses with the help of suitable data such as video feeds containing views inside and outside the bus. A vehicle can be remotely driven to a suitable destination such as home or a medical facility if the human driver is unable to drive due to a personal situation (e.g. fatigue) or a health condition.

2.5 UAVs or drones

An unmanned aerial vehicle (UAV) or drone is a low-altitude (e.g. up to few hundred meters) flying vehicle that can be used to provide communications for a short time and/or in a limited geographic area. A UAV typically operates for up to 1 hour [TR 22.829]. After providing communications for a suitable time period, the UAV returns to its base for charging. A UAV may be controlled by a controller in the cloud, and delay-sensitive applications can be supported using multi-access edge computing (MEC). Artificial intelligence (AI) can also be used to control UAVs. Since traditional antennas in a cellular network use downtilting, support for UAVs requires adjusting existing antenna systems or separate antenna systems. Here are example use cases where UAVs can be used.

- **Live video broadcast.** A 360° spherical camera can be mounted on a UAV. This UAV can communicate with a gNB on the ground to send the 4k/8k video to a server in the cloud. People with AR glasses can then enjoy live video broadcast as if they were present at the venue.

- **Temporary radio access with internet connectivity.** In disaster or emergency situations, a UAV can act as a gNB (where it connects to a core network using wireless backhaul) or a relay (where it connects to a ground gNB that provides connectivity to the 5G core) to provide coverage quickly and cost-effectively.

- **Isolated radio access with private connectivity.** In some situations, such as construction in an isolated area, there is no traditional cellular radio access coverage or backhaul. A UAV can provide coverage more quickly and cost-effectively than ground based solutions. The UEs in a private group can communicate with one another via the UAV.

- **Swarm of UAVs for logistics.** A group of UAVs can be used in a coordinated fashion to deliver packages. Medicine and food supplies can be delivered in disaster situations even when the ground infrastructure has been damaged and become unusable.

2.6 Audio-visual production

A 5G network can facilitate audio-visual (AV) production services by providing flexibility, reducing costs and reducing communications setup times. Media could be produced within or outside the premises of a production company. Here are examples of AV production use cases where 3GPP can contribute [TR 22.827].

- **Studio based production.** Media could be produced in a studio using wireless microphones connected to a variety of audio sources, including singers, musical instruments and audio mixers. A 5G system can replace a costly and inflexible fixed infrastructure.

- **Newsgathering.** This use case represents unplanned ad-hoc production such as covering an important event. A 5G system can be set up quickly to produce relevant AV media and supply this media to the central facility for further processing and distribution.

- **Planned outside broadcasts.** An elaborate AV infrastructure with numerous cameras, microphones and mixers can be installed for a planned event (e.g. for elections or sporting events). A 5G system can facilitate media transmission from such event facilities to the central production base. Some media preprocessing could also be carried out locally. Sometimes a large coverage area is needed (e.g. a cycling race) and an airborne 5G NG-RAN can be deployed. Examples of audio production use cases include an onsite live audio presentation (with mixing of the presenter talk and audience questions) and audio streaming (with mixing of a singer's voice and audio streams of instruments, amplification of the mixed signal and distribution of combined audio streams on loudspeakers in the hall). Suitable devices can communicate with a 5G system to facilitate the production and distribution of media.

- **Live immersive media service.** Multiple cameras can be installed at various locations throughout the stadium and on players to create an immersive experience for the local and global audiences. An Olympic event is an example of an event that can be enjoyed through such an immersive experience.

2.7 Cyber-physical control applications

Cyber-physical control applications control the physical processes of cyber-physical systems, which consist of engineered and interacting networks of physical components and computational components. Cyber-physical control applications can be used in verticals such as industrial automation and energy automation. Here are example use cases related to these verticals [TR 22.104] [TR 22.832].

- **Factories of the future.** The manufacturing industry is experiencing the 4th industrial revolution or Industry 4.0, which aims to enhance flexibility, versatility, resource efficiency, cost efficiency, worker support and quality of industrial production and logistics [TR 22.104]. A cyber-physical system is an enabling technology where 5G can be used. 5G can be applied to various aspects of automated factories such as factory automation, process automation, human-machine interfaces (HMI), production IT, logistics and warehousing, and monitoring and maintenance. Factory automation involves robotics and computer-aided manufacturing and is seeing the rising trends of modular and mobile production systems. Process automation involves the automation of processes that control the production and handling of substances such as chemicals, food and beverages. 5G can help establish communications among sensors, actuators and controllers. Various HMI devices such as panels associated with a production line and headsets exploiting AR/VR (e.g. step-by-step support from a remote expert for a specific task) will benefit from 5G connectivity. Logistics and warehousing involve controlling the flow and storage of substances using mechanisms such as automated guided vehicles (AGV) and forklifts. Monitoring and maintenance involve processing suitable sensor data to ensure long-term operation of the factory and to perform predictive maintenance.

- **Electric power distribution.** Smart grid is the emerging power distribution grid where insights are used to manage the distribution of power. In particular, the increasing focus on renewable energy (e.g. solar and wind energy), bidirectional electricity flows, and increasingly dynamic power systems require intelligent management of suitable resources. 5G can help connect a large number of local power generators, such as solar power units and wind turbines, to the smart grid. 5G based communications can facilitate fault detection and automatic restoration of electricity by using suitable measurement and control mechanisms.

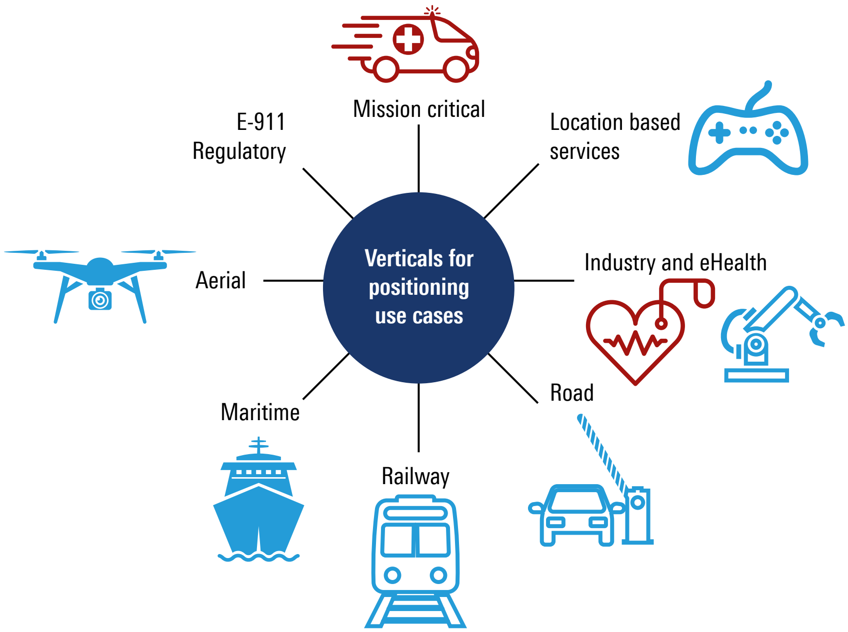
- **Central power generation.** Centralized power generation involves converting chemical energy and other forms of energy into electric power. Large gas turbines, steam turbines, combined-cycle power plants and wind farms help generate electric power outputs of 100 MW or more. 5G can facilitate operations, monitoring and maintenance of such plants.

Time-sensitive networking (TSN) is an essential aspect of cyber-physical systems. Traditional TSN makes use of IEEE 802.3 Ethernet based wired networks to ensure packet transport with bounded delays, latency variations and packet loss. 5G is expected to work with IEEE 802.1 based TSN. Both device-to-device communications and UE-network communications may be used. Since Ethernet based communications is quite common in factories today, 5G-LAN service will play an important role in automated factories.

2.8 Positioning

While 4G LTE and 5G Phase 1 can certainly support location based services, use cases are being expanded significantly in R16 and beyond thanks to increased positioning accuracy. Fig. 2.5 summarizes example verticals that can benefit from positioning use cases [10].

Fig. 2.5: Verticals for positioning use cases



- **Mission critical.** In emergency situations, accurate positioning enables a user to get help from first responders by contacting a public safety answering point (PSAP), even in challenging environments such as urban canyon and deep indoors.

- **Location based services.** AR goggles and head-up displays (HUD) can make use of accurate positioning to superimpose contextual information on the user's real-world view to facilitate navigation, video recording and identification of targets. A shared bike service can benefit from accurate positioning where users can pick up and drop off bikes at suitable locations. Outdoor sports and leisure activities such as motorcycling, skiing and gaming can also make use of accurate positioning.

- **Industry and eHealth.** Accurate positioning is critical in many factory automation applications, including assembly and container management. In a hospital setting, people and medical equipment can be located accurately to facilitate prompt, high-quality care.

- **Road.** In the vehicular setting, 3D positioning facilitates traffic monitoring, management and control for smoother traffic flow to reduce commute times, save fuel and support emergency situations. Road user charging (RUC) levies a charge on a user based on the use of the road infrastructure.

- **Railway and maritime.** Asset tracking in railway and maritime applications increases transportation efficiency, reduces the possibility of lost or stolen containers, and facilitates logistics.

- **Aerial.** UAVs or drones can significantly benefit from accurate positioning for automatic landing as well as for personal or professional missions (e.g. delivery of medical supplies). Images and sensor data (e.g. infrared sensor data) can be merged with positioning data to facilitate UAV operations.

- **E-911 and regulatory.** The UE location supports E-911 calls and helps meet (and even exceed) regulatory requirements for lawful intercept.

3GPP aims to support a variety of positioning techniques in support of the use cases mentioned above [TR 38.305]. The standard positioning methods supported for NG-RAN access include network assisted global navigation satellite system (GNSS) methods, observed time difference of arrival (OTDOA) positioning, enhanced cell ID methods, WLAN positioning, Bluetooth® positioning, terrestrial beacon system (TBS) positioning and sensor based methods (e.g. barometric pressure sensor and motion sensor). Hybrid positioning using multiple positioning methods is also supported. To support these methods, the UE and/or the network measures suitable signals (e.g. GNSS and LTE/NR signals) and estimates the position.

The GNSS based method makes use of UEs with GNSS radio receivers such as global positioning system (GPS) receivers. Different GNSSs such as GPS and Galileo can be used separately or in combination to determine the location of a UE. In the OTDOA positioning method, the UE measures timings of downlink signals received from multiple transmission points (TP) such as LTE/NR base stations. Enhanced cell ID (E-CID) positioning involves the use of the cell ID together with UE measurements and/or NG-RAN measurements. The barometric pressure sensor method uses barometric sensors to determine the vertical component of the position of the UE. In the WLAN positioning method, access point (AP) identifiers, WLAN measurements made by the UE, and databases are used to determine the UE location. The Bluetooth® positioning method involves the use of beacon identifiers and measurements of Bluetooth® beacons. In the TBS positioning method, the UE measures TBS signals. A TBS consists of a network of ground based transmitters that broadcast signals only for positioning purposes. Examples of TBS signals include metropolitan beacon system (MBS) signals and positioning reference signals (PRS). The motion sensor method makes use of various sensors such as accelerometers, gyros and magnetometers to determine the UE displacement.

2.9 Haptic services

Haptic is a sense perceived by touching an object. Haptic includes tactile sensing (touching surfaces) and kinesthetic sensing (sensing movement within the body) [TR 22.987]. Recent advances in haptic feedback devices have been applied to different applications (e.g. haptic feedback from game controllers such as joysticks and steering wheels to simulate the tactile sense and/or kinesthetic sense for a player in a VR game). Because of its low latency, a 5G system could be used to deliver haptic feedback related to vibrations, temperature, texture or electronic stimulus. Examples of haptic senses include vibrotactile sense, shear sense, thermal sense and pneumatic sense.

A haptic service delivers haptic information from one party to another. Such a service could be initiated by the UE or the network and could be delivered asynchronously or synchronously. Here are some examples of haptic services.

- **Haptic emoticon delivery.** This service delivers the haptic information or haptic emoticon for enhanced communications experience by conveying emotions or feelings such as laughter and heartbeat. The haptic emoticon could be conveyed synchronously in real time together with voice and video or asynchronously in an SMS, MMS or IM.

- **Customized alerting.** This service replaces the default or customized alerting tones with a multimodal tone that combines customized haptic alerting with sound, video and other senses. When the calling party tries to establish a call to the called party, customized haptic alerting information along with typical information about the incoming call is sent to the called party's UE. The called party's UE generates suitable customized haptic alerting feedback for the user.

- **Call waiting alerting.** A subscriber may be notified of an incoming call through haptic feedback when engaged in an active call or holding a call. Such haptic feedback could be customized for different callers. The haptic feedback results in a more seamless communications experience by avoiding interruption.

- **Accident or health crisis.** An older adult may fall, triggering an alert to a suitable server and enabling prompt assistance. Even if a person is immobilized, help would be on the way due to automatic handling during the crisis.

2.10 Miscellaneous services

3GPP is evaluating NR based broadcast and multicast services (MBS), extended reality (XR) services, and multi-subscriber identity modules (SIM) as part of the R17 work/study items.

Broadcast and multicast services can significantly improve system efficiency and the user experience. The MBS over a 5G system (5GS) can be applied to use cases such as public safety, mission-critical services, V2X, transparent IPv4/IPv6 multicast delivery, IPTV, software delivery over wireless, group communications and IoT applications. The MBS over the 5GS would be supported for all NR RRC states: RRC_CONNECTED, RRC_INACTIVE and RRC_IDLE. A group scheduling mechanism would allow UEs to receive broadcast/multicast services. And a dynamic change between multicast and unicast would be supported. Mobility with service continuity would also be supported. In the initial implementation, the R15 physical layer would be reused. Any required changes to increase reliability (e.g. via uplink feedback) would also be studied. The resource allocation between unicast and multicast would be flexible.

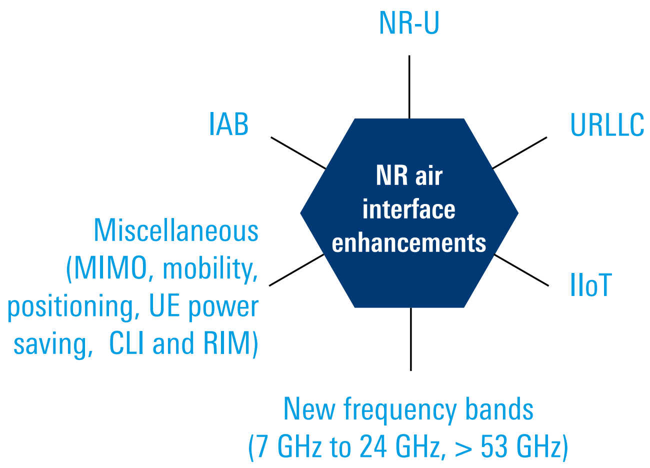
XR is an umbrella term that encompasses augmented reality (AR), virtual reality (VR) and mixed reality (MR). Edge computing is expected to facilitate the realization of XR applications. NR in R15 is designed to be capable of supporting low latency, high reliability communications. In R17, 3GPP will evaluate various aspects of supporting XR, such as power consumption, capacity and mobility.

Since a user could have a personal subscription and a business subscription, a multi-universal subscriber identity module (MUSIM) can be quite beneficial. A USIM may be a physical SIM or an electronic SIM (eSIM). USIMs can belong to the same operator or different operators. Currently, MUSIM is supported in an implementation-specific manner. Standardized MUSIM support leads to enhanced performance due to more predictable UE behavior. For example, standardized MUSIM support reduces paging failures (e.g. a page sent in one network while the UE is in another network) and reduces the probability of missed packets (e.g. the user scheduled but is unable to receive traffic).

3 NR ENHANCEMENTS BEYOND RELEASE 15

3GPP created a high performance, ultra-flexible NR air interface in R15. The NR air interface is expected to serve as a strong foundation for subsequent releases. Fig. 3.1 lists potential NR enhancements[5] in R16 and beyond in support of the various new or enhanced services described in section 2.0. These NR features are explained in sections 3.1 to 3.6.

Fig. 3.1: NR enhancements beyond 5G Phase 1

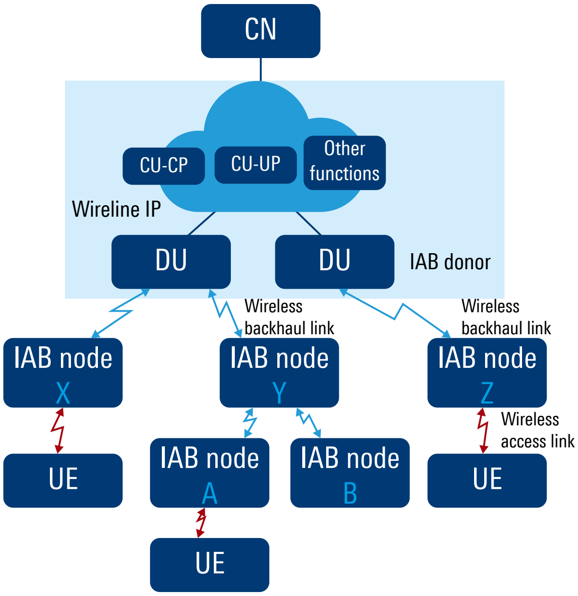


3.1 Integrated access and backhaul (IAB)

Integrated access and backhaul (IAB) means that spectrum can be shared between (i) wireless access to serve UEs and (ii) wireless backhaul to enable base station-core network connectivity. IAB can be used for outdoor small cell deployments, indoors or even mobile relays (e.g. on buses or trains) in the future. IAB can be viewed as a cost-effective deployment solution that simplifies radio-core connectivity and reduces the complexity of the associated fiber based transport network. IAB also reduces the overall time for deployment. Fig. 3.2, adapted from [TR 38.874], illustrates example IAB deployments.

[5] 3GPP extensively studied an adventurous multiple access scheme called non-orthogonal multiple access (NOMA) but decided not to pursue it further. This means OFDMA (and optionally SC-FDMAjF) will continue to be the multiple access scheme of choice for the near-term future.

Fig. 3.2: Integrated access and backhaul



In Fig. 3.2, two base stations, IAB node X and IAB node Z use the spectrum to provide wireless access to their UEs and to communicate with the IAB donor base station that provides connectivity with the core network (CN). The IAB node does not have direct connectivity with the CN, while the IAB donor has CN connectivity. In addition, the IAB donor can provide wireless access to its own UEs. The 5G gNBs can be decomposed or disaggregated into a central unit (CU) and a distributed unit (DU) as specified in R15. IAB also supports a multi-hop link where the IAB node A base station connects to IAB donor through IAB node Y. Network synchronization among base stations is essential for effective IAB deployment. It is also important to effectively manage crosslink interference (CLI) between the access link and the backhaul link.

The IAB node contains a DU and a mobile termination (MT)[6]. The IAB node uses DU to establish RLC channels toward UEs and toward MTs of downstream IAB nodes. The IAB node uses the MT to connect to an upstream IAB node or the IAB donor. The IAB donor contains a CU for its own DU as well as the DUs of all of its IAB nodes and a DU to support its own UEs and MTs of downstream IAB nodes.

Here are the potential characteristics or features of IAB.

- **In-band and out-of-band backhaul.** In-band backhauling implies that the access link and the backhaul link at least partially overlap in frequency. Out-of-band backhauling does not have such frequency overlap. Both sub 6 GHz spectrum and above 6 GHz spectrum are supported.

- **RAT and SA and NSA modes.** While NR based backhaul is the primary focus, LTE based backhaul may be supported. The IAB node may operate in standalone NR mode or non-standalone NR mode.

- **Topology adaptation.** This feature autonomously reconfigures the backhaul network to mitigate the effects of blockage and loading variations. Blockage may occur due to vehicles, foliage or new construction. Loading variations and subsequent node congestion could occur due to traffic variations.

[6] Mobile termination (MT) terminates the radio interface layers of the backhaul Uu interface toward the IAB donor or the IAB node.

3.2 NR unlicensed (NR-U)

LTE based licensed assisted access (LAA) uses licensed spectrum for an anchor carrier frequency and unlicensed spectrum carriers on an opportunistic basis to improve throughput. LAA uses carrier aggregation across licensed spectrum and unlicensed spectrum to transmit data in parallel. Since unlicensed spectrum may have a large amount of unlicensed spectrum available at an instant, LAA tries to make use of such spectrum when interference is below a threshold. R16 reuses the concept of LAA with NR based air interface and supports additional deployment scenarios using unlicensed spectrum [TR 38.889]. Potential deployment scenarios for NR-U are summarized below.

Scenario A: CA between licensed spectrum NR (primary cell or PCell [7]) and unlicensed spectrum NR (secondary cell or SCell). An NR SCell in the unlicensed spectrum may have both DL and UL, or DL only. A gNB serving a small cell can easily implement such CA.

Scenario B: Dual connectivity between licensed spectrum LTE (PCell) and unlicensed spectrum NR (primary SCell or PSCell). Dual connectivity implies two independent schedulers at two base stations, which are an LTE eNB and an NR gNB in this scenario.

Scenario C: Standalone NR in unlicensed spectrum. In this scenario, there is no need for the anchor carrier frequency to be in the licensed spectrum. NR is used solely in the unlicensed spectrum. Such a scenario is like MulteFire, where LTE is used in the unlicensed spectrum with no dependence whatsoever on the licensed spectrum.

Scenario D: DL in unlicensed spectrum and UL in licensed spectrum. An NR based gNB uses unlicensed spectrum for the downlink, but licensed spectrum for the uplink for a given UE. This scenario targets DL-heavy traffic situations such as video streaming.

Scenario E: Dual connectivity between licensed spectrum NR (PCell) and unlicensed spectrum NR (PSCell). In this scenario, one gNB uses licensed spectrum to provide PCell, while the second gNB uses unlicensed spectrum.

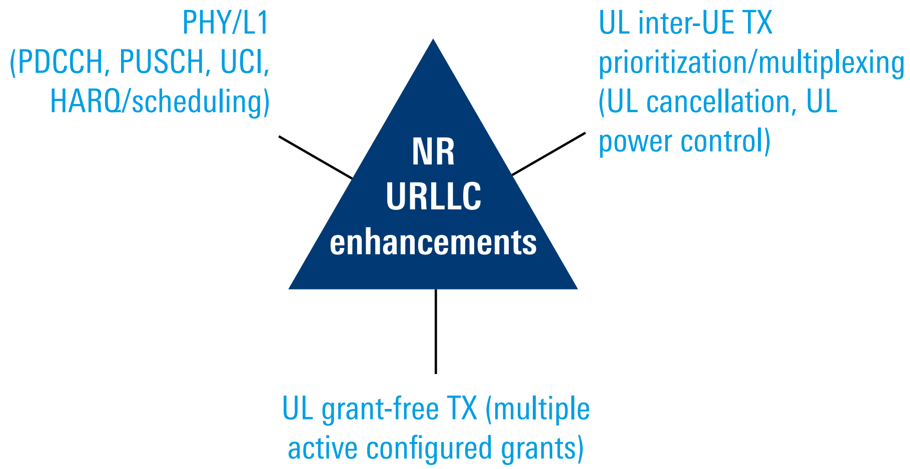
The initial focus of NR-U is on unlicensed spectrum below about 7 GHz, with support for higher frequency unlicensed spectrum expected in future releases. Example frequency bands being targeted for NR-U include the widely used 5 GHz band (e.g. 5.150 GHz to 5.925 GHz) and the new 6 GHz band (e.g. 5.925 GHz to 7.125 GHz in the USA and 5.925 GHz to 6.425 GHz in Europe).

[7] Primary cell or PCell provides an RRC signaling connection (and quite often radio resources for user traffic) to the UE on a specific carrier frequency. Secondary cell or SCell typically provides additional radio resources for user traffic on a separate carrier frequency.

3.3 URLLC enhancements

R15 NR defines the frame structure that can be used as the baseline to support URLLC applications. However, for enhanced AR/VR for the entertainment industry, factory automation, transport industry (e.g. ITS use cases and remote driving use case) and electrical power distribution, additional NR enhancements are needed to increase reliability (e.g. from 10^{-5} to 10^{-6} error rate), to reduce latency (e.g. on the order of 0.5 ms to 1 ms) and to ensure tight synchronization (e.g. on the order of few microseconds). Fig. 3.3 summarizes target enhancements to support more URLLC use cases.

Fig. 3.3: NR enhancements for URLLC



- **PHY/L1 and MAC enhancements.** Enhancements are being targeted for several physical layer aspects such as PDCCH, PUSCH, UCI and HARQ/scheduling. PDDCHs can use compact DCI for faster processing and configurable field sizes. More PDCCHs can be monitored within a slot. PUSCH can be repeated in a slot or in consecutive slots. UCI can support more than one PUCCH for HARQ-ACK transmission, and at least two HARQ-ACK codebooks can be supported to cater to different services for a given UE. Out-of-order HARQ-ACK is supported, where the HARQ-ACK for the second PDSCH can be sent before the HARQ-ACK for the first PDSCH. A second PUSCH can be scheduled before the first PUSCH is over.

- **UL inter-UE transmission prioritization/multiplexing.** Example enhancements include UL cancellation and enhanced UL power control. The UE may be sent an indication about UL cancellation. If transmission has already started, the UE cancels the UL transmission. Otherwise, the UE does not start the transmission. Potential power control enhancements include dynamic power boost for URLLC, enhanced TPC parameters such as larger TPC range and finer granularity of transmit power adjustments.

- **Enhanced UL grant-free transmissions.** R15 supports configured grants to facilitate grant-free transmissions in the uplink. Beyond R15, there can be multiple simultaneously active configured Type 1 and Type 2 grants. A Type 1 grant means that RRC signaling is used for configuration as well as activation and deactivation of the grant. In contrast, a Type 2 grant means that configuration is provided by RRC signaling but activation and deactivation are carried out using PDCCH signaling.

3.4 Industrial IoT (IIoT) enhancements

While industrial IoT would undoubtedly benefit from the URLLC enhancements summarized in section 3.3, industrial IoT has specific requirements that need additional enhancements. For example, wireless Ethernet and time-sensitive networking (TSN) need to be supported. The following are IIoT-specific enhancements being targeted by 3GPP [TR 38.825].

- **PDCP duplication.** R15 supports PDCP duplication for increased reliability. Beyond R15, multiple RLC entities (e.g. up to a limit such as 4) can be configured to allow multiple PDCP copies of data. The actual subset of RLC entities can be controlled dynamically (e.g. using a MAC control element). Since duplication consumes more resources, mechanisms to increase resource utilization efficiency become important when PDCP duplication is active. Selective duplication, selective discarding and activation/deactivation of PDP duplication enhancements are examples of such mechanisms.

- **Intra-UE prioritization.** To cater to higher priority IIoT traffic, suitable prioritization methods can be helpful. Examples include higher priority for a later dynamic grant compared to an earlier dynamic grant, higher priority for a configured grant compared to a dynamic grant, and resolution of the transmission conflict between the scheduling request for higher priority traffic and lower priority user traffic.

- **TSN reference timing.** To facilitate precise timing synchronization, reference times can be delivered from the gNB to the UE using broadcast and/or unicast RRC signaling. The goal for the timing granularity is at least 50 ns.

- **Scheduling.** To facilitate QoS-aware scheduling of TSN traffic, information about TSN traffic patterns such as message periodicity, message size, DL message arrival time at gNB and UL message arrival at the UE could be provisioned from the core network to the RAN. Multiple simultaneously active configured grants (CG) and semi-persistent scheduling (SPS) configurations for a given BWP of a UE would be supported. Additionally, support for shorter SPS periodicities than the existing ones would further reduce latency.

- **Wireless Ethernet.** Ethernet header compression would be supported to reduce overhead.

3.5 New frequency bands

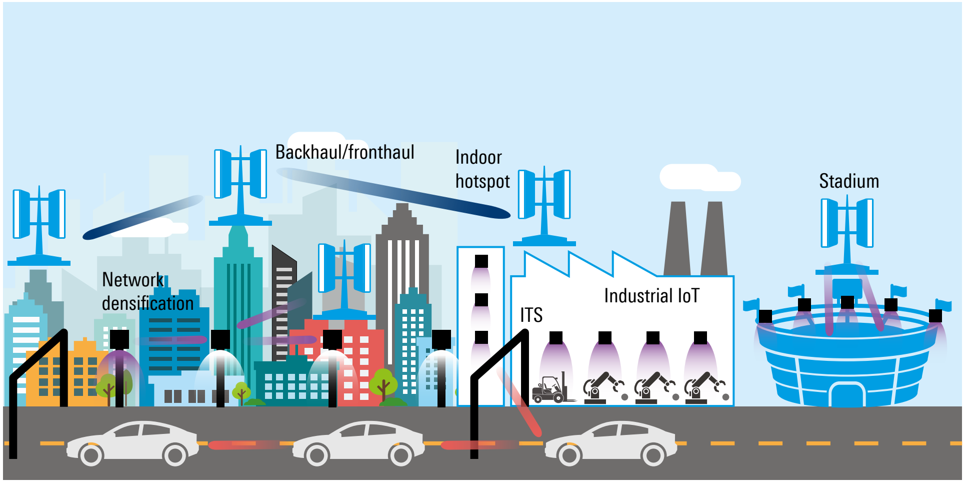
In R15, 3GPP initially defined FR1 to cover 450 MHz to 6 GHz and FR2 to cover 24.250 GHz to 52.6 GHz. FR1 was later extended in R15 to cover 410 MHz to 7.125 GHz to include the 6 GHz unlicensed spectrum in the higher frequencies and any available spectrum around 400 MHz (e.g. T-GSM 410 or GSM trunking system from about 410 MHz to about 430 MHz). 3GPP is exploring further frequency band increases in the 7.125 GHz to 24.250 GHz range and above 52.6 GHz. The 7.125 GHz to 24.250 GHz frequency range may be divided into multiple frequency bands such as 7.125 GHz to about 10-13 GHz, 10-13 GHz to 16-18 GHz, and 16-18 GHz to 24.250 GHz. The existing FR1/FR2 may be extended or new FRs may be defined. In higher frequencies such as 52.6 GHz to 71 GHz, new OFDM numerologies may be defined.

Higher frequencies such as those greater than 52.6 GHz are characterized by the challenges of higher propagation path loss, higher phase noise, larger insertion losses in the RF frontend, more low noise amplifier (LNA) noise, more analog-to-digital converter (ADC) noise, and lower power amplifier efficiency compared to lower frequencies[8].

[8] 3GPP is studying several waveforms that are different than the currently used OFDM waveforms. These new waveforms may be better suited for higher frequencies.

However, these higher frequencies offer the benefit of large channel bandwidths and subsequently high throughput, low latency and high capacity. Fig. 3.4 depicts example use cases that could be supported using the spectrum above 52.6 GHz.

Fig. 3.4: Example use cases for the spectrum above 52.6 GHz



Network densification. With the ultra high definition displays, AR/VR apps and mobile 3D projects, data traffic demand is expected to soar even further. Network densification is an effective mechanism to meet the ever-increasing data traffic demand. Higher frequency bands are suitable for the small cell deployments needed for network densification.

Backhaul and fronthaul. The availability of large bandwidth at higher frequencies makes these frequencies suitable for wireless backhaul. Decomposition or disaggregation of the gNB requires two logical parts of the gNB to communicate with each other. In one possible scenario, baseband and RF portions can communicate with each other using wireless fronthaul.

Indoor hotspots and stadiums. Heavy indoor or outdoor data traffic demand can be met by deploying large bandwidth, high frequency hotspots. And higher frequency reuse is possible due to small cells.

ITS. Vehicle-to-vehicle and vehicle-to-infrastructure communications in an intelligent transport system (ITS) is typically carried out over short distances. Large bandwidths enable wireless transfer of high definition videos and sensor data between the vehicles and of high definition maps from the infrastructure to the vehicles.

Industrial IoT. Factory automation can benefit from private 5G networks using high frequency spectrum in a local area with significant frequency reuse thanks to small cells. Larger subcarrier spacing can reduce latency, and wider channel bandwidths can achieve high data rates and high reliability.

3.6 Miscellaneous NR enhancements

- **UE power saving.** The UE battery life is an essential aspect of the user's overall service experience. Several mechanisms can be employed to reduce the UE's battery consumption in connected mode and non-connected mode [TR 38.840]. For example, monitoring of control channels such as PDCCHs, RRM measurements, suitable transitions between the connected mode and power-efficient mode, adaptation of MIMO layers, BWP switching, efficient paging, cross-slot scheduling and flexible DRX cycles can be used to influence the UE's power consumption. The UE may provide assistance information such as mobility history and power preferences, which can be used by the network to minimize power consumption while avoiding a significant adverse impact on the service performance (e.g. latency).

- **MIMO enhancements.** R15 provides benefits such as enhanced codebooks, reference signal design flexibility and support for advanced antenna techniques for both sub 6 GHz and above 6 GHz deployments. Beyond R15, MIMO can be further enhanced to increase robustness, reduce overhead and/or reduce latency. For example, MU-MIMO can be enhanced by supporting more than two layers in CSI Type II feedback, reducing PAPR for reference signals, control signaling for non-coherent joint transmission, more antenna panels, enhanced beam failure recovery and enhanced DL/UL beam selection [24].

- **Mobility enhancements.** R15 uses LTE-like handover, where the network controls mobility based on measurements provided by the UE. However, meeting the 0 ms interruption time target can be a challenge in the current break-before-make approach when there is a change in the gNB or secondary cell group (SCG). In particular, the beamformed NR interface introduces complexities. Example mobility enhancements include random access channel (RACH)-less handover, fast handover failure recovery, and handover or secondary cell group (SCG) change with simultaneous connectivity with source cell and target cell. Various R15-supported scenarios such as intra-frequency handover, inter-frequency handover, inter-CU handover, intra-CU/inter-DU handover and intra-DU handover would be supported in conjunction with mobility enhancements.

- **NR positioning.** NR based positioning techniques aim to achieve < 3 m accuracy in horizontal and vertical positioning for indoor deployments and < 10 m accuracy in horizontal positioning and < 3 m accuracy in vertical positioning for outdoor deployments [TR 38.855]. New positioning reference signals would be used. Example positioning techniques include DL time difference of arrival (DL-TDOA), DL angle of departure (DL-AoD), UL time difference of arrival (UL-TDOA), UL angle of arrival (UL-AoA), round trip time (RTT) and enhanced cell identity (E-CID). The UE and the gNB make measurements in support of these techniques. The UE observes reference signals from serving and neighboring gNBs and makes DL measurements such as reference signal time difference (RSTD), reference signal received power (RSRP) and UE RX-TX time difference. In the radio network, the following measurements are made at serving and neighboring gNBs: relative time of arrival (RTOA), angle of arrival (AoA) (including azimuth and zenith angles), RSRP and gNB RX-TX time difference.

- **CLI and RIM.** In a TDD system, when two gNBs use the same slot format on a given carrier frequency, co-channel interference and adjacent channel interference are minimized. However, if dynamic TDD is implemented and if gNBs independently choose their slot formats, co-channel crosslink interference (CLI) occurs. 3GPP's work includes the definition of reference signals and measurements to quantify CLI, investigation of CLI mitigation mechanisms and identification of coexistence requirements [TR 38.828]. Another interference of interest is remote interference, where a remote gNB signal from a macro cell undergoes tropospheric bending and causes interference at another macro gNB. 3GPP is exploring remote interference management (RIM) mechanisms (e.g. a reference signal to facilitate detection of remote interference and adjustment of the guard period) to mitigate such remote interference.

- **NR light.** NR light aims to reduce the complexity and the cost of certain types of devices relative to typical R15 based devices. Smartphones and URLLC based devices are high-end devices with stringent data rate, latency and/or reliability performance requirements. Many IoT devices are low-end devices (e.g. smart water meters and smart sensors) with relaxed latency and data rate requirements. However, devices such as smart wearables are somewhere between these two extremes; they have mid-range cost and performance requirements. NR light aims to reduce the complexity of such mid-range devices.

- **NR coverage enhancement.** Coverage influences service quality and expenditures such as CAPEX and OPEX. Since NR is often intended for frequencies higher than those typically used for LTE, this study item aims to carry out an evaluation of NR coverage performance. Both FR1 and FR2 would be considered. And potential coverage enhancement solutions would be studied, with voice over internet protocol (VoIP) and eMBB as target services. Example coverage enhancements include time domain solutions, frequency domain solutions and demodulation reference signal (DM-RS) enhancements (including DM-RS-less transmissions).

- **NR small data transmissions.** UEs with infrequent periodic or aperiodic traffic may be kept in the RRC_INACTIVE state. 3GPP is working on support for small data transmissions in the RRC_INACTIVE state. Such support eliminates transitions between RRC_CONNECTED and RRC_INACTIVE states, saving power, reducing the amount of signaling and increasing network performance and efficiency. Examples of applications that can benefit from this feature include smartphone applications (e.g. instant messaging, push notifications, and keep-alive traffic from applications such as email) and non-smartphone applications (e.g. wearable device traffic involving positioning, sensor data and smart meter traffic). This feature benefits from several building blocks defined in R15 and R16, such as 2-step RACH, 4-step RACH and configured grant type 1. Small data transmissions may accompany certain messages during the RACH procedure. More flexible payload sizes may be defined.

- **NR QoE management and optimizations.** NR is designed to be flexible so that services with diverse performance requirements can be supported. R17 would study quality of experience (QoE) aspects such as the collection of suitable experience parameters and adaptive QoE management schemes to enable intelligent network optimization to meet user experience requirements for diverse services. For example, NR RAN may need to collect user key performance indicators (KPI) such as an end-to-end reliability statistic indicator. QoE parameters can be UE-specific and service-related and more elaborate than traditional metrics such as throughput, capacity and coverage. QoE metrics can be used to evaluate the network quality, and solutions could be evaluated from the user experience and service experience perspectives. A generic framework for triggering, configuring and reporting QoE measurements would be defined. The potential impact of QoE management on network interfaces would be studied.

4 5G NETWORK ARCHITECTURE ENHANCEMENTS

While the network architecture defined in R15 is quite flexible, 3GPP is making enhancements to expand the utility of the network. Below are some examples of network enhancements related to V2X, network automation, Common API Framework (CAPIF) and IP Multimedia Subsystem (IMS).

- **V2X enhancements.** The 5G system (5GS) is undergoing several enhancements to support NR based V2X. For example, NR based PC5 and Uu interfaces are supported [TS23.287]. The UE provides V2X capabilities to the 5GC and receives V2X configuration parameters (e.g. destination Layer 2 IDs for device-to-device communications) over the N1 interface. The policy control function (PCF) provides V2X policy parameters to the UE. A V2X application server exchanges unicast V2X data with the UE in the downlink and the uplink. The unified data repository (UDR) stores V2X service parameters, while unified data management (UDM) manages V2X subscriptions.

- **Network automation.** A step toward network automation was taken when the network data analytics function (NWDAF) was defined in R15. 3GPP is working on enhanced network automation by enhancing NWDAF interactions with other network functions (NF) and with operations, administration and management (OAM) [15]. In particular, NFs and OAM provide raw data to NWDAF, and NWDAF calculates network analytics. These analytics can be used by NFs and OAM to modify parameters that influence network operations (e.g. load balancing via cell selection and handover parameters). While NWDAF would typically be a centralized entity, its local instance may exist in a given geographic area in support of edge computing. Furthermore, NFs may also calculate network analytics and convey those to NWDAF. Artificial intelligence (AI) techniques can be applied to NWDAF or any suitable NF. 3GPP would continue to define NWDAF inputs and outputs for various functions. AI techniques would be implementation-specific with suitable measurement support from 3GPP NFs.

- **Enhanced CAPIF (eCAPIF).** R15 defines CAPIF to enable third parties to interface with the 3GPP network (e.g. LTE or 5G) in support of various applications, including edge applications. 3GPP is enhancing the original CAPIF by adding features such as support for multiple API providers, charging requirements, multiple deployment models and for both EPS and 5GS network exposure.

- **IMS.** 3GPP is enhancing the IMS network so that 5G capabilities such as network slicing can be exploited [16]. IMS modifications to the interface with the SBA of the 5GC are being investigated. Any IMS changes to support local traffic and associated service continuity are being studied. Support for URLLC such as a local instance of IMS as opposed to typical centralized IMS is also being explored.

- **Edge computing.** In R15, 3GPP defined support for edge computing where a UPF close to the UE could be selected for user traffic to derive benefits such as reduced end-to-end latency and reduced transport bandwidth requirements. 3GPP is exploring an architecture to enhance edge computing for a 3GPP network [14]. In this architecture, the UE has an edge application client and an edge enabler client. The edge data network, which would be close to the UE, has an edge application server and an edge enabler server. The core network also has an edge data network configuration server. The edge enabler server is responsible for the provisioning of configuration information to enable the exchange of application data traffic between the edge application client and the edge application server. The edge enabler server also conveys information about the edge application servers (e.g. availability of servers) to the edge enabler client. An edge data network configuration server provisions the edge data network configuration information in the edge enabler client. Such information includes service area information and information needed to establish a connection with an edge enabler server (e.g. uniform resource identifier). Deployment of edge computing apps requires communication between the 3GPP management system (e.g. OAM) and non-3GPP management systems such as ETSI multi-access edge computing (MEC) and ETSI NFV management and orchestration (MANO).

- **RAN slicing enhancements.** 3GPP defined network slicing in R15 to meet diverse customer requirements and widely different QoS requirements in a variety of verticals and industries. 3GPP is studying enhancements to RAN slicing in R17 so that network operators have more control of RAN resources to meet different customer requirements by customizing RAN design, deployment and operation. Network operators can benefit directly from the business success of their customers through customization rather than merely supporting over-the-top business practices. Generic slice template parameters may be studied. Mechanisms such as slice based cell reselection, sliced based random access, and slice based service continuity (e.g. slice remapping due to handover, fallback and data forwarding) may be considered.

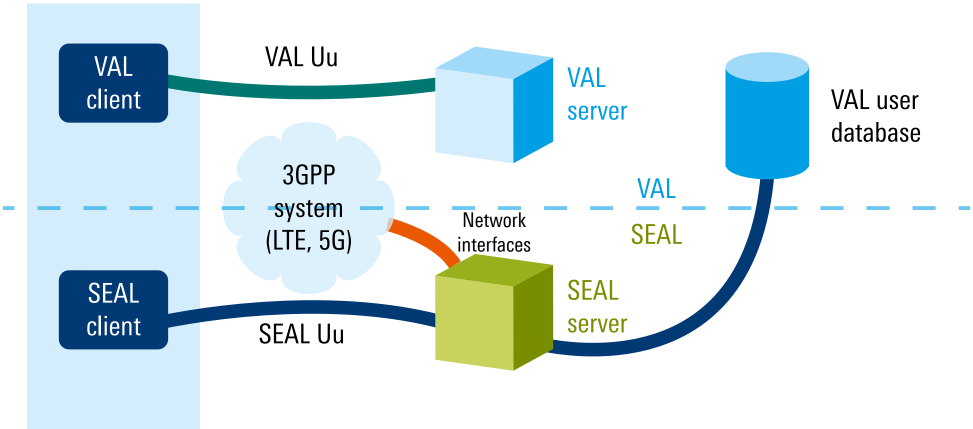
5 MISCELLANEOUS ENHANCEMENTS

This section looks at auxiliary enhancements such as SEAL, SON and security.

5.1 SEAL

The service enabler architecture layer for verticals (SEAL) defines an application-level functional architecture to support a variety of verticals, including V2X and mission-critical services [13]. SEAL provides services such as group management, configuration management, location management, identity management, key management and network resource management. SEAL defines functional models for both application layer support aspects for verticals and the signaling control plane[9]. For the application layer support, there are two functional models: on-network and off-network. The on-network model means that the UE is connected to the radio network via the Uu interface, and, the off-network model is applicable when a UE is using the PC5 interface. Fig. 5.1 illustrates the on-network model.

Fig. 5.1: SEAL on-network model for application layer support



The UE has one or more vertical application layer (VAL) clients and one or more SEAL clients. Within the UE, VAL and SEAL clients use SEAL-C to communicate with each other. SEAL offers its services, such as group management and configuration management, to VAL. The UE communicates with VAL and SEAL servers using an LTE based or 5G based VAL Uu and SEAL Uu. The VAL Uu interface supports unicast and multicast delivery modes. VAL and SEAL servers communicate using SEAL-S. It is also possible for two SEAL servers to communicate with each other using SEAL-X. The SEAL server uses VAL-UDB with the VAL user database (which could be part of the home subscriber server) to store and retrieve user profiles. VAL clients and VAL servers are application-specific for a given vertical, while SEAL provides a common framework to multiple VAL applications.

In the off-network mode, VAL clients on two UEs use VAL-PC5 to communicate with each other, and SEAL clients on two UEs use SEAL-PC5 to communicate with each other. In this mode, one UE can act as a UE-to-network relay to enable suitable UEs to access VAL servers over VAL Uu.

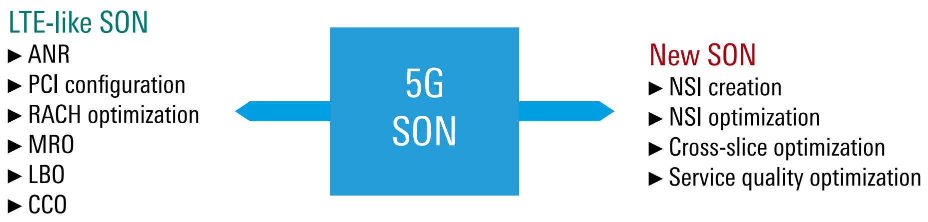
VAL and SEAL services may be provided by PLMN operators or third parties.

[9] The signaling control plane involves the exchange of session initiation protocol (SIP) signaling between the UE and the SIP core. The SIP core could be IMS based or non IMS based. Such SIP signaling helps with SIP session management, subscriptions and authentication.

5.2 5G SON

A self-organizing network (SON) was defined earlier for LTE. SON includes self-configuration, self-optimization and self-healing. In addition, a given SON algorithm's deployment could be centralized, distributed or hybrid (i.e. a combination of centralized and distributed). A SON process is an open loop process when some human intervention exists. In the closed loop SON process, there is no human involvement (there can be exceptions). Fig. 5.2 shows examples of SON algorithms and use cases in 5G. 5G SON algorithms can be categorized as LTE-like algorithms and new 5G algorithms [17].

Fig. 5.2: 5G SON



- **LTE-like SON algorithms.** Since LTE and 5G share several similarities, many SON algorithms defined for LTE can be applied to 5G. Examples of LTE-like algorithms that can be extended to 5G include automatic neighbor relation (ANR), physical cell identifier (PCI) configuration, random access channel (RACH) optimization, mobility robustness optimization (MRO), load balancing optimization (LBO) and capacity and coverage optimization (CCO). ANR enables the automatic creation of a neighbor list for a given cell to facilitate handover decision-making and UE measurement configuration. PCI configuration aims to address PCI related issues such as PCI collision (two neighbors with the same PCI) and PCI confusion (a cell with two neighbors using the same PCI). RACH optimization, as the name suggests, optimizes RACH parameters to improve the accessibility performance for RACH. MRO adjusts handover parameters to address issues such as early handover, late handover and handover to an incorrect cell. LBO redistributes users among cells by adjusting cell selection and handover parameters. CCO observes capacity and coverage metrics and adjusts the network configuration and operational parameters to enhance capacity and coverage.

- **New SON algorithms.** Network slicing is a new concept defined in 5G, so several SON algorithms related to network slicing are new algorithms in 5G. Examples of new 5G SON algorithms include automatic network slice instance (NSI) creation, NSI resource allocation optimization, cross-slice network resource optimization and service quality optimization. Automatic NSI creation enables the network operator to create a set of NSIs on demand based on customer requirements, which involves instantiation and configuration of NFs and connectivity among the NFs. NSI resource allocation optimization observes NSI performance data such as the number of registered UEs and protocol data unit (PDU) sessions and QoS measures to identify traffic patterns, predict the demand for network resources and optimize the allocation of network resources. Cross-slice network resource optimization aims to optimize the allocation of virtual and physical resources for NG-RAN and NGC across NSIs. Service quality optimization involves observing performance data for a given service (e.g. average latency for URLLC) and adjusting relevant configuration and operational parameters in the NG-RAN and NGC NFs.

R17 would address any unresolved SON features from R16. To support SON and minimization of drive tests (MDT), data collection mechanisms would be enhanced. For example, UE reporting to enhance network configuration and support new use cases (e.g. 2-step RACH optimization) may be specified. Both logged MDT (i.e. a UE report sent much later than the time of measurements) and immediate MDT (i.e. a UE report sent soon after UE measurements) would be enhanced. MDT for multi-radio access technology dual connectivity (MR-DC) (i.e. UE simultaneously connected to two RATs such as NR and LTE) would be specified. Any new Layer 2 (L2) measurements, if required, may be introduced.

5.3 Security enhancements

In developing 5G, security has been a top concern from the start. R15 set the security framework [25], and R16 has followed up with many details, addressing many identified weaknesses in the framework. Security for 5G is particularly challenging because it is highly complex and extremely adaptable to support a wide variety of services that have conflicting requirements [26]. For instance, for URLLC applications low latency is of ultimate performance concern, yet it takes processing time to provide robust authentication and encryption. This means security must be optimized and appropriate for the specific 5G application. Optimization of the 5G system performance requires optimizing across various layers of the system, which means security must also be optimized across all the layers. Security must be designed as a chain; it is only as good as its weakest link and therefore 5G security design should aim for end-to-end assurance of security. This is particularly challenging since a 5G system may consist of equipment, software, transport links, services and systems from various entities.

Within 5G R16, numerous issues are being addressed, including:

- Security mechanism to prevent access to other network slices
- Trusted non-3GPP access
- Authentication of the user with security credentials
- Security for small data mode
- User plane DoS attacks
- Broadcast/multicast security
- Lawful intercept
- Battery sensitive security
- Location services security
- Edge device security
- Session management security
- Base station security test cases
- Security against false base stations
- Mission-critical architecture security

In addition, R16 has numerous ongoing studies that, if not integrated into R16, may be incorporated into future releases. These studies include:

- Relay security
- Security and connectivity from 5G to local area networks (may be studied in R17)
- Voice continuity
- Convergence of wireless and wireline systems
- Enhanced URLLC security
- Restrictions on local operators
- Enhanced virtualization security

One of the more attractive features of 5G is the ability to customize security and authentication with network slicing. But this feature does open up a number of different attack surfaces with SDN and NFV. Many vulnerabilities will still need to be addressed in future releases. Potential security vulnerabilities of 5G at various security layers have been identified in [28]. There is no doubt that security issues will continue to be addressed with each 3GPP release.

6 6G: A CRYSTAL BALL PERSPECTIVE

"Prediction is very difficult, especially if it's about the future." Niels Bohr, Nobel Laureate in Physics

"The best qualification of a prophet is to have a good memory." Marquis of Halifax

If LTE stands for long term evolution, 5G is longer term evolution. However, it is a good idea to explore what the future may hold for 6G.

6.1 Predicting the 6G future

Predicting the future can be a futile task, but we all do it – we must in order to get ready for the future. Predicting the next generation of wireless technology is a favorite pastime for wireless engineers. Perhaps it is easier to do for the wireless field than for most fields since it is possible to look at the activities of standards bodies to gain insight into what vendors and service providers are trying to accomplish (and what they need to fix from the last standard). Even before the technology is debated in standards bodies, researchers are developing new ideas that can clearly provide improvements in performance over current systems.

History has taught us lessons that come from observing standards over the past five generations. For example,

1. Not all features spelled out in a given release of the standard are implemented immediately or simultaneously; rather, it could take some time for features to become practical. Likely this will be even more true for 5G given the unprecedented enormous scope of 5G technologies.

2. Weaknesses in the current standard become technology drivers for the next generation standard. This process has been especially true with privacy and security weaknesses.

3. We may be able to predict technology trends, but we are less successful in predicting business models that leverage those technology developments.

4. Sometimes new technologies may work great in simulations or prototypes used to create the standard. However, scaling from the lab models to commercial production and deployment does not always work so well and may take much longer than expected. Antenna arrays are a prime example.

5. New generations of wireless cellular standards tend to come in approximately 10-year increments. For example, LTE deployments started around 2008 and 5G was standardized in 2018.

6. The scope of the problems that wireless addresses increases with each generation. For example, 1st generation started with voice, 2nd generation enabled rudimentary connections to machines such as vending machines, 3rd generation enabled high-speed internet access including enhanced web browsing, and 4th generation made video entertainment over wireless practical. A greatly expanding application scope of 5th generation standards is widely anticipated.

7. New technologies adopted in standards may have much more impact than expected because of the development of synergistic technologies that together create a much more powerful effect. The development of high rate data transmission along with the improvement of display technology drove data demand even higher because it enabled mobile video entertainment.

8. In general, it takes longer to roll out all the capabilities of a standard than the initial hype might imply, but in the end the standard exceeds overall expectations.

These have been fairly consistent trends across all five generations of standards. What is new for the 6th generation of standards is that nations now recognize the importance of wireless standards for national economic well-being and national security. As a result, creating the fundamental technologies behind 6G has become much more competitive [29].

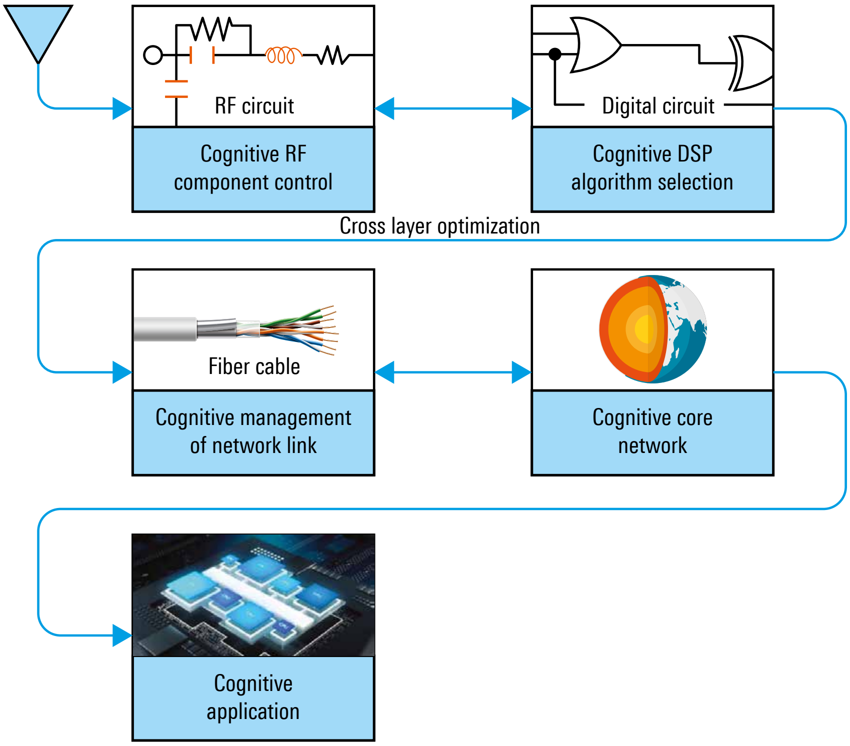
6.2 Key technologies as 6G enablers

One of the ways to predict what 6G may provide is to examine the direction of current fundamental and applied research. Three key enabling technologies are poised to drive the development of 6G: artificial intelligence (AI), advanced RF and optical technologies, and network technologies.

6.2.1 Artificial intelligence

No one would doubt that AI has become one of the most studied areas across many engineering disciplines. While 5G is known for a revolution in flexibility, 6G will likely be known for using AI to capitalize on flexibility [30]. In the past, wireless research activities have made use of AI in various areas, such as the design of handover algorithms using neural networks and fuzzy logic [31]. However, practical implementations of AI based algorithms in wireless networks have been relatively rare. The situation is changing now. Recent advances in learning techniques such as deep learning and new computing architectures that can make these complex algorithms practical have been key drivers behind this trend. Wireless communications is no exception to this trend. Fig. 6.1 shows what a 6G network could look like, with AI/cognition spread across all levels and optimized jointly across the levels in the radio access network, the core network and applications. Such adaptability can improve the resilience of the network and lower operational costs and maintenance costs.

Fig. 6.1: AI-driven 6G network



RF can benefit from cognitive tuning of components to optimize for environmental impairments (such as interference) or the impact of aging or detuning of the circuitry. Modems and protocols can be adaptive to facilitate better spectrum management and demodulation, especially in the case of heterogeneous interference, something to be expected with the emergence of spectrum sharing. Federated learning techniques can leverage each mobile unit as a sensor to provide a holistic yet detailed view of the interference and coverage issues across a broad region [32]. Mechanisms for supporting fronthaul and backhaul can be made more robust by using AI to find the appropriate mechanism for routing information, including the use of satellite or terrestrial wireless relaying. Studies are underway to examine the use of AI within the core network for system optimization, orchestration and maintenance [33]. Security of this overall AI-RAN can be continuously improved through the use of adversarial learning – competition between an AI network attacker and an AI network defender to find vulnerabilities and their solutions [34]. At the application level, AI can anticipate the context and need for application information and preset the network parameters to accommodate the anticipated information flow. (A form of "precognition", a term from the science fiction movie Minority Report.)

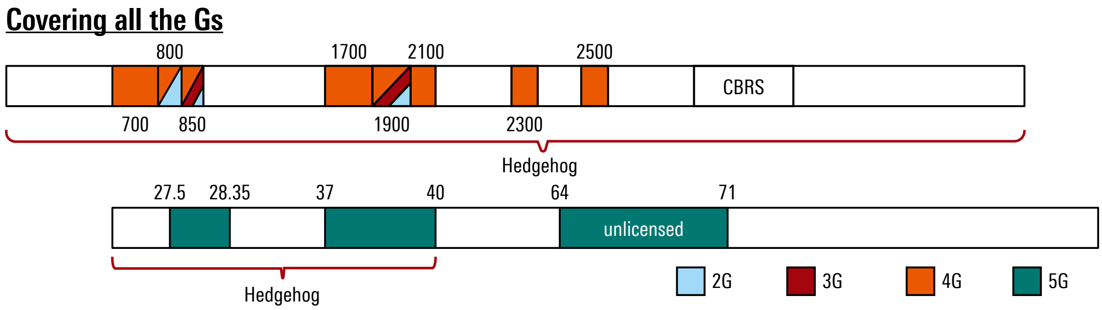
6.2.2 RF and optical technologies

One of the key enablers of 5G has been the low-cost production of mmWave devices in recent times (in addition to the huge amount of spectrum available in the mmWave frequency bands). This trend is expected to continue, with higher frequency, more power efficient devices. Eventually, this technology trend may make terahertz (THz) communications economically feasible [10)]. A complete phased array can be placed on a chip [35]. Such a phased array chip would not need external power pins to communicate if wireless power is used.

Another factor is flexibility in RF components. The DARPA HEDGEHOG program is an example of such technology that is built on an RF field programmable gate array (FPGA) to create a very small radio that is highly configurable to cover a variety of bands from 10 MHz to 40 GHz – see Fig. 6.2 [36].

Fig. 6.2: Configurable RF: specs of Hedgehog (experimental DARPA radio)

Parameter	Specification
Frequency range	DC to 40 GHz
IBW	10 MHz to 2 GHz
Channels	8 TX, 8 RX
Integrated processing	▶ GPP and FPGA ▶ over 280 Gbps I/O
Converters	▶ 16 × 14-bit DACs ▶ 16 × 12-bit DACs ▶ integrated with processor



Such flexibility will work synergistically with AI to adapt the radio for the users' service needs and the RF environment. Taking full advantage of such technology requires the development of new communication protocols.

Single-frequency full-duplex has been demonstrated and is a testimony to ever-improving RF technology [38]. In such a system, the transmitter and receiver operate at the same time and on the same frequency, conceptually doubling the spectral efficiency of a system by eliminating the need for frequency or time duplexing. Such systems work by performing interference cancellation at the RF stage to remove the high-power transmit signal. Such technology will provide an even more flexible spectrum management technique for the 6th generation of wireless communications.

6G will no doubt extend beyond 95 GHz into the high mmWave and terahertz range, including the optical spectrum. At such frequencies, communications tend to be short range, but the devices can be tiny to support technologies such as ultra-massive MIMO and applications such as small swarms (insect-sized collaborating robots).

[10)] The FCC has made THz spectrum in the 95 GHz to 3 THz range available for experimentation as part of the Spectrum Horizons order [37].

Optical 6G also shows promise with reduced interference, tremendous bandwidths, privacy to line-of-sight and an established technology base of devices that transmit and receive. Interestingly, ultraviolet light does NOT require line of sight; it scatters in the atmosphere [11)].

6.2.3 Network technologies

Like 5G, network technologies for 6G will continue the use of SDN, NFV and network slicing. However, 6G could take these concepts to the extreme, allowing customized network slices according to an individual's needs and applications to create a truly customized quality of experience for that individual. Such a system with personalized network slices would inevitably leverage edge computing on a massive scale and create a very complex distribution of network responsibilities between the core network and edge computing nodes.

6.3 Potential performance targets for 6G

New standards have a variety of metrics that include typical specifications of data rates, latency and availability. 6G will continue with the trend begun with 5G of defining quality of experience (QoE) over individual metrics. Certainly, there will be higher data rates, perhaps terabits per second. Latencies may be as low as tens of microseconds, and perhaps information will be freshness dated with the age-of-information to aid in prioritized processing of information. Power consumption reductions that are already targeted for 10 year battery life for IoT devices in 5G could be further reduced to allow energy harvesting, including backscatter communications [39]. 6G might also include both metrics and standards for energy harvesting and wireless power requirements. One might expect to see metrics for security resilience in 6G standards, especially with the potential of quantum computing to be able to break most encryption standards by the time 6G appears.

6.4 Potential 6G services

So what sort of services might 6G and beyond wireless systems provide? 6G will build on 5G to enhance existing services as well as introduce additional modes to handle applications with widely different needs [40]. For example, while 5G will introduce holograms, 6G would likely enable high-fidelity holograms on a massive scale. One possible new application area is providing ultra-low-power communications to tiny devices through energy harvesting or wireless power. Such devices could be part of the fabric of clothes or embedded into plastic or glass. They could constitute the communications between swarms of small UAVs or robots that can coordinate to perform complex tasks such as assembly and repairs. There may eventually be many thousands of radios per individual. Accomplishing this would require a standard with protocols that facilitate energy transfer (wireless power) or energy harvesting configuration merged with communications protocols.

We could see new applications that require a whole new level of latency management. For example, low enough latency for precise power grid control with distributed energy sources and sinks. Tactile sensing applications also push the limits for low latency. This could be accomplished with freshness dating information using an age-of-information metric to prioritize processing or it could be achieved by using AI to anticipate communications or application needs or potential faults to provide robust connectivity. Such capability will allow imperceptible seamless coverage, including a rapid transition between satellite communications and terrestrial communications.

[11)] In the late 1990s, an infrared version existed in the early 802.11 specification to provide up to 2 Mbps connectivity. It could be found on selected laptops at that time.

Services that require data rates even higher that ultra high are inevitable. One possible service may be video wallpaper that uses large display technology to form the walls of a room with projected images. We are now seeing the emergence of 8k video, and data speeds to support 8k video are around 360 Mbps. Scaling this up to provide an immersive experience on each wall means that one wall may need well over 10 Gbps of communications speed for a real-time display. In this case, a terabit per second link is not an unreasonable need.

Sensing as a service is a possible new category for 6G applications. Could 6G signals be used to measure moisture or other particulates in the air to create a micro-climate profile? Could it be possible to leverage the signal as a radar signal to get very precise localization for indoor flying UAVs?

It is difficult to say at this point what 6G may bring. While an initial version of 6G might come in the 2030 time range, it will also undergo several years of revisions. Predicting what the standard will evolve to in 2035 is a fascinating but very speculative endeavor.

7 SUMMARY

5G Phase 1 or R15 provides a strong foundation for enhancements in future releases by defining a high performance NR air interface and flexible network architecture. R16 and later releases focus on new verticals to significantly expand the applications of wireless communications. This trend to support verticals is expected to accelerate in 6G.

Going beyond the eMBB-centric R15, R16 and later releases will expand the supported services. 5G LAN can replace or augment fixed or wireless LAN and provide flexibility and enhanced performance. In non-terrestrial networks, satellites use 5G to provide service ubiquity, service continuity and service scalability. Critical medical applications benefit from 5G performance to improve healthcare and reduce costs. 5G enables new V2X use cases such as platooning, advanced driving and remote driving. 5G based UAVs can support a variety of scenarios including delivery of medical supplies in disaster situations. 5G facilitates audio-visual production services inside and outside studios. Cyber-physical control applications can exploit 5G to make Industry 4.0 a reality on a large scale. NR based positioning supports numerous use cases, including emergency situations, UAV operations, AR/VR/XR and factory automation. Haptic communication takes the user experience to a whole new level by exploiting the haptic sense.

NR undergoes numerous enhancements beyond R16. NR-U uses NR in unlicensed spectrum and supports a variety of scenarios, including carrier aggregation and dual connectivity. IAB enables the use of spectrum for backhaul in addition to traditional access to reduce deployment costs and simplify radio-core connectivity. URLLC-centric enhancements include increased reliability, faster processing, more flexible HARQ, uplink cancellation and enhanced uplink power control. Industrial IoT related NR enhancements include support for TSN reference times and Ethernet, flexible grants and scheduling. New frequency bands between 7 GHz and 24 GHz and above 53 GHz open up more spectrum for numerous use cases, including densification, industrial IoT, backhaul, fronthaul and ITS. NR also makes enhancements related to MIMO, mobility, positioning and UE power savings.

R15 defines virtualization-friendly service based architecture. This architecture is enhanced for V2X, network automation, CLI/RIM, eCAPIF and IMS. V2X related enhancements include support for the NR based PC5 interface. NWDAF and its interactions with other NFs are being expanded to increase the degree of automation and to facilitate AI based operations. The work on CLI/RIM aims to enable dynamic TDD while reducing overall interference. eCAPIF supports multiple API providers and addresses charging requirements. IMS is being enhanced to work with SBA and to support edge computing.

3GPP is also defining SEAL and SON for 5G and enhancing the security framework. At the application layer, SEAL provides services such as group management and configuration management to applications of various verticals by working with the vertical application layer (VAL). 5G SON supports traditional LTE-like algorithms such as ANR and PCI configuration along with new algorithms related to network slicing. Security is being further tightened, especially in light of the expansion into new verticals.

While R16 and later releases for 5G have immense untapped potential, 6G will take the user experience to a whole new level and would revolutionize many industries. Data rates on the order of terabits per second, latency on the order of few microseconds, and high energy efficiencies for the devices and the network could be hallmarks of 6G. High-fidelity holographic communications and multisensory communications could become part of our daily lives. While industries such as healthcare, manufacturing, entertainment and transportation would begin to be influenced by 5G, they would be transformed on a larger scale by 6G.

The world around us will be significantly shaped by the upcoming enhancements in wireless communications. Be prepared to be amazed.

8 LITERATURE

[1] Nishith D. Tripathi and Jeffrey H. Reed, “5G Cellular Communications - Journey and Destination”, multimedia eBook, https://thewirelessuniversity.com/, May 2019

[2] Rohde & Schwarz, “5G New Radio”, https://www.mobilewirelesstesting.com/5g-new-radio-digital-book/, 2019

[3] 3GPP, TS 22.104, “Service requirements for cyber-physical control applications in vertical domains; Stage 1”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3528

[4] 3GPP, TR 22.821, “Feasibility Study on LAN Support in 5G”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3281

[5] 3GPP, TR 22.822, “Study on using satellite access in 5G”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3372

[6] 3GPP, TR 22.826, “Study on communication services for critical medical applications”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3546

[7] 3GPP, TR 22.827, “Study on Audio-Visual Service Production”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3520

[8] 3GPP, TR 22.829, “Enhancement for Unmanned Aerial Vehicles (UAVs)”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3557

[9] 3GPP, TR 22.832, “Study on enhancements for cyber-physical control applications in vertical domains”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3629

[10] 3GPP, TR 22.872, “Study on positioning use cases”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3280

[11] 3GPP, TR 22.886, “Study on enhancement of 3GPP support for 5G V2X services”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3108

[12] 3GPP, TS 23.287, “Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3578

[13] 3GPP, TS 23.434, “Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3587

[14] 3GPP, TR 23.758, “Study on Application Architecture for enabling Edge Applications”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3614

[15] 3GPP, TR 23.791, “Study of enablers for Network Automation for 5G”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3252

[16] 3GPP, TR 23.794, “Study on Enhanced IMS to 5GC Integration”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3421

[17] 3GPP, TR 28.861, “Telecommunication management; Study on the Self-Organizing Networks (SON) for 5G networks”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3556

[18] 3GPP, TR 38.824, "Study on physical layer enhancements for NR ultra-reliable and low latency case (URLLC)", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3498

[19] 3GPP, TR 38.825, "Study on NR industrial Internet of Things (IoT)", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3492

[20] 3GPP, TR 38.840, "Study on User Equipment (UE) power saving in NR", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3502

[21] 3GPP, TR 38.855, "Study on NR positioning support", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3501

[22] 3GPP, TR 38.874, "Study on integrated access and backhaul", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3232

[23] 3GPP, TR 38.889, "Study on NR-based access to unlicensed spectrum", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3235

[24] 3GPP, RP-182863, "Revised WID: Enhancements on MIMO for NR", https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=RP-182863

[25] 3GPP TS 33.501, "Security architecture and procedures for 5G system (Release 15)", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[26] 5G Americas, "The Evolution of Security in 5G: A "Slice" of Mobile Threats, July 2019", white paper, https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper_8.15.pdf

[27] 3GPP, specification series for security issues, https://www.3gpp.org/DynaReport/33-series.htm

[28] UK5G, "Technical Report on 5G Network Architecture and Security", A collaborative paper, DCMS Phase 1 5G Testbeds & Trials Programme, UK5G Report, December 2018, https://uk5g.org/5g-updates/research/technical-report-5g-network-architecture-and-secur/.

[29] Martijn Rasser, "Setting the Stage for U.S. Leadership in 6G", August 13, 2019, LawFare, https://www.lawfareblog.com/setting-stage-us-leadership-6g

[30] M. Yao, M. Sohul, V. Marojevic, J.H. Reed, "Artificial Intelligence0Defined 5G Radio Access Networks", IEEE Communications Magazine, Volume 57 Issue 3, March 2019, pages 14-20. doi>10.1109/MCOM.2019.1800629

[31] Nishith D. Tripathi, Jeffrey H. Reed, and Hugh F. VanLandingham, "Radio Resource Management in Cellular Systems", Kluwer Academic Publishers, 2002

[32] Solmaz Niknam, Harpreet S. Dhillon, Jeffery H. Reed, Federated Learning for Wireless Communications: Motivation, Opportunities and Challenges, https://arxiv.org/abs/1908.06847, (Submitted on 30 Jul 2019 (v1), last revised 24 Aug 2019 (this version, v2))

[33] Improved operator experience through Experiential Networked Intelligence (ENI) Introduction – Benefits – Enablers – Challenges – Call for Action, ETSI White Paper No. 22, 1st Edition, October 2017, ISBN No. 979-10-92620-16-0. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp22_ENI_FINAL.pdf

[34] Y. Shi, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu and J. H. Li, "Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies", 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, 2018, pp. 1-6. doi: 10.1109/ICCW.2018.8403655Satcomm

[35] M. M. Assefzadeh and A. Babakhani, “Broadband beamforming of terahertz pulses with a single-chip 4×2 array in silicon”, 2016 IEEE International Symposium on Antennas and Propagation (APSURSI), Fajardo, 2016, pp. 589-590. doi: 10.1109/APS.2016.7696003

[36] Tom Rondeau, “RF Convergence: From the Signals to the Computer”, IEEE Workshop on 5G Technologies for Tactical and First Responder Networks Columbia, MD, 10/23/2018

[37] FCC 19-19, “Spectrum Horizons First Report and Order”, ET Docket No. 18-21, https://www.fcc.gov/document/fcc-opens-spectrum-horizons-new-services-technologies-0

[38] C. D. Nwankwo, L. Zhang, A. Quddus, M. A. Imran and R. Tafazolli, “A Survey of Self-Interference Management Techniques for Single Frequency Full Duplex Systems”, in IEEE Access, vol. 6, pp. 30242-30268, 2018. doi: 10.1109/ACCESS.2017.2774143

[39] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang and D. I. Kim, “Ambient Backscatter Communications: A Contemporary Survey”, in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2889-2922, Fourth quarter 2018. doi: 10.1109/COMST.2018.2841964

[40] P. Yang, Y. Xiao, M. Xiao and S. Li, “6G Wireless Communications: Vision and Potential Techniques”, in IEEE Network, vol. 33, no. 4, pp. 70-75, July/August 2019. doi: 10.1109/MNET.2019.1800418

[41] 3GPP, TR38.305, “Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3310

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support

PD 3608.3326.52 | Version 01.00 | March 2020 (ch)
White paper | 5G evolution – on the path to 6G
Data without tolerance limits is not binding | Subject to change

3608332652
3608.3326.52 01.00 PDP 1 en

Mobile Network Testing of 5G NR FR1 and FR2 Networks: Challenges and Solutions

Christoph Hausl, Julian Emmert, Manuel Mielke, Benjamin Mehlhorn and Corbett Rowell
Rohde & Schwarz, Munich, Germany

This article describes a mobile network testing approach for 5G new radio (NR) using a passive scanner, which measures synchronization signal (SS)/physical broadcast channel (PBCH) blocks, or SSBs, broadcast from 5G NR base stations. It starts with relevant background information about 5G NR and mobile network testing, followed by a description of a typical measurement methodology for the frequency ranges one (FR1) and two (FR2). Next, it addresses two typical challenges: 1) finding carrier frequencies with SSBs and 2) network synchronization. A solution is proposed for each.

5G wireless radio access technology, known as NR, contains more flexibility to address different usage scenarios.[1,2,3] The 5G NR specification allows optimization to reduce the latency and to significantly increase the data rate. These optimizations require many new technology components, including new frequency bands, beamforming support for synchronization and broadcast and multi-connectivity to enable the combination of 5G network elements with LTE. 5G NR supports operation in two frequency ranges: FR1 below 7,125 MHz[4] and mmWave bands (FR2) between 24.25 and 52.6 GHz.[5]

Throughout the entire chain of laboratory testing, field trials, network rollout, optimization and benchmarking, measurement tools for mobile network testing (MNT) are required to characterize the conditions of the wireless channel and network coverage in the field.[6,7] For example, measurements of received power enable verification of 5G NR cell beamforming and its impact on the coverage area. Measurements of the channel impulse response result in deeper knowledge about the propagation of wireless signals in different environments, i.e., reflection, absorption and scattering in urban versus rural areas. Measurements of arrival times enable verification of network synchronization aspects.[8]

5G and associated technologies such as beamforming and frequencies above 3 GHz have raised potential health concerns due to the human exposure to the electromagnetic field of base stations. Consequently, 5G base station deployment requires that the electrical field strength (V/m) is below the specific threshold for each country. Frequency selective measurement methods of exposure to 5G base stations have been described,[9,10] emphasizing the need for code selective measurement methods, especially in networks with several base stations and with data traffic.

A mobile network operator must evaluate the quality of the network to investigate network problems, unwanted interference or assessment of new base stations. While it is possible to evaluate the performance of the network using a mobile phone, the disadvantage is measurement variation, as results vary depending on the chip set or installed software. Therefore, a reference measurement device such as a receiver or scanner is required, which provides a common ground for comparison.

With the use of non-standalone (NSA) and dynamic spectrum sharing, the 5G NR FR1 and corresponding LTE channel must be measured at the same time to ensure that both network links work as expected. Detection and measurement of these base station cells is challenging because the measurement must achieve a high sensitivity while avoiding false alarms that result in detecting non-existing cells (i.e., ghost codes).

Measurement of the carrier frequencies of a mobile network enables independent characterization of the network and, together with a wideband passive receiver, enables benchmarking of different networks—even networks that are completely unknown—removing the influence of the mobile phone. As this measurement approach is completely passive, all public and private networks, such as campus networks, can be detected and measured.

BACKGROUND

5G NR Synchronization Signal/PBCH Blocks (SSBs)

5G NR technology uses orthogonal frequency division multiplexing (OFDM)[2] for downlink transmission. A band dependent table[4,5] defines whether time division duplexing (TDD) or frequency division duplexing is used to divide the downlink (DL) and uplink (UL). A 5G NR cell broadcasts SSBs to enable cell search and initial access. One SSB is mapped to four OFDM symbols and 240 subcarriers (SC).

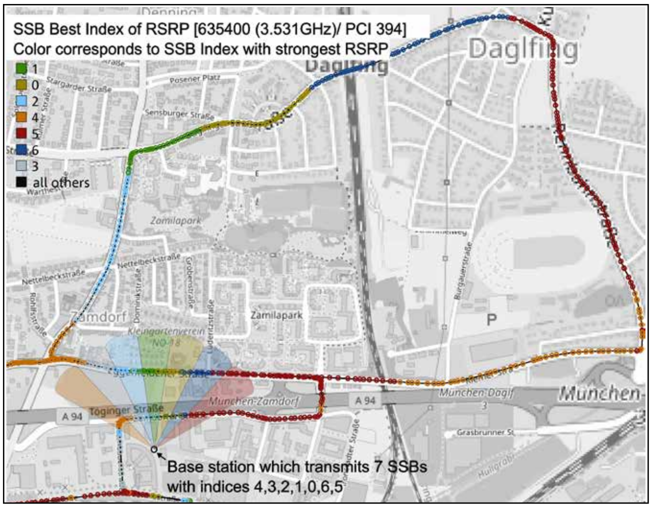
The SSB consists of one PBCH block, a primary and a secondary synchronization signal (PSS and SSS). There are different SC spacings (SCS) defined: from 15 kHz for Case A in FR1 to 240 kHz for Case E in FR2.[11] Therefore, the bandwidth of one SSB is between 3.6 and 57.6 MHz. Correspondingly, the SSB duration is between 285 and 18 µs, enabling flexibility to use 5G NR in different frequency ranges and use cases.[1]

One cell transmits up to 64 SSBs within a 5 ms window (i.e., up to four or eight SSBs for SCS of 15/30 kHz). Each of these SSBs has a specific index, which is encoded beside the cell-specific physical cell identity (PCI) into the SSB-signal. The start time of a SSB within the 5 ms window depends on the index, as defined by the 3GPP technical specification.[11] The cells broadcast these 5 ms windows periodically, with the default period 20 ms.

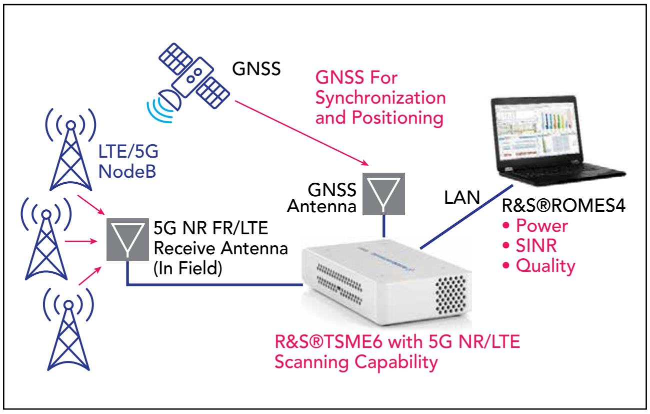
Typically, a cell uses beamforming to transmit the SSBs in different directions (i.e., beam sweeping) and, consequently, the SSBs are also referred to as beams. These beams can be considered as micro sectors that further split the macro sector of the complete cell—typically 120-degree azimuth coverage—into smaller angular portions.[6] ***Figure 1*** illustrates the main transmission direction of seven SSBs of one cell on a map. The use of beamforming for synchronization signals and PBCH provides better overall coverage. Note that the direction of the beams can be two-dimensional in the sense that each SSB transmits into a specific azimuth and tilt angle.

Mobile Network Testing

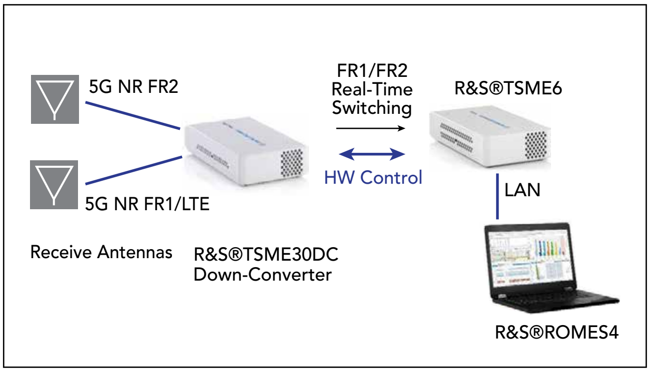
Figure 1 also shows the route of a drive test, a method often used for MNT. The aim of the drive test is to measure the reception quality of the base station cells and their SSBs to determine network quality and coverage. The drive tests are also used to find interference, either from other cells or unlicensed deployments. Variations of conventional drive tests are walk tests, bike tests and drone tests, the latter requiring small passive receivers with low power consumption because of limited battery capacity.



▲ Fig. 1 Transmission direction of seven SSBs of one cell estimated by comparing the measured received power for all SSBs during a drive test. The color of the route corresponds to the SSB with the strongest receive power.[7]



▲ Fig. 2 Setup for sub-6 GHz measurements of 5G NR FR1 and LTE signals.



▲ Fig. 3 Setup with mmWave antenna and down-converter for simultaneous 5G NR FR2 and sub-6 GHz measurements.

MEASUREMENT SETUP

Sub-6 GHz Measurement Setup

Figure 2 shows the proposed measurement setup with a passive receiver or scanner, such as the R&S TSME6 mobile network scanner. Fed by an external antenna, the scanner measures the wireless signal from 5G FR1 and LTE cells, converts this signal into a digital baseband signal of I/Q symbols and sends it to a connected laptop for demodulation, analysis and presentation. The scanner contains an internal global navigation satellite system (GNSS) receiver to measure its geographical position, as well as receiving date and time information. For security reasons, the scanner itself is a passive receiver with no transmission capability. It can measure a baseband signal with a bandwidth of 20 MHz between 350 MHz and 6 GHz, the frequency range controlled by the measurement software on the laptop. The measurement software can be based on R&S ViCom, an open application programming interface, which enables custom scanner applications. Alternatively, ready-to-use software such as R&S Romes can be used.

FR2 Measurement Setup

The carrier aggregation framework in 5G NR allows complementary operation in FR2 with an FR1 carrier to ensure good coverage,[1] requiring simultaneous SSB measurements in FR1 and FR2. ***Figure 3*** shows the measurement setup for FR2. It requires a down-converter which converts the mmWave signal to an intermediate frequency below 6 GHz, so a single scanner with dedicated antennas can support simultaneous measurements in FR1 and FR2. One single scanner with one down-converter supports SSB measurements in FR2, and it is possible to connect several scanners with one down-converter, extending the baseband bandwidth to 100 MHz; however, this is not necessary for current applications.

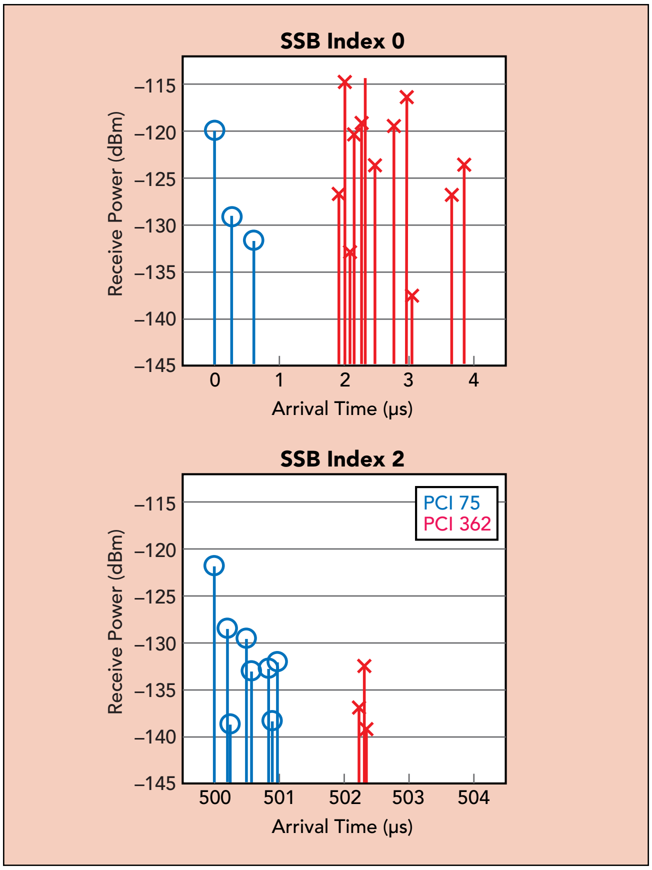
CHALLENGE 1: HOW TO ANALYZE THE 5G NR SSBS?

Accessing or measuring a 5G NR carrier starts with discovering the center frequencies of the SSBs. In LTE, the PSS/SSS and PBCH signals are always transmitted around the center frequency of the carrier with fixed periodicity, making it possible to manually detect them in the power spectral density measured with a receiver. In 5G NR, however, the transmission characteristics of the SSBs are more flexible, creating new challenges to configuring a 5G NR receiver/scanner.

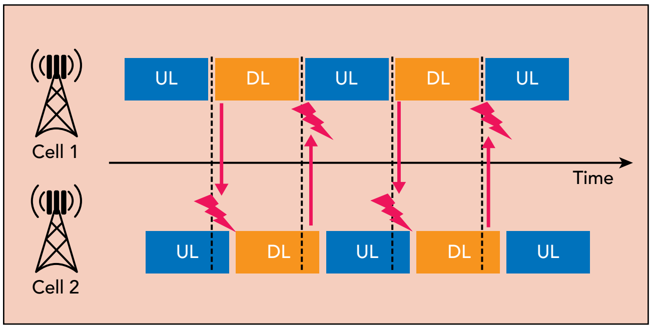
The most challenging problem is the flexibility regarding the SSB center frequency (SSRef). The 3GPP standard defines a frequency raster for the appearance of SSBs,[4,5] but the raster is narrow with hundreds of possibilities within a 5G NR carrier. Further, a single SSB only appears for a short time, so it is difficult to detect the SSB with a traditional swept-tuned spectrum analyzer; the SSB periodicity is flexible with the frame starting point and its corresponding period: 5, 10, 20, 40, 80 or 160 ms.[12]

To avoid time consuming spectrum scans, wrong scanner configuration or simply guessing the correct SSB center frequency, the proposed receiver/scanner solution is detecting the SSRef using an algorithm called Automatic Channel Detection (ACD). ACD can search quickly through large frequency ranges, where it runs an internal spectrum scan and searches for SSBs.[13] ACD delivers the correct SSRefs within seconds, enabling the scanner to analyze both in-band and out-of-band, i.e., competitor networks where the cellular network parameters are completely unknown.

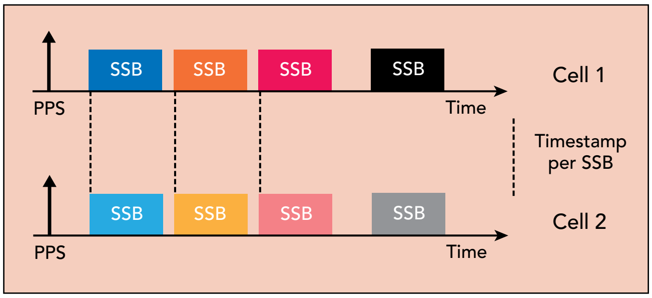
The ACD algorithm first provides a list of the SSB center frequencies; then, the scanner starts the SSB measurement algorithm (SSBmeas) for these frequencies. ACD can run in the background of the baseband processing, continuously searching for new SSB center frequencies. As soon as the scanner receives the signal



▲ **Fig. 4 Measured arrival times and channel impulse response of SSB indices 0 and 2 for two cells.**



▲ **Fig. 5 Interference between two cells.**



▲ **Fig. 6 UTC synchronized base stations.**

of a base station cell strong enough for ACD sensitivity during a measurement, the corresponding SSRef will be scanned with the more sensitive SSBmeas for the remaining portion of the measurement. The ACD algorithm expects a 3GPP compliant 5G NR SSB transmitted on frames with an increasing system frame number. Internally, it uses the 3GPP band table to select the SSB transmission case for the selected frequency bands. This accelerates the ACD algorithm and avoids checking for unnecessary cases (e.g., Case E for band n1).

From the SSB measurement, many network features can be obtained to assess network quality, such as synchronization signal signal-to-interference-plus-noise ratio (SS-SINR) and synchronization signal reference signal received power (SS-RSRP).[14] It is also possible to extract the cell identity (PCI), the SSB index, the channel impulse response and the arrival time for all detected cells and beams. SSB detection includes a decoding of the PBCH, preventing ghost codes, as the PBCH payload contains a cyclic redundancy check for error detection.

Figure 4 illustrates the measured arrival times of peaks of the channel impulse response for SSB-indices 0 and 2 of two cells (PCI 75 and PCI 362) at SSRef 3,574.56 MHz (Case C). The measurement is primarily interested in the arrival time difference to the first measured peak to measure the delay spread. The measurement confirms the expectation[11] that the SSB with index 2 is transmitted 500 μs later than SSB with index 0. From Figure 4, the distribution of the peaks indicates how much reflection and scattering occurred with higher delay spread for index 0. The signal of the cell with PCI 362 arrives approximately 2 μs later than the one from the other cell with PCI 75, which is mainly caused by the larger cell-to-receiver-distance for PCI 362.

CHALLENGE 2: NETWORK SYNCHRONIZATION MEASUREMENTS

Ensuring base station synchronization is a critical component for successful network deployment. If a base station is out of sync, the handover of active connections will fail, leading to dropped calls for the user and a poor user experience. For TDD, the synchronization requirement is particularly crucial, as a time offset can lead to an overlap of uplink and downlink time slots, impacting base station performance and interfering with correctly synchronized neighboring base stations (see ***Figure 5***).

The allowed time alignment error is specified by the 3GPP (Release 15, Section 6.5.3). To ensure proper synchronization, the cells receive their reference time from the network or via a connected GNSS receiver.[8] Networks of different operators must be synchronized to avoid interference due to intermodulation products between networks on neighboring frequencies. This enables all operators to minimize interference.

Previously, these timing measurements were performed with a spectrum analyzer and special test ports on the base station, requiring cabled measurements. In 5G NR, the common deployment of remote radio heads and active antenna systems without special test ports makes conventional timing measurements difficult and requires over-the-air timing measurements.

To verify the time synchronization of a network, the proposed scanner uses two possible measurements of varying precision: 1) a time of arrival (ToA) measurement of the received SSBs and 2) a time alignment error (TAE) measurement of the received SSBs. The ToA measurement provides a time stamp for the received SSB. This provides a good indication whether a certain base station cell is out of sync compared to other base stations received. The ToA measurement provides a precision of about 400 ns. To achieve higher precision and fulfill the coordinated universal time (UTC) second synchronicity requirement, a TAE measurement is used.

For the TAE measurement, line-of-sight (LoS) to the cell is required where the distance between measurement antenna and cell antenna is known—which can be measured with a laser range finder—together with good GPS reception or an external time base as the time reference. The receiver/scanner can calculate the UTC transmission time of every received SSB as well as the frequency error of the cell (see ***Figure 6***). Measurement precision is then dependent on the provided reference of the integrated GNSS receiver. Good GPS reception yields a time accuracy below 30 ns. From the known distance between measurement position and base station, the transmit time can be calculated, identifying timing issues rooted in the setup of the base station. Experimentally, it has been verified that the following conditions need to be fulfilled to enable such a precise measurement:

- The signal from the measured base station must have a SINR above 15 dB
- The delay spread needs to be below 17 ns, which is used as indicator for LoS
- To obtain best performance with a GNSS receiver, movement faster than 30 kmph is recommended to remove reflections from the received signals.
- A high accuracy pulse per second (PPS) signal must be available, either from the GNSS receiver or an external connection
- The PPS signal needs to provide higher accuracy than the internal time base
- The GNSS receiver must report a valid UTC time synchronization.

CONCLUSION

This article demonstrated how to use a passive scanner for measurements in 5G NR networks, with special attention to network synchronization in both the FR1 and FR2 bands. Methods for the measurement of network coverage, network synchronization and channel impulse response were proposed and are straightforward to implement. An approach for ACD to find the relevant carrier frequencies for 5G MNT in networks with an unknown configuration was presented. Finally, the proposed methods were applied for deployed 5G networks to demonstrate effectiveness.

References

1. X. Lin, J. Li, R. Baldemair, T. Cheng, S. Parkvall, D. Larsson, H. Koorapaty, M. Frenne, S. Falahati, A. Grövlen and K. Werner, "5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology," *IEEE Communications Standards Maga-*

zine, Vol. 3, No. 3, September 2019, pp. 30-37.
2. S. Ahmadi, "5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards," *Academic Press*, 2019.
3. M. Kottkamp, A. Pandey, D. Raddino, A. Roessler and R. Stuhlfauth, "5G New Radio: Fundamentals, Procedures, Testing Aspects," Rohde & Schwarz, 2019.
4. "3GPP Technical Specification TS 38.101-1, NR; User Equipment (UE) Radio Transmission and Reception; Part 1: Range 1 Standalone," 3GPP, V16.8.0, June 2021.
5. "3GPP technical specification TS 38.101-2, NR; User Equipment (UE) Radio Transmission and Reception; Part 2: Range 2 Standalone," 3GPP, V16.8.0, June 2021.
6. A. Sibila, "5G NR Network Rollout is Now – Let's Test!" *Microwave Engineering Europe*, July 2019.
7. M. Mielke and M. Hylen, "5G NR Network Measurements using Network Scanners and Advanced Data Analytics," Rohde & Schwarz, Version 3.0, April 2019.
8. S. Rufini, M. Johansson, B. Pohlman and M. Sandgren, "5G Synchronization Requirements and Solutions," *Ericsson Technology Review,* January 2021.
9. S. Aerts, K. Deprez, D. Colombi, M. Van den Bossche, L. Verloock, L. Martens, C. Törnevik and W. Joseph, "In-Situ Measurement Methodology for the Assessment of 5G NR Massive MIMO Base Station Exposure at Sub-6 GHz Frequencies," IEEE Access, Vol. 7, December 2019, pp. 184658-184667.
10. C. Bornkessel, T. Kopacz, A. M. Schiffarth, D. Heberling and M. A. Hein, "Determination of Instantaneous and Maximal Human Exposure to 5G Massive-MIMO Base Stations," 15th European Conference on Antennas and Propagation, 2021.
11. "3GPP technical specification TS 38.213, NR; Physical layer procedures for control," 3GPP, V16.6.0, June 2021.
12. "3GPP technical specification TS 38.331, NR; Radio Resource Control (RRC) protocol specification," 3GPP V16.3.1, January 2021.
13. O. Wanierke, "Method and System for Channel Detection," U.S. Patent No. 10,833,800. U. S. Patent and Trademark Office, 2020, Web: https://patents.justia.com/patent/10833800.
14. "3GPP Technical Specification TS 38.215, NR; Physical Layer Measurements," 3GPP, V16.4.0, December 2020.

Antenna Beam Characterization of 5G Mobile Devices and Base Stations Using the R&S®NRPM Over-the-Air (OTA) Power Measurement Solution
Application Note

Products:

- R&S®NRPM3
- R&S®NRPM-A66
- R&S®NRPM-ZD3
- R&S®TS7124
- R&S®TS-F24-AR
- R&S®TS-F24-AH1
- R&S®TS-F24-AH2
- R&S®TS-F2X-VH4

Radio frequencies in bands around 28 GHz are being discussed as candidates for mobile communications of the fifth generation (5G). Beam steering will be a key feature in the context of 5G. It will be a major challenge to test the beam steering capabilities of base stations and user equipment in every phase from research and development through production. Conducted measurements will be mainly replaced by over-the-air measurements of electromagnetic radiation. Rohde & Schwarz offers the R&S®NRPM Over-the-Air (OTA) Power Measurement Solution that perfectly fits such measurement needs.

Part of this solution are the R&S®NRPM-A66 antenna modules. They have integrated diode detectors. Thus, there are no cables between the antenna and the detector as in traditional setups. This avoids high and potentially unknown RF losses. The R&S®NRPM-A66 antenna modules with their integrated diode detectors are factory calibrated, which means that the user does not have to calibrate them to achieve highly accurate measurement results.

This application note contains theoretical background on OTA power and pattern measurements. It gives step-by-step instructions for the verification of the power level and the radiation pattern of a device under test (DUT) in comparison to a golden device, and it presents an approach for verifying the accuracy of beam steering.

Note:

Please find the most up-to-date document on our homepage
http://www.rohde-schwarz.com/appnote/1GP118

Application Note
F. Gerbl
8.2017 – 1GP118_0E

ROHDE&SCHWARZ

CONTENTS

1 Note

The following abbreviations are used in this application note for Rohde & Schwarz products:

- The R&S®NRPM3 Three-channel sensor module is referred to as NRPM3 sensor module.
- The R&S®NRPM-A66 Single polarized antenna module is referred to as NRPM-A66 antenna module.
- The R&S®NRPM-ZD3 Filtered cable feedthrough is referred to as NRPM-ZD3 feedthrough.
- The R&S®TS7124 RF shielded box is referred to as TS7124 RF shielded box.
- The R&S®TS-F24-AR antenna ring is referred to as TS-F24-AR antenna ring.
- The R&S®TS-F24-AH1 half antenna ring is referred to as TS-F24-AH1 half antenna ring.
- The R&S®TS-F24-AH2 antenna holder is referred to as TS-F24-AH2 antenna holder.
- The R&S®TS-F2X-VH4 adapter is referred to as TS-F2X-VH4 adapter.

2 Introduction

Radio frequencies in bands around 28 GHz are being discussed as candidates for mobile communications of the fifth generation (5G). As frequencies are increasing, components and systems are shrinking. In order to minimize losses and the susceptibility to influences from outside, the level of integration is increasing. As a consequence, test points such as in the signal path from the output of a power amplifier to the input of an antenna will no longer exist. Conducted measurements, i.e. measurements that are done while the device under test (DUT) is connected to the measurement equipment via cables, will be mainly replaced by over-the-air (OTA) measurements, i.e. measurements of electromagnetic radiation.

Besides that, antenna elements and thus their effective areas are shrinking as frequencies are getting higher. Accordingly, the so-called path loss between transmitting and receiving antennas is increasing. To overcome this issue, antenna elements can be arranged in arrays that yield higher gain than a single antenna element. However, this does not mean that the overall transmitted power increases, but that the available power is focused to certain directions.

In mobile communications, the relative positions of a mobile device and a base station vary over time. In order to receive sufficient power, the beam directions of the transmitting and/or the receiving antenna are adjusted. This is accomplished by means of beam steering. Therefore, beam steering is a key feature in the context of 5G. It will be a major challenge to test the beam steering capabilities of base stations and user equipment in every phase from research and development through production.

Rohde & Schwarz offers the NRPM Over-the-Air (OTA) Power Measurement Solution that perfectly fits such tests. As sketched in Figure 1, the solution essentially consists of NRPM-A66 antenna modules and an NRPM3 sensor module.

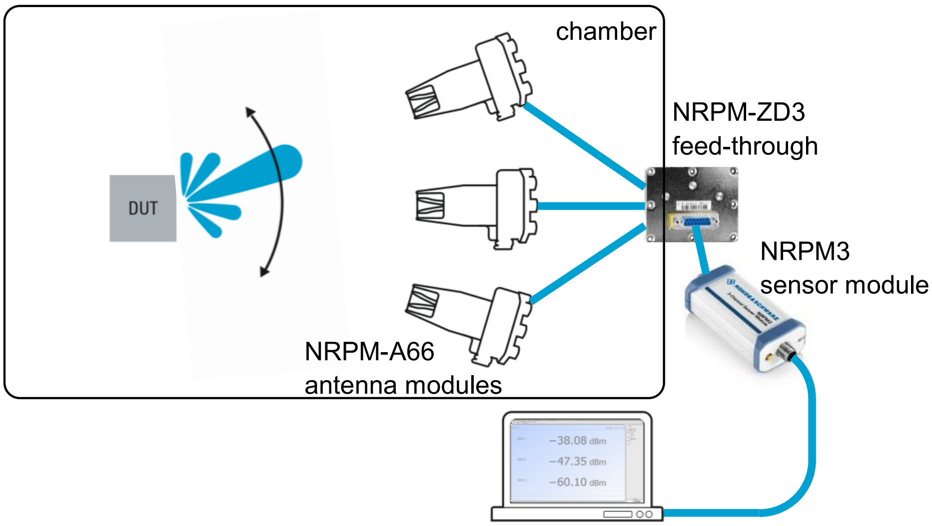


Figure 1: Sketch of the NRPM Over-the-Air (OTA) Power Measurement Solution used to characterize the spatial distribution of the power radiated by the DUT

A variety of antenna holders are available. Together with the NRPM-ZD3 feedthrough, the solution can be perfectly integrated into a TS7124 RF shielded box.

The R&S®NRPM-A66 antenna modules have integrated diode detectors. Thus, there are no cables between the antenna and the detector as in traditional setups. This avoids high and potentially unknown RF losses. The R&S®NRPM-A66 antenna modules with their integrated diode detectors are factory calibrated, which means that the user does not have to calibrate them to achieve highly accurate measurement results.

This application note contains theoretical background on OTA power and pattern measurements. It gives step-by-step instructions for the verification of the power level and the radiation pattern of a device under test (DUT) in comparison to a golden device, and it presents an approach for verifying the accuracy of beam steering. It also gives ideas for modifying those procedures in order to cope with special requirements, as well as points to consider before implementing a particular setup.

3 Theoretical Background on Power and Antenna Pattern Measurements

The RF power P_{DUT} radiated by a DUT distributes in space according to its gain function $G_{\mathrm{DUT}}(\theta_{\mathrm{DUT}}, \phi_{\mathrm{DUT}})$, where θ_{DUT} is the elevation angle and ϕ_{DUT} is the azimuth angle as seen from the DUT. A receiving antenna accepts radiation from different directions in space according to its gain function $G_r(\theta_r, \phi_r)$, where θ_r is the elevation angle and ϕ_r is the azimuth angle as seen from the receiving antenna. Each of the gain functions can be split into the product of their maximum values, $G_{\mathrm{max,DUT}}$ and $G_{\mathrm{max},r}$, and the spatial distribution functions $C_{\mathrm{DUT}}(\theta_{\mathrm{DUT}}, \phi_{\mathrm{DUT}})$ and $C_r(\theta_r, \phi_r)$ according to

$$G_{\mathrm{DUT}}(\theta_{\mathrm{DUT}}, \phi_{\mathrm{DUT}}) = G_{\mathrm{max,DUT}} \cdot C_{\mathrm{DUT}}(\theta_{\mathrm{DUT}}, \phi_{\mathrm{DUT}}) \quad (1)$$

and

$$G_r(\theta_r, \phi_r) = G_{\mathrm{max},r} \cdot C_r(\theta_r, \phi_r). \quad (2)$$

$C_{\mathrm{DUT}}(\theta_{\mathrm{DUT}}, \phi_{\mathrm{DUT}})$ is the radiation pattern of the DUT, while $C_r(\theta_r, \phi_r)$ is the radiation pattern of the receiving antenna.

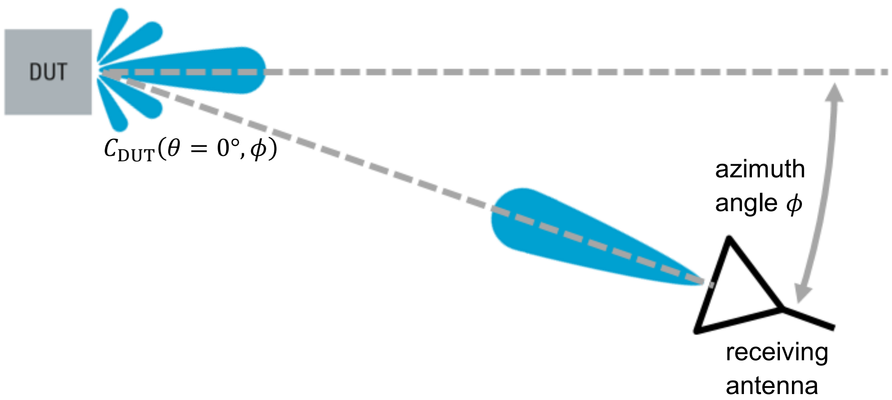


Figure 2: Arrangement of DUT and receiving antenna. ϕ is the azimuth angle. θ is the elevation angle.

The equation that describes the received power as a function of the transmitted power is named the Friis equation [1]. In case

- the antennas are complex conjugate matched to the source and load,
- the receiving antenna is oriented such that its maximum gain is in the direction of the DUT, as indicated in Figure 2,
- the distance between the antennas is sufficient (s. 3.1),
- there are no unwanted echoes or interfering signals (s. 3.2) and
- the antennas are polarization matched (s. 3.3) to each other

the Friis equation can be written as

$$\frac{P_r}{P_{\mathrm{DUT}}} = \left(\frac{\lambda}{4\pi R}\right)^2 \cdot G_{\mathrm{max,DUT}} \cdot C_{\mathrm{DUT}}(\theta, \phi) \cdot G_{\mathrm{max},r} \quad (3)$$

and eventually as

$$C_{\mathrm{DUT}}(\theta,\phi) = P_r(\theta,\phi) \cdot \frac{1}{P_{\mathrm{DUT}} \cdot G_{\max,\mathrm{DUT}} \cdot G_{\max,r}} \cdot \left(\frac{4\pi R}{\lambda}\right)^2. \quad (4)$$

R is the distance between the antennas, $\lambda = c/f$ the wavelength of the transmitted signal of frequency f, and c is the speed of light.

According to (4), samples of the radiation pattern of the DUT, $C_{\mathrm{DUT}}(\theta,\phi)$, can be determined by measuring the power P_r received by receiving antennas placed in the respective spatial directions (θ,ϕ). As long as the wavelength, the transmitted power and the distance between the antennas are kept constant, the antenna pattern of the DUT and the received power are interrelated by

$$C_{\mathrm{DUT}}(\theta,\phi) = P_r(\theta,\phi) \cdot k, \quad (5)$$

where k is a constant that accounts for the constant terms in (4).

The pattern can be sampled by either moving a single receiving antenna to the relevant angles one after another or by placing multiple antennas in the relevant spatial directions.

The equivalent isotropically radiated power of a DUT, $\mathrm{EIRP}_{\mathrm{DUT}}$, is defined as

$$\mathrm{EIRP}_{\mathrm{DUT}}(\theta,\phi) = P_{\mathrm{DUT}} \cdot G_{\mathrm{DUT}}(\theta,\phi). \quad (6)$$

Using (3), it can be rewritten as

$$\mathrm{EIRP}_{\mathrm{DUT}}(\theta,\phi) = P_r(\theta,\phi) \cdot \left(\frac{4\pi R}{\lambda}\right)^2 \cdot \frac{1}{G_{\max,r}}. \quad (7)$$

It can be determined from measurements of the power P_r received by antennas placed in particular directions (θ,ϕ) and pointing to the DUT. NRPM-A66 antenna modules are factory calibrated such that the power reading corresponds to a gain of 1 for radiation that comes from the boresight direction of the NRPM-A66 antenna module. In case the NRPM-A66 antenna module is pointing to the DUT, the EIRP can therefore be determined according to

$$\mathrm{EIRP}_{\mathrm{DUT}}(\theta,\phi) = P_r(\theta,\phi) \cdot \left(\frac{4\pi R}{\lambda}\right)^2. \quad (8)$$

3.1 Distance between the antennas

The space around an antenna can be divided into the near-field and the far-field region. The far-field is characterized by two essential properties. First, the power density is inversely proportional to the square of the distance from the antenna operating in transmit mode. Second, the angular power distribution is independent of distance. A very commonly assumed inner boundary of the far-field region–for an antenna with dimensions larger than the wavelength–is at distance $R_{\min}$ according to

$$R_{\min} = \frac{2D^2}{\lambda}, \quad (9)$$

where D is the largest lateral dimension of the antenna. In case of an aperture antenna, its largest lateral dimension is the size of its diagonal. In case the antenna is embedded in a device, parts of the device itself might contribute to the overall radiation and have influence on the radiation characteristics. If so, D has to be chosen according to the size of the radiating structure rather than the size of the antenna alone.

In order to determine the far-field pattern of a DUT from power measurements according to (5), the power measurements have to be done with the DUT and the receive antenna in each other's far-field, since the pattern generally changes with distance within the near-field. In this case, the sum of largest lateral dimensions of both antennas has to be chosen as the value of D.

However, depending on the type of the DUT and the information that is to be extracted from such a measurement, it might be justified to choose a distance smaller than R_{min}. This is especially true in case of relative measurements, where the values obtained for the DUT are compared to values obtained for a golden device.

Equation (9) is also a criterion for the accuracy of the Friis equation. The Friis equation is an approximation that is correct to within a few percent when the antennas are spaced by at least R_{min}, determined using the largest lateral dimension of either antenna as the value of D [2].

For closer spacings, the Friis equation might not predict the received power very well, but violating the criterion might be justified especially in the case of relative measurements.

3.2 Multipath propagation and interference by other signal sources

The Friis equation is valid only for the line of sight without any additional signal paths between the transmit and the receive antenna. Such additional paths result from echoes as they might occur when objects are in the vicinity of the measurement setup. Those echoes are superimposed on the signals of the desired signal path. This may yield a change of the electromagnetic field at the location of the receive antenna and thus a biased estimation of the properties of the transmit antenna.

The Friis equation assumes that there are no interfering signals. In case the frequency of an interfering signal is inside the range of frequencies to which the power sensor is sensitive, this signal contributes to the measured power and thus yields a biased estimation of the properties of the transmit antenna.

Therefore, the measurements have to be performed in the absence of echoes and interferers. Section 5.3.2 gives hints on suitable environments.

3.3 Polarization matching

The Friis equation in the form presented above assumes that the receive antenna's polarization matches the polarization of the incoming wave. If this is not the case, the power delivered to the receive antenna's load is less than it would be in case of polarization matching. Then, measurements would have to be taken for two orthogonal polarizations, and the obtained powers would have to be added prior to determining the pattern according to (4).

4 Measurement Setup

The setup that will be used for the applications described in the next section is shown in Figure 3. It is common to all of the applications that the DUT operates in transmit mode.

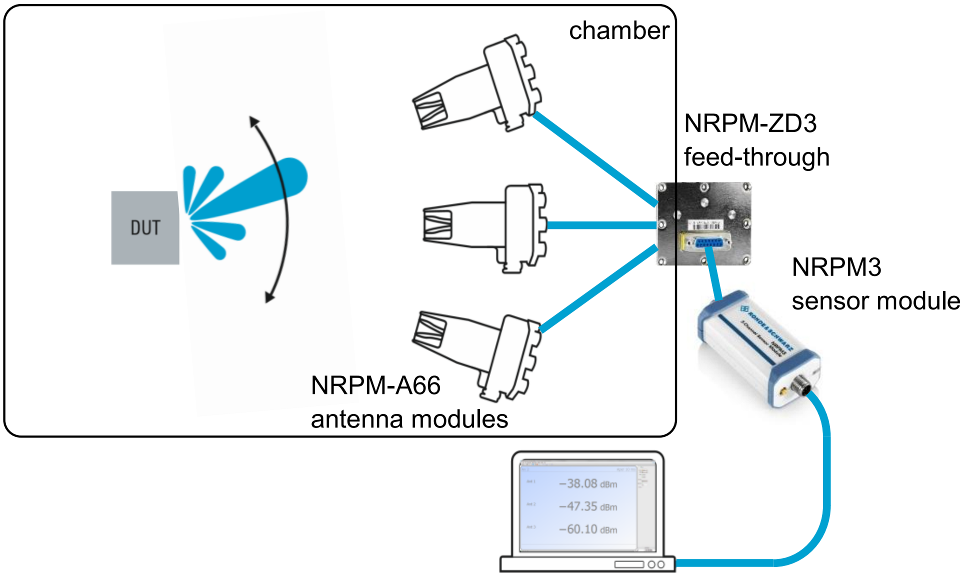


Figure 3: Block diagram of the setup

The setup consists of the DUT and

- 3 NRPM-A66 antenna modules
- 1 NRPM-ZD3 feedthrough
- 1 NRPM3 sensor module
- 1 TS7124 RF shielded box with absorber material
- 1 TS-F24-AH1 half antenna ring with TS-F2X-VH4 adapters
- 1 PC for acquiring data from the NRPM3 sensor module via USB

The beam steering capability of a 5G device is simulated using a rotatable horn antenna transmitting a signal generated by a signal generator. Figure 4 shows how the horn antenna and the NRPM-A66 antenna modules are arranged geometrically.

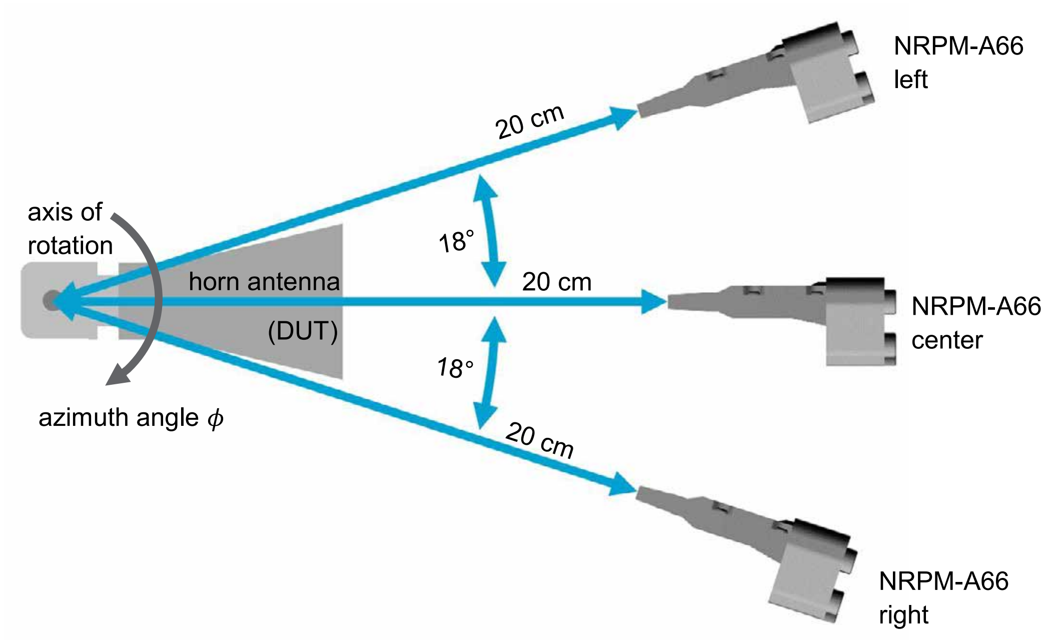


Figure 4: Relative positions of the NRPM-A66 antenna modules with respect to the horn antenna's axis of rotation

The NRPM-A66 antenna modules are pointing towards the horn antenna's axis of rotation. They are oriented such that they are polarization-matched to the horn antenna.

The NRPM-A66 antenna modules are placed at azimuth angles of -18°, 0° and 18° as counted from a line connecting the DUT and the center NRPM-A66 antenna module.

The distance between the axis of rotation and the closest point of the NRPM-A66 antenna modules is approximately 20 cm on average with only minor deviations among the NRPM-A66 antenna modules. As a consequence, the path losses between the DUT and each of the NRPM-A66 antenna modules can be considered identical. This is not a requirement for the application described in 5.1, but it can be very convenient in order to compare the radiation to different spatial directions without having to account for potentially unknown individual path losses.

The measurements are performed using a continuous wave (CW) signal at 28 GHz. In general, the presented setup and procedures are applicable to arbitrary frequencies within the extremely large frequency range (27.5 to 75 GHz) of the NRPM-A66 antenna modules.

The horn antenna's aperture has a diagonal of 6.5 cm length. According to criterion (9) the far-field starts 80 cm from the horn antenna at 28 GHz. As can be seen from Figure 4, this criterion is not met with the chosen setup. This is, however, no limitation for the presented applications, since they are based on the comparison of the DUT and a golden device. The presented applications prove the excellent capabilities of such a compact setup.

Figure 5 shows a photograph of the setup.

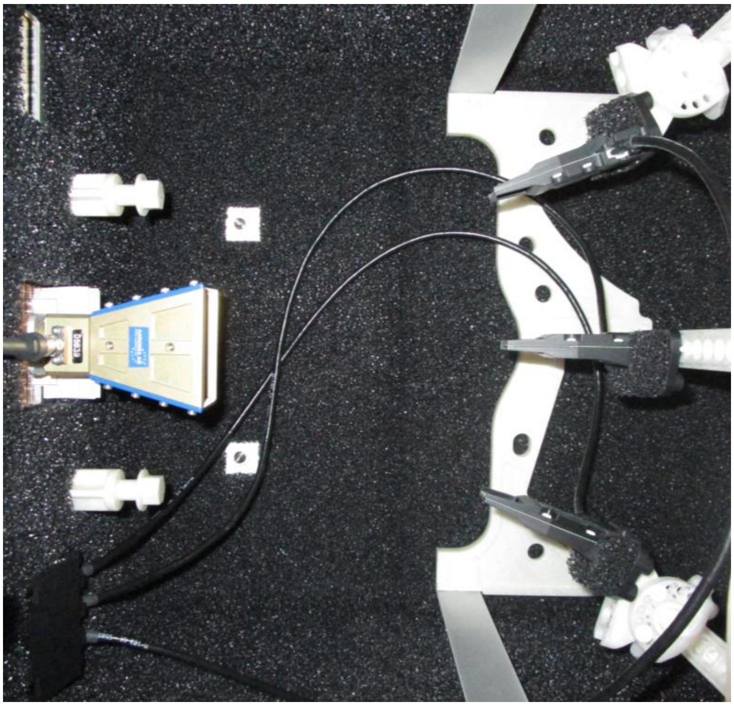


Figure 5: TS7124 RF shielded box, horn antenna and 3 NRPM-A66 antenna modules, mounted on a TS-F24-AH1 half antenna ring and TS-F2X-VH4 adapters.

To give a first and illustrative impression on possible measurements, Figure 6 shows the powers received by individual NRPM-A66 antenna modules as the horn antenna is steered to various directions. For angles around -18°, the left NRPM-A66 antenna module (red curve) shows the highest received power. As the horn antenna is steered towards 0° and eventually to positive angles, the center NRPM-A66 antenna module (green curve) and eventually the right NRPM-A66 antenna module (blue curve) receive the maximum power.

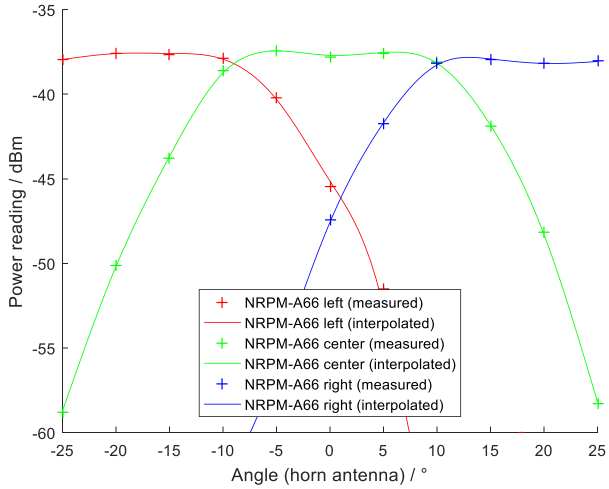


Figure 6: Power readings obtained with the NRPM-A66 antenna modules arranged for polarization-matching

The NRPM-A66 antenna modules are expected to be co-polarized to the waves that are radiated by the horn antenna. The left plot in Figure 7 shows the same measurement data as the plot in Figure 6 but with the y-axis extended to lower powers as compared to Figure 6. The right plot in Figure 7 shows the power received by the NRPM-A66 antenna modules rotated by 90° and thus expected to be cross-polarized with respect to the horn antenna.

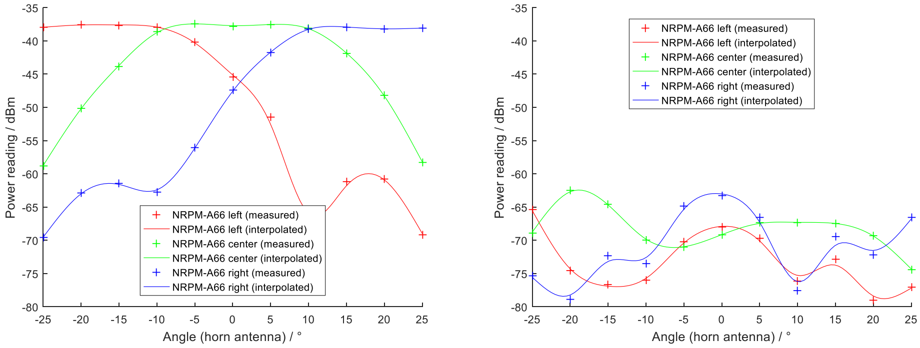


Figure 7: Power readings obtained with the NRPM-A66 antenna modules arranged to be co-polarized (left) and cross-polarized (right) with respect to the horn antenna.

5 Applications

In this section, two applications are described. The first one is the verification of the power level and the radiation pattern of a DUT in 5.1.

The second one is the verification of the accuracy of beam steering in 5.2.

In 5.3, points are discussed that should be considered before implementing a particular setup.

5.1 Verifying the power level and the radiation pattern of a DUT

Properties of the DUT

- The DUT operates in transmit mode.
- The beam of the DUT can be steered to different azimuth angles.

Task

- Verify that the power level and the radiation pattern of the DUT are within the defined boundaries

Approach

- Use a golden device to obtain reference values
- Measure the radiation of the DUT and compare the readings to the reference

5.1.1 How to measure the golden device?

1. Put the golden device in place.
2. For each of the defined beam directions:
   a) Steer the beam to the defined direction.
   b) Record the power readings of all NRPM-A66 antenna modules.
3. Remove the golden device.

5.1.2 How to measure the DUT?

1. Put the DUT in place. Make sure that the location and the orientation are the same as with the golden device.
2. For each of the defined beam directions:
   a) Steer the beam to the defined direction.
   b) Record the power readings of all NRPM-A66 antenna modules.

5.1.3 How to evaluate the measured data?

The data obtained for the DUT is compared to the respective reference data obtained using the golden device. Depending on the deviations, the test is considered as passed or failed.

5.1.4 Measurement results

Each of the following figures contains an illustration of the direction to which the horn antenna is pointing and the corresponding display in the R&S®Power Viewer Plus software.

As the horn antenna points towards the left NRPM-A66 antenna module (beam is directed to -18°, Figure 8), the corresponding power reading is maximum. As expected, the reading of the center antenna is lower, and that of the right antenna is minimum.

The opposite is true for the case when the horn antenna points to the right NRPM-A66 antenna module (beam is directed to 18°, Figure 10).

Rotating the horn antenna towards the center NRPM-A66 antenna module (beam is directed to 0°, Figure 9) results in the maximum power reading for the center NRPM-A66 antenna module and lower readings for the left and the right NRPM-A66 antenna module.

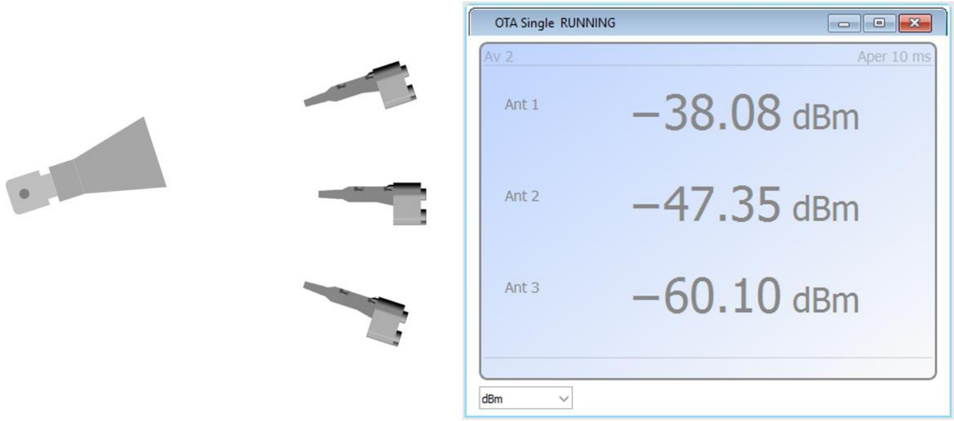


Figure 8: Horn antenna directed to the left NRPM-A66 antenna module

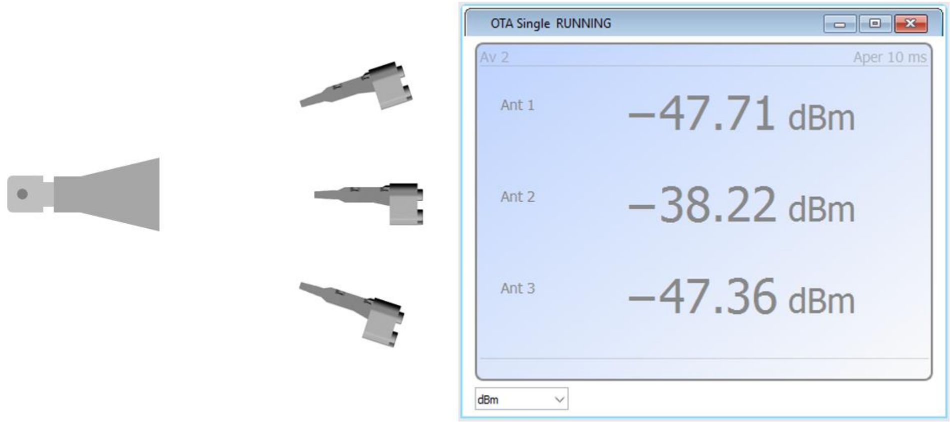


Figure 9: Horn antenna directed to the center NRPM-A66 antenna module

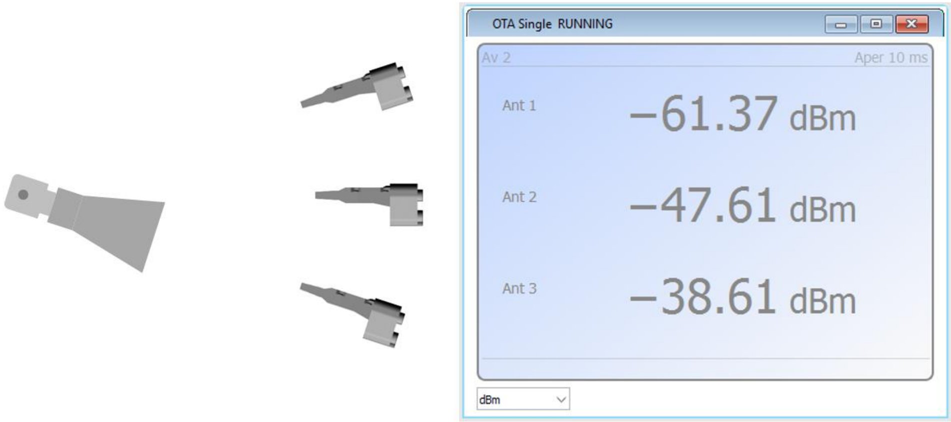


Figure 10: Horn antenna directed to the right NRPM-A66 antenna module

5.1.5 Prerequisites

It is advisable to consider the points mentioned in 5.3.

5.1.6 Ideas for modifications

- If more spatial samples with respect to azimuth are desired, additional NRPM-A66 antenna modules can be used.
- If information on the power distribution with respect to elevation is desired, additional NRPM-A66 antenna modules can be placed below or above the existing NRPM-A66 antenna modules.
- Up to 4 NRPM3 sensor modules and thus 12 NRPM-A66 antenna modules are supported by the R&S®Power Viewer Plus software. This limit does not apply when communicating with the NRPM3 sensor modules via VISA.

5.2 Verifying the accuracy of beam steering

Properties of the DUT

- The DUT operates in transmit mode.
- The beam of the DUT can be steered to different azimuth angles.

Task

- Verify that the beam of the DUT points to the intended direction (even when this direction is not in line with one of the 3 NRPM-A66 antenna modules).

Approach

- Obtain a reference pattern using a golden device.
- Put the DUT in place, take a single set of power measurements and determine the beam direction by fitting the reference pattern to the measured powers.

The prerequisites given in 5.2.5 have to be fulfilled.

5.2.1 How to measure the golden device?

The golden device–horn antenna A in this case–is put in place. It is steered to different azimuth angles. For each of those angles, the power reading of the center NRPM-A66 antenna module is recorded. Those power readings, when processed according to (4), yield samples of the reference radiation pattern. For the horn antenna, angles between -25° and 25° in steps of 5° have been chosen. The measured values and the result of an interpolation are shown in Figure 11.

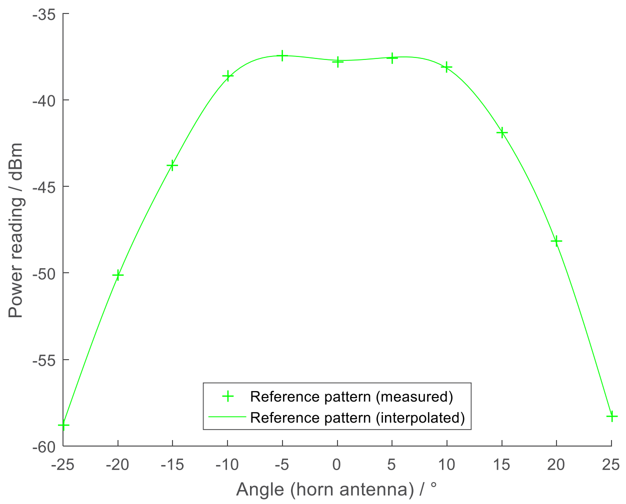


Figure 11: Reference pattern obtained with horn antenna A and the center NRPM-A66 antenna module

Note that the horn antenna is not rotated about its phase center, which is the point from which the radiation is said to emanate. Note also that the NRPM-A66 antenna modules are not in the far-field of the horn antenna, which begins in a distance of approximately 80 cm from the horn antenna at a frequency of 28 GHz according to (9). Therefore, the obtained radiation pattern is not necessarily the horn antenna's far-field radiation pattern, but a characteristic pattern that allows to find the horn antenna's beam direction.

5.2.2 How to measure the DUT?

1. Put the DUT in place. Make sure that the location and the orientation are the same as with the golden device.
2. For each of the defined beam directions:
   a) Steer the beam to the defined direction.
   b) Record the power readings P_1, P_2 and P_3 of the left, the center and the right NRPM-A66 antenna module, respectively.

5.2.3 How to evaluate the measured data?

The evaluation is identical for all of the considered beam directions of the DUT. P_1, P_2 and P_3 denote the powers measured by the three NRPM-A66 antenna modules located at equal distances and at azimuth angles ϕ_1, ϕ_2 and ϕ_3 as seen from the DUT. $P_{\mathrm{ref}}(\phi)$ denotes the reference pattern (the green solid curve in Figure 11).

An estimate of the beam direction of the DUT is that angle ϕ_{est} that minimizes the cost function

$$f = (P_1 - P_{\mathrm{ref}}(\phi_1 - \phi_{\mathrm{est}}))^2 + (P_2 - P_{\mathrm{ref}}(\phi_2 - \phi_{\mathrm{est}}))^2 + (P_3 - P_{\mathrm{ref}}(\phi_3 - \phi_{\mathrm{est}}))^2, \quad (10)$$

i.e. that best fits the reference pattern to the measured values in a least squares sense.

The minimization is carried out with respect to the physical quantity power in (milli)watts (and not for instance in the logarithmic unit dBm). A power level P_{dBm} stated in dBm can be converted to the corresponding power P in milliwatts according to

$$P = 10^{P_{\mathrm{dBm}}/10}\ \mathrm{mW}. \quad (11)$$

Once the actual beam direction is determined, it is compared to the defined beam direction. Depending on the deviation, the test is considered passed or failed.

5.2.4 Measurement results

Each of the plots in the following figures corresponds to a particular beam direction (azimuth angles of -10°, -5°, 0°, 5° and 10°).

Each plot shows the identical reference pattern obtained with the golden device–horn antenna A–in green.

The red diamonds represent the power readings P_1, P_2 and P_3 of the left, center and right NRPM-A66 antenna modules, respectively, obtained when the DUT–horn antenna B–was steered to a certain azimuth angle.

The red curves are copies of the green reference curves, shifted by those angles ϕ_{est} that best fit the reference pattern to the powers measured by the three NRPM-A66 antenna modules for the different beam directions.

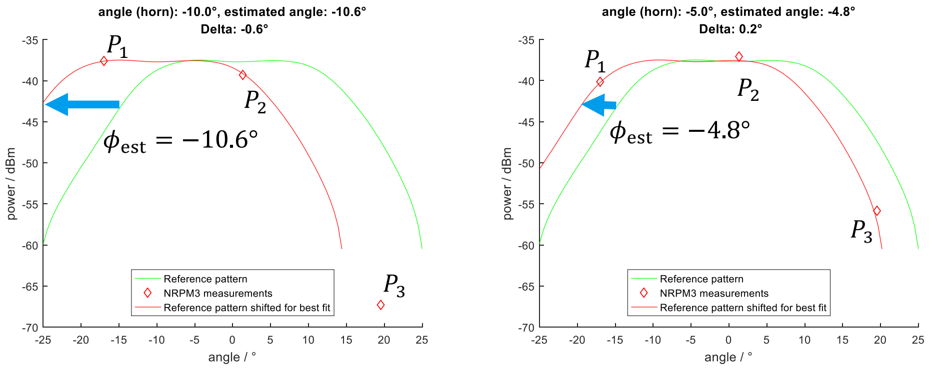


Figure 12: Estimates of the angle of rotation for the DUT rotated to the left by 10° (left plot) and 5° (right plot)

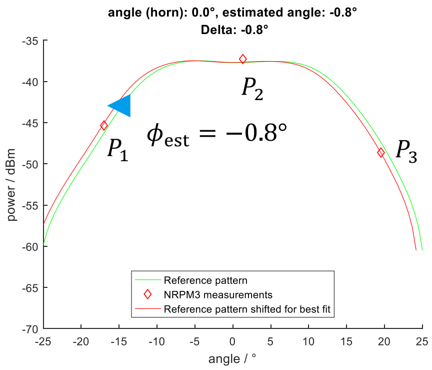


Figure 13: Estimate of the angle of rotation for the unrotated DUT

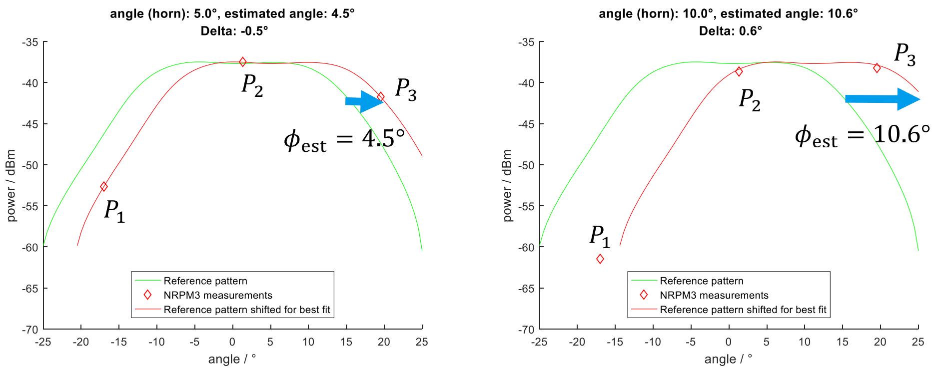


Figure 14: Estimates of the angle of rotation for the DUT rotated to the right by 5° (left plot) and 10° (right plot)

As can be seen from the plots, the estimation of the beam direction of the DUT, based on a single set of measurements with three spatially separated NRPM-A66 antenna modules, is in very good agreement with the true beam direction of the DUT.

5.2.5 Prerequisites

- In equation (10), the only degree of freedom is ϕ_{est}. The estimation of the beam direction might degrade as the radiated power differs between the golden device and the DUT. It has to be ensured that the power levels are sufficiently similar. In case this is not possible, the ideas given in 5.2.6 might help to overcome this issue. The maximum tolerable deviation depends on the particular pattern and the desired accuracy of the estimation of the beam direction.
- The presented approach is based on best-fitting a known pattern to a set of measured values. For the used DUT–a horn antenna–the pattern is invariable irrespective of what angle the horn antenna is rotated to. The only feature that varies as the horn antenna is rotated is the beam direction.
  For antenna arrays it is common that while the beam is steered off the direction normal to the antenna elements, the beamwidth increases and the maximum gain decreases. That means that not only the beam direction changes, but also other characteristics of the pattern. In such a case it might be advantageous to apply one of the ideas given in 5.2.6.
- The number of NRPM-A66 antenna modules and their locations have to be chosen appropriately with regard to the number of unknowns to be estimated and the particular pattern of the DUT. It has to be ensured that a sufficient number of NRPM-A66 antenna modules is covered by the DUTs beam so that there are enough measured values to obtain robust fitting. The number of unknowns is 1 in case of applying equation (10), but it might be greater than 1 when other ways of estimating the beam direction are applied (s. 5.2.6).
- The power reading of an NRPM-A66 antenna module is influenced by the impinging power as well as the calibration of the NRPM-A66 antenna module. In order to maximize the accuracy of the angle estimation, the power readings of all used NRPM-A66 antenna modules have to be sufficiently similar for equal impinging powers. The maximum allowable difference depends on the actual pattern of the DUT. The similarity of the power readings can be checked by mounting the relevant NRPM-A66 antenna modules at identical positions with identical orientations one after the other. For each of the NRPM-A66 antenna modules, the power reading is recorded while the DUT is radiating, enabling a comparison of the NRPM-A66 antenna modules. In case the deviation is too high for a given application, the differences can be used as offsets for a relative calibration. Due to the extraordinary linearity of the NRPM-A66 antenna modules, the offsets are valid for the entire power measurement range of the NRPM-A66 antenna modules. In order for the mentioned procedures to be meaningful, it is necessary to provide each of the NRPM-A66 antenna modules with identical signals and identical powers. It is therefore advisable to place the NRPM-A66 antenna modules in such a region relative to the DUT where a slight variation of the actual positions of the NRPM-A66 antenna modules yields only a small variation in the received power.

5.2.6 Adaptations for 5G devices

- In case it is necessary to obtain resolution with respect to elevation, additional NRPM-A66 antenna modules can be placed below or above the existing NRPM-

A66 antenna modules. Then, the reference pattern has to be determined in two dimensions (azimuth and elevation), and the evaluation of the elevation angle has to be incorporated into the cost function.

- Depending on the expected variation of the power radiated by individual DUTs, it might be necessary to increase the number of degrees of freedom in the cost function (10) in order to obtain the highest estimation accuracy. This can be accomplished by incorporating a factor a into (10) that is applied to the reference pattern. The cost function then reads as
$f = (P_1 - aP_{\mathrm{ref}}(\phi_1 - \phi_{\mathrm{est}}))^2 + (P_2 - aP_{\mathrm{ref}}(\phi_2 - \phi_{\mathrm{est}}))^2 + (P_3 - aP_{\mathrm{ref}}(\phi_3 - \phi_{\mathrm{est}}))^2$
and is a more realistic representation of the measurement situation in case the power level varies between individual DUTs. Therefore, minimizing this cost function–with respect to a and ϕ_{est}–yields higher accuracy in estimating the beam direction. The resulting value of a is an estimation of the power radiated by the DUT with respect to the power radiated by the golden device.

- There are several ways to cope with patterns whose characteristics change as the beam is steered to different beam directions.
One of them is to record a set of reference patterns for different beam directions and approximate them by a two-dimensional analytical expression, where the two dimensions are the beam direction and the observation angle. Useful characteristics for the analytical description of the pattern might be the maximum gain and the beamwidth. Both parameters generally change as an antenna array is steered to different angles. The estimation of the beam direction is done by formulating a two-dimensional cost function and minimizing it with respect to the beam direction. In order to determine the reference patterns, the beam of the DUT has to be steered to different directions. For each direction, the pattern is determined by either rotating the DUT or orbiting the used NRPM-A66 antenna around the DUT.
Another option is using a higher number of NRPM-A66 antenna modules. When arranged with sufficiently small angular spacing, the maximum value and thus the beam direction can be determined immediately or if necessary after an interpolation. Proceeding this way renders the use of a golden device unnecessary.

5.3 Points to consider

Before choosing a setup for a particular application, at least the following aspects should be considered in order to get the maximum benefit from the measurements. Those aspects are strongly related to the theoretical considerations in section 3.

5.3.1 Appropriate distance between DUT und NRPM-A66 antenna modules

In order to obtain the radiated power or far-field characteristics of the DUT as e.g. the far-field pattern of the DUT according to (4), the DUT and the NRPM-A66 antenna modules have to be located in each other's far-field.

For short distances between the DUT and the NRPM-A66 antenna modules, the Friis equation might not predict the path loss very well. In order to have equal–even though unknown–path losses between the DUT and each of the NRPM-A66 antenna modules, it is advisable to choose equal distances.

In the presented applications, the measurements are done in the near field. This is no limitation, since the measured values are compared to those obtained with a golden device in the same setup.

In case of doubts about the proper distance between the DUT and the NRPM-A66 antenna modules, it is advisable to start with a large distance and check whether the same conclusions can be drawn from measurements that are taken with smaller distances. Further discussion on this topic can be found in [3].

5.3.2 Appropriate environment

If the NRPM-A66 antenna modules are used to measure how much power is radiated by the DUT to particular spatial directions, the measurements are degraded as

- not only the line-of-sight signal but also echoes from other objects or
- interfering signals with frequencies for which the NRPM-A66 antenna modules are sensitive

reach the NRPM-A66 antenna modules, as also addressed in 3.2. Therefore, it must be ensured that the levels of echoes and interfering signals are sufficiently low. This can be accomplished using absorbers and shielding.

The level of interfering signals can be determined by measurements with a turned-off DUT. Depending on the level of interference, it might be necessary to shield the test setup from interfering signals. The TS7124 RF shielded box is a perfect solution for this problem.

Echoes can be avoided by placing the measurement setup inside an anechoic chamber or by removing objects not needed for the measurement sufficiently far from the test setup. Those objects that are necessary parts of the setup may have to be covered with absorbing material appropriate for the relevant frequencies. A TS7124 RF shielded box shields the setup from interferers and suppresses unwanted echoes.

5.3.3 Orientation of the NRPM-A66 antenna modules

The NRPM-A66 antenna modules are linearly polarized. It has to be kept in mind that the power reading of the NRPM sensor module refers to only that part of the incident wave that is associated with the polarization direction of the NRPM-A66 antenna. Figure 7 clearly shows the effect of rotating the NRPM-A66 antenna modules by 90° about their boresight on the power readings.

The NRPM-A66 antenna modules have to be oriented such that they are co-polarized to the desired polarization of the incident wave. The NRPM-A66 antenna module has maximum sensitivity when the E field vector of the incident wave is parallel to the substrate of the NRPM-A66 antenna module.

In order to obtain consistent results when measuring multiple DUTs, the relative locations and orientations of the golden device, the DUTs and the NRPM-A66 antenna modules have to be kept fixed.

A versatile means for fixing the NRPM-A66 antenna modules are the TS-F24-AR antenna rings or the TS-F24-AH1 half antenna rings, if necessary with TS-F2X-VH4 adapters (s. Figure 15) to adjust the NRPM-A66 antenna module's tilt angle. Apart from that, TS-F24-AH2 antenna holders (s. Figure 15) are available that can e.g. be directly attached to the front and back walls of a TS7124 RF shielded box.

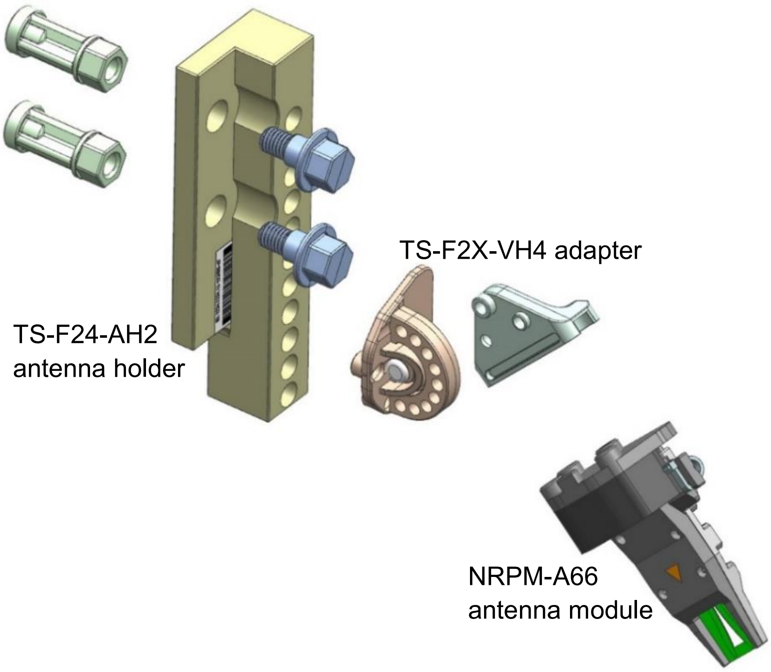


Figure 15: TS-F24-AH2 antenna holders, TS-F2X-VH4 adapter and NRPM-A66 antenna module

5.3.4 Influence of modulated signals

Measurements can be done with CW signals as well as with modulated signals. In order to obtain the most reliable and comparable results, the signals of the golden device and the DUTs should be identical.

5.3.5 Ways of controlling the NRPM sensor module

There are several ways of controlling the NRPM sensor module from a computer. One particularly convenient way is using the R&S®Power Viewer Plus software [4]. However, any programming language that supports VISA can be used. Detailed information on controlling the NRPM sensor module can be found in the NRPM User Manual [5].

6 References

[1] **Balanis, Constantine A.**, *Antenna Theory*, Wiley, 2005

[2] **Friis, Harald T.**, "A Note on a Simple Transmission Formula", *Proceedings of the I.R.E. and Waves and Electrons*, May 1946

[3] R4-1706859 “Minimum Measurement Distance at 28GHz”, Rohde & Schwarz, 3GPP TSG RAN WG4 Meeting NR#2 AH

[4] https://www.rohde-schwarz.com/software/nrpm/

[5] **Rohde & Schwarz**, *NRPM OTA Power Measurement Solution User Manual*

7 Ordering Information

Please visit the product websites at www.rohde-schwarz.com for comprehensive ordering information ("Options") on the following Rohde & Schwarz products:

- R&S®NRPM3 (1425.8563.02)
- R&S®NRPM-A66 (1425.8740.02)
- R&S®NRPM-ZD3 (1425.8786.02)
- R&S®TS7124 (1525.8564.02 / .12, 1525.8587.02 / .12)
- R&S®TS-F24-AR (1525.8906.02)
- R&S®TS-F24-AH1 (1525.8887.02)
- R&S®TS-F24-AH2 (1525.8893.02)
- R&S®TS-F2X-VH4 (1525.8758.02)

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, this independent company has an extensive sales and service network and is present in more than 70 countries.

The electronics group is among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

Regional contact

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1 888 TEST RSA (1 888 837 87 72)
customer.support@rsa.rohde-schwarz.com

Latin America
+1 410 910 79 88
customersupport.la@rohde-schwarz.com

Asia Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86 800 810 82 28 |+86 400 650 58 96
customersupport.china@rohde-schwarz.com

Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management ISO 9001

Certified Environmental Management ISO 14001

This and the supplied programs may only be used subject to the conditions of use set forth in the download area of the Rohde & Schwarz website.

1GP118_0E

1: 3573.7380.02/02.05/EN/

Rohde & Schwarz GmbH & Co. KG
Mühldorfstraße 15 | 81671 Munich, Germany
Phone + 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com

Virtual Cable Calibration for OTA Testing of 5G mmWave Devices

Taro Eichler, Ute Philipp, Heinz Mellein and Lorenz Rädler
Rohde & Schwarz, Munich, Germany

5G New Radio (NR) is the first standard to use the mmWave frequency region for highest data transfer rates. The highly integrated front-ends and array antennas necessitate advanced over-the-air (OTA) testing methods and new RF test metrics for assessing current and future mobile communication. Such test metrics include virtual cable calibration (VCC), which is mandatory for reproducible and reliable OTA throughput testing. For performance tests where fading is emulated—such as radio resource management (RRM) conformance and demodulation testing—the VCC method is crucial to assess defined antenna correlations with minimal crosstalk from the OTA link. The measurement results presented in this article demonstrate the proposed concepts for VCC can be applied to ensure device compliance to the 3GPP standard.

5G has pioneered the use of mmWave frequencies with large bandwidths to enable the reliable, high data transmission rates necessary for demanding real-time applications with low latencies. To increase the system capacity, as well as data rate, and to handle diverse services, 5G NR deploys at much higher frequencies and bandwidths compared to LTE, as well as very high configuration flexibility. A signal bandwidth of up to 400 MHz can be used in 5G NR, compared to 20 MHz in LTE. Since the spectrum below 6 GHz is already used extensively, high bandwidths are only available at higher frequencies, with two mmWave frequency ranges identified (see ***Figure 1***). The overall bands used for 5G NR are:

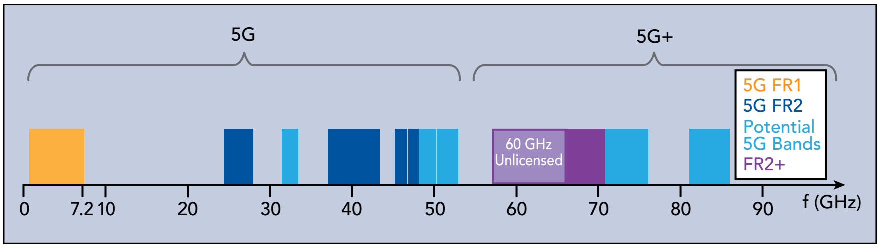
- Frequency range 1 (FR1) spans frequencies from 410 MHz to 7.125 GHz.
- Frequency range 2 (FR2) is the spectrum from 24.25 to 52.6 GHz.
- For future extension, the frequency range designated FR2+ covers 52.6 to 71 GHz.

5G technologies such as massive MIMO and beamforming further increase the complexity of testing user equipment (UE), as defined in 3GPP TS 38.521-4,[1] where highly integrated antennas require radiated test methods.

VCC FOR 5G MIMO

One of the biggest challenges for test and measurement manufacturers is implementing standardized evaluation and verification methods for UE under repeatable and realistic conditions, which are also reliable with mass production processes. For LTE and 5G NR FR1 tests, conductive testing methods are the norm for MIMO devices. During testing, the antennas of the device under test (DUT) are disconnected from the antenna ports, and the DUT is directly connected to the test system using a coaxial cable (see ***Figure 2***). However, for testing UEs in the FR2 bands, this approach is not practical: the large number of integrated antennas on the UE for spatial multiplexing and beamforming requires testing OTA, without cable connections.

OTA testing introduces challenges. The transmitted signal propagating in the air channel, represented by



▲ **Fig. 1 Designated 5G NR frequency bands (FR1, FR2 and FR2+) and possible future bands.**

OTA Channel A in Figure 2, is affected by other signals and noise, becoming distorted. To have defined and reproducible conditions similar to conductive testing, the effects of the OTA channel must be eliminated. One approach to solve this issue is to calculate the unknown transfer matrix A by accounting for the complete OTA environment, including the transmitter and receiver antenna characteristics. This approach is complex and, in most cases, not possible: UE manufacturers are not required to give detailed information about their antenna characteristics, including the phase information required to apply this method.

An alternative approach, described here, equalizes the channel matrix using only the Reference Signal Received Power per Branch (RSRP-B) feedback parameters, which can be retrieved from an FR2 UE per the 3GPP standards. This enables having a quasi-conducted or "virtual cable" connection or "virtual cabling" in an FR2 radiated test environment.[2] The approach lays the foundation for practical 5G UE performance testing for maximum throughput, as well as testing under various channel conditions, such as fading. An equalized channel is also mandatory for conformance tests with fading, which are needed for RRM tests.

SIGNAL QUALITY USING RSRP-B FEEDBACK

The secondary synchronization RSRP-B (SS-RSRP-B) is defined as the linear average power per branch, in watts, of the resource elements that carry secondary synchronization signals. For FR2, the SS-RSRP-B is measured for each receiver branch based on the combined signal from the antenna elements corresponding to the receiver branch. The RSRP-B is an important parameter to assess signal quality, and it is the UE's task to calculate the SS-RSRP-B and fulfill the accuracy requirements. The power per resource element is determined from the energy received during the useful part of the symbol, i.e., excluding the cyclic prefix. In 5G NR, RSRP measurement is performed and reported at layer 1, the physical layer, and layer 3, the radio resource control (RRC) layer. For example, a 5G capable device can provide SS-RSRP measurements at layer 1 when sending channel state information and at layer 3 when sending an RRC protocol measurement report to the next-generation node B (gNB).

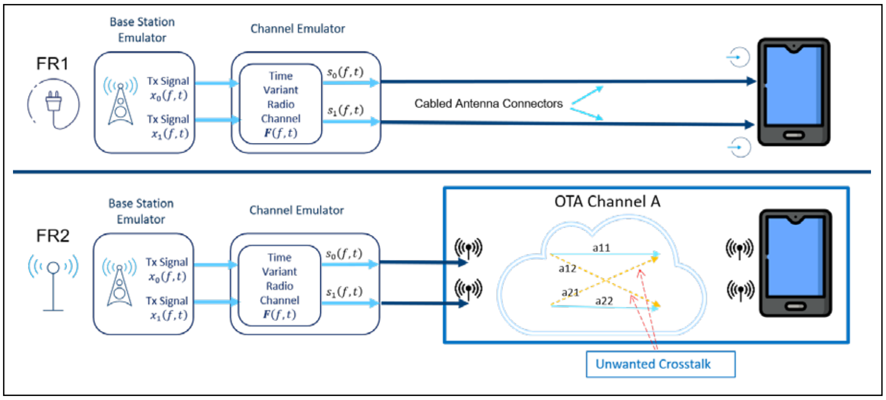
The level 1 measurements are relevant for the following implementation, and the SS-RSRP-B reporting range is defined from -140 to -40 dBm with 1 dB resolution. The RSRP-B is the linear average power measured at each receiver branch of the DUT. 3GPP requires the 5G NR FR2 device to support RSRP-B, which enables the determination of a calibration matrix which can equalize the channel.

CALIBRATION METHOD

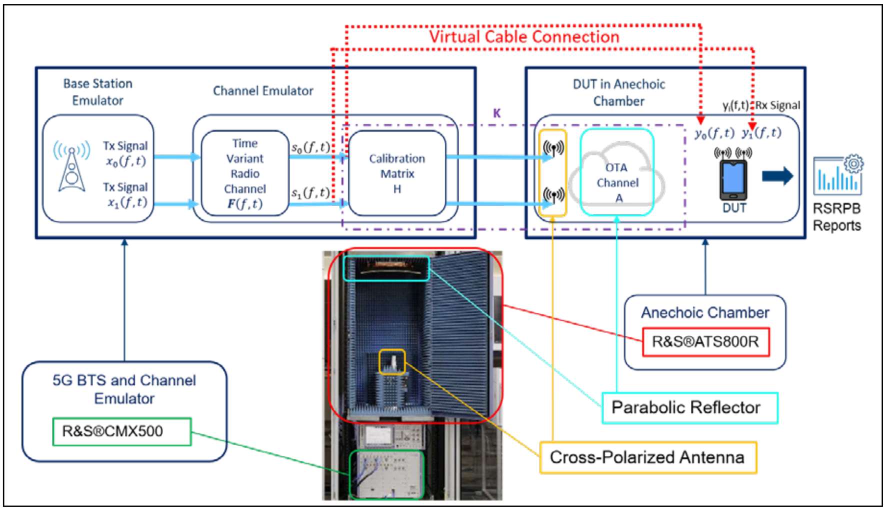
As propagation conditions and antenna characteristics are the most important factors for field performance of MIMO devices, mobile receiver performance tests must include these parameters. These conditions are generally simulated through a fading simulator or channel emulator. The channel emulator is a measuring instrument for reproducing the actual radio wave propagation environment described by the matrix F(f,t), which can include dynamic scenarios in moving environments. It reproduces the fading environment defined by 3GPP and the virtual environment of multiple MIMO channels.

As shown in ***Figure 3***, the UE is placed in a controlled wireless environment, such as an anechoic chamber, to minimize the distortions caused by multipath propagation and reflection. The setup in the figure shows the case of 2 × 2 MIMO; however, the concept can be extended to N × N, where N > 2.

For development and conformance tests, the base station emulator simulates a mobile 5G base station's operation, enabling the DUT to perform a network entry procedure and establish a communication link. The modulated signals then pass through the channel emu-



▲ **Fig. 2 UE testing for 2 x 2 MIMO with channel fading, showing connected (FR1) and OTA (FR2) approaches. OTA testing introduces unwanted crosstalk.**



▲ **Fig. 3 Setup for calibrating 2 x 2 MIMO OTA measurements.**

lator with various fading and propagation parameters, simulating real life scenarios.

In the case of a perfect conducted situation without any crosstalk between the cable branches, the OTA channel matrix A is identical to the unity matrix. With the OTA measurement, the objective of the calibration procedure is to determine the calibration matrix H so the channel K, which is the combination of the calibration matrix H and the OTA channel matrix A, is as close as possible to the unity matrix: $K = A \times H \approx I_2$. After calibration, the combined channel matrix K will approximately equal the unity matrix, effectively establishing a virtual cable connection with s_0 and s_1 connected directly to the UE antennas.

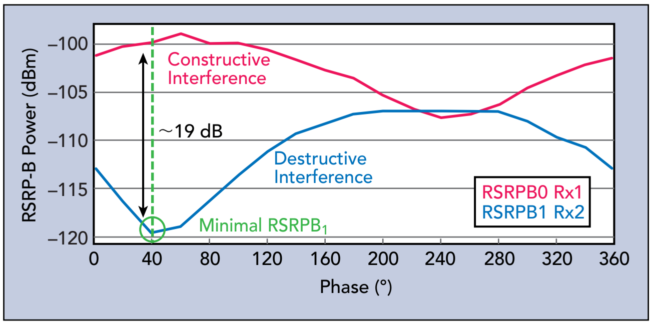
DEMONSTRATION RESULTS

To demonstrate the procedure, a 5G NR signal at 39 GHz (band n260) was generated using a 5G radio communication tester as a base station emulator. The precoding matrix H was generated using the channel emulator of the tester to simulate fading. The resulting signal was transmitted via two cross-polarized antennas in an anechoic chamber containing a compact antenna test range (CATR) reflector. A CATR has a parabolic reflector with a feed antenna placed at its single focal point to transform a spherical wavefront into a planar wave and vice versa. In this case, the plane wave impinges on the DUT, which returns the RSRP-B value for each branch, i.e., corresponding to its two antennas.

The VCC procedure requires the presence of a signaling connection between the DUT and base station emulator. To find a suitable matrix H which fulfills the requirement for quasi-conducted conditions ($K \approx I_2$), the matrix H is defined so the phase applied for the contributions from the two input signals can be controlled by a single complex factor for each branch (i.e., the secondary diagonal elements). The calibration itself comprises three major steps: initialization of the gain factor, search for the optimal phase and final tuning of the gain. The calibration of the two branches can be carried out independently by disabling the input signal, which is currently not calibrated. This process can be followed by an optional step of branch equalization.

Figure 4 shows an example measurement sweeping the phase multiplier for the first branch. The top RSRP-B0 curve represents the measured power at antenna Rx1 of the DUT; the bottom RSRP-B1 curve represents the power at antenna Rx2 of the DUT, the crosstalk from Tx1. 3GPP specifies that the crosstalk between the virtual cables should be less than 12 dB.[1,3] The measurement shows the peak isolation is 19 dB, which exceeds the 3GPP requirement for a virtual cable.

The calibration method implemented in the test system uses "intelligent" search algorithms to determine the channel parameters in the minimum time, which is crucial for cost-effective device verification. The approach and results confirms this method is an effective way to implement a quasi-connected testing environment with reproducible and defined channel conditions for throughput performance measurements and assessing performance under fading conditions.



▲ **Fig. 4 Commercial UE measurement in an anechoic chamber, showing RSRP-B power levels vs. calibration phase for one branch.**

CONCLUSION

Although 3GPP specifies crosstalk limits between virtual cables, it does not specify the calibration method to be used. Repositioning a DUT could, in principle, be used; in practice, however, this method would be too slow, not systematic and likely not possible with every DUT. The VCC method described and demonstrated in this article provides a systematic approach with fast convergence to determine the precoding calibration matrix parameters, which will be a crucial component for FR2 testing. For RRM measurements to assess handovers among multiple base stations, the method can be extended using a setup with multiple CATRs.[5]

As 6G research is aiming at frequencies beyond 100 GHz, the trend toward more integration of antennas will continue, requiring the same OTA testing. This same measurement approach can be extended to D-Band (i.e., 110 to 170 GHz)—one of the bands for 6G research.■

ACKNOWLEDGMENT

The authors thank the following Rohde & Schwarz colleagues for fruitful discussions regarding the concepts and measurements: Jimson Eng and Oussema Harguem.

References

1. 3GPP Technical Specification (TS) 38.521-4 Version 16.6.0 NR; User Equipment (UE) Conformance Specification; Radio Transmission and Reception 3rd Generation Partnership Project (3GPP), *3rd Generation Partnership Project (3GPP)*, 2020.
2. Ibid, Appendix H.
3. 3GPP Technical Specification (TS) 38.509 Version 15.9.0 5GS; Special Conformance Testing Functions for User Equipment (UE) 3rd Generation Partnership Project (3GPP), *3rd Generation Partnership Project (3GPP)*, 2020.
4. R&S "5G New Radio: Fundamentals, Procedures, Testing Aspects," January 2021, Online: www.rohde-schwarz.com/5g-ebook.
5. Corbett Rowell, Benoit Derat and Adrian Cardalda Garcia, "Design of a Multiple CATR System for Multiple Angles of Arrival Measurement of 5G mmWave Devices," *Microwave Journal*, March 2021.

Choosing The Right Signal Source for Reliable Measurements

Frank-Werner Thümmler
Rohde & Schwarz, Munich, Germany

The primary goal when measuring a device under test (DUT) is that its measured parameters are unaffected by ambient conditions and unwanted influences from the test setup. While environmental influences are easier to compensate or correct, more effort and know-how may be required with the test setup. This effort increases disproportionately with how precisely the DUT performance is to be determined.

In principle, test and measurement (T&M) setups are often similar. A signal source provides the input signal to the DUT, and the output is measured with a spectrum analyzer, network analyzer or power sensor. For a quick test of the DUT performance, it may be sufficient to simply use this setup and record the measurement; however, more precise data requires more effort. Under certain circumstances, for example, losses or full S-parameters from the test fixture must be considered, as well as the performance of the T&M instrument itself (e.g., phase noise, power supply noise).

In this article we examine the role of the signal source, showing that unwanted influences from an "unsuitable" signal source never yield useful results. Using measurement examples, we show the actual performance of the DUT can only be determined with a "suitable" signal source, i.e., with performance that ensures accurate measurement results that are not falsified by the T&M instrument. As examples, we have selected several components and three typical measurements: harmonics, compression and single sideband (SSB) phase noise (PN). In each example, the performance of the signal source is measured alone and its influence on the measurement result discussed. We refer to typical or measured performance to make it easier to understand how the actual performance of the DUT can be hidden by unwanted factors, such as insufficient harmonic suppression of the signal source.

HARMONIC MEASUREMENTS

When a single CW tone is applied to a nonlinear component such as a power amplifier (PA), unwanted signals will be generated at n multiples of the original frequency, n being the order of the harmonic. To illustrate how the signal source will affect the harmonic performance of a PA, we used two signal sources: 1) an analog RF and microwave signal generator with high harmonic suppression, the suitable signal source. The R&S SMA100B was used for these measurements. 2) An "unsuitable" source with harmonics greater than -30 dBc. The PA used for the measurements was a GaAs design covering 100 MHz to 7 GHz with 27 dBm saturated output power (Psat) and 7 to 8 dB gain.

Figure 1 shows the test setup for the harmonic measurements, using an R&S FSW signal and spectrum analyzer to measure the second harmonic. The suitable

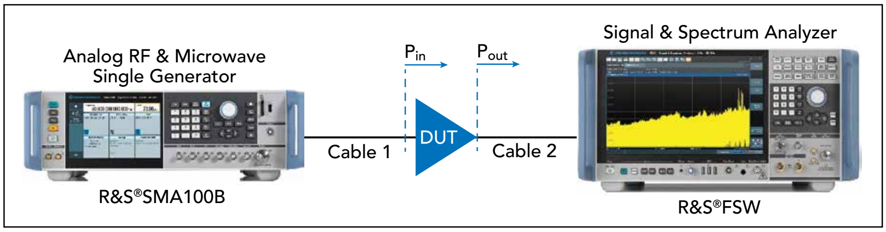


Fig. 1 Test setup for measuring the second harmonic.

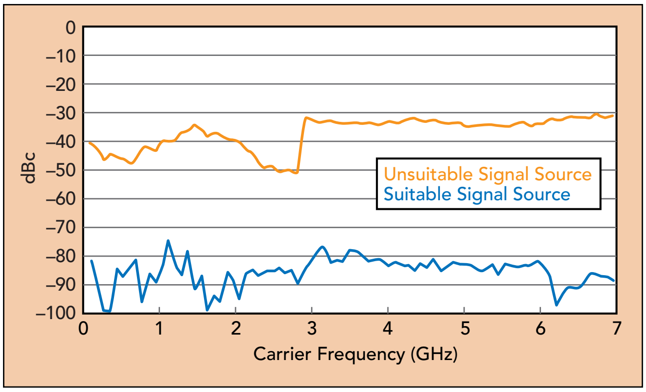


Fig. 2 Second harmonic of the suitable and the unsuitable signal sources.

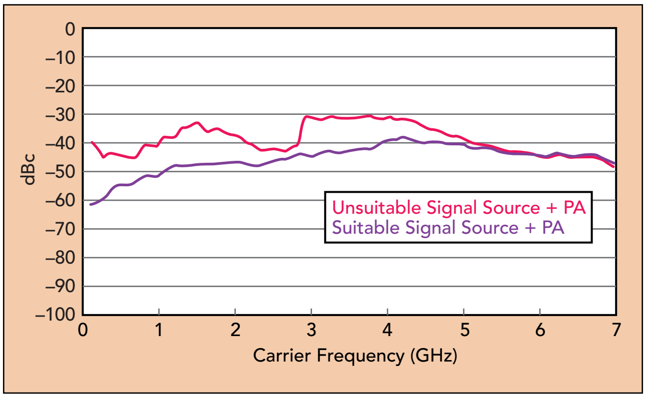


Fig. 3 PA second harmonic measurements with the two signal sources.

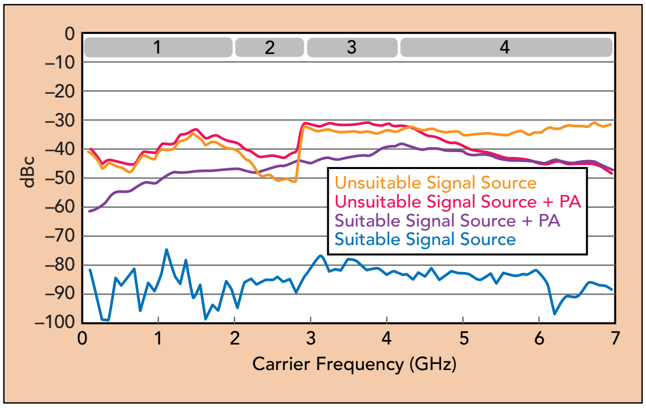


Fig. 4 Comparing second harmonic measurements of the two signal sources and PAs driven by the respective sources.

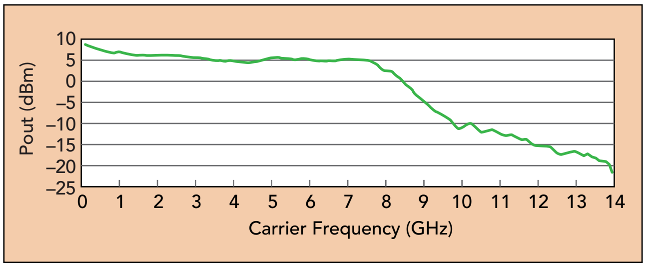


Fig. 5 Measured PA frequency response.

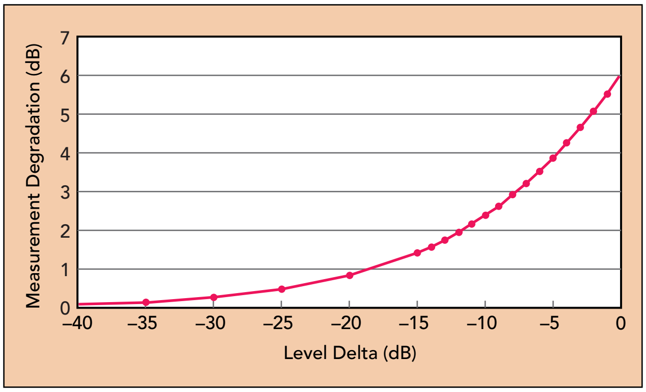


Fig. 6 Measurement degradation caused by the second harmonic of the signal source.

and unsuitable signal sources were used to drive the PA, sweeping from 100 MHz to 7 GHz while keeping the output power (Pout) of the PA constant at approximately 7 dBm. The input power (Pin) was leveled to compensate for the cables and the frequency response of the PA.

The measured second harmonic performance of the two signal sources is plotted in ***Figure 2***, showing a significant difference in harmonic suppression between the suitable and unsuitable sources. Inserting the PA and measuring the harmonic performance with each reveals how the harmonics from the unsuitable signal source make the apparent performance of the PA worse (see ***Figure 3***). The effects of the harmonic performance of the signal sources is clearer by comparing the measurements of the individual sources with the combination in a single plot (see ***Figure 4***), where the sweep is divided into four frequency ranges. Because the harmonic performance of the combination is the vector sum of the harmonics from the signal source and the PA, depending on the relative phase of the two signals, the combined performance is not simply the addition of the magnitudes of the two.

In ranges 1 and 3, the measurement reflects the performance of the unsuitable signal source rather than the PA's harmonics. In range 2, the measurement is closer to the PA's actual performance because the performance of the unsuitable signal source is slightly better than the PA's, so the contribution from the source is less. The interpretation of the measurement in range 4 is trickier. Why is the performance of the unsuitable signal source with the PA better than the source's, when the opposite is expected? The PA's frequency response provides the answer (see ***Figure 5***). Above 8 GHz the gain drops; consequently, as the carrier frequency increases above 4 GHz, the second harmonic of the source is increasingly attenuated by the PA, and the measurement of the second harmonic from the combination gets closer to the PA's actual performance.

The conclusion of the test: to avoid harmonic contributions from the signal source, a source with low harmonics should be used to prevent the source from "distorting" the PA measurement. ***Figure 6*** quantifies how much better the signal source should be to obtain reliable measurements, assuming the worst case where the second harmonics of the signal source and the PA are in phase. For instance, if the second harmonic from the source is 30 dB below the PA's actual

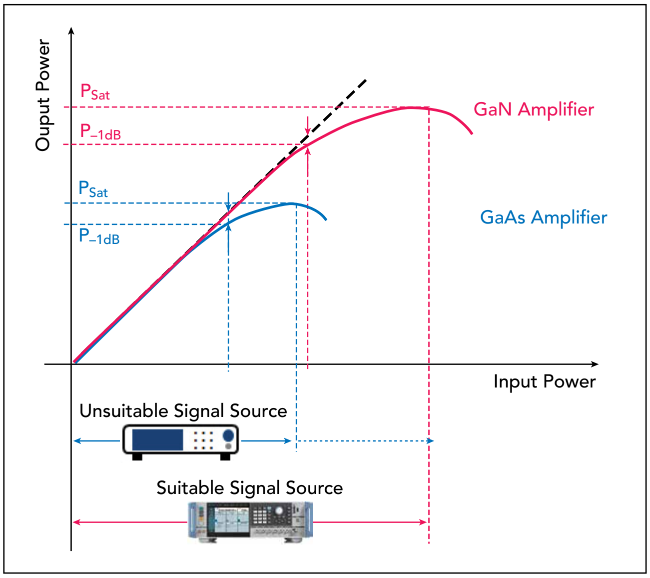


Fig. 7 Input power range required for GaAs and GaN PAs.

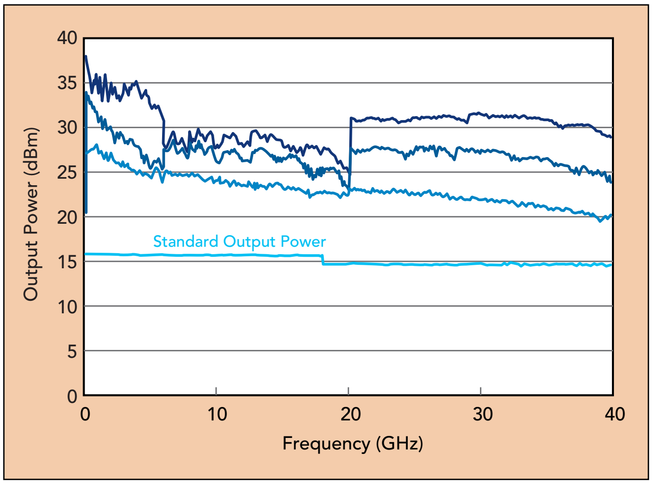


Fig. 8 Output power options of the R&S SMA100B signal generator.

performance, the second harmonic measurement of the PA will be degraded by approximately 0.3 dB, worst case.

COMPRESSION MEASUREMENTS

The 1 dB compression point (P_{1dB}) at the output of a PA defines the boundary between linear and nonlinear behavior. This is the input power where the small-signal gain of the PA is reduced by 1 dB. As the input power increases, the PA becomes increasingly nonlinear and produces significant harmonic distortion and intermodulation products.

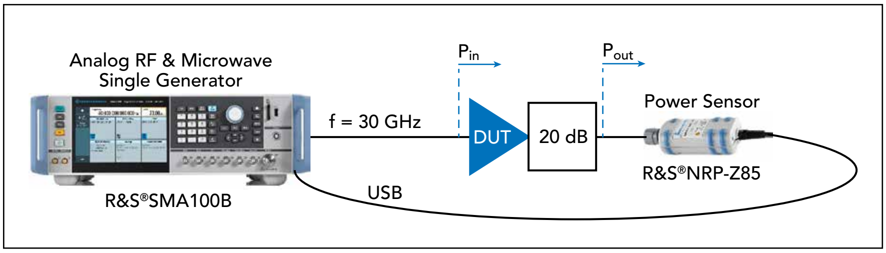


Fig. 9 Test setup for measuring 1 dB compression (P_{1dB}) and saturated (P_{sat}) power.

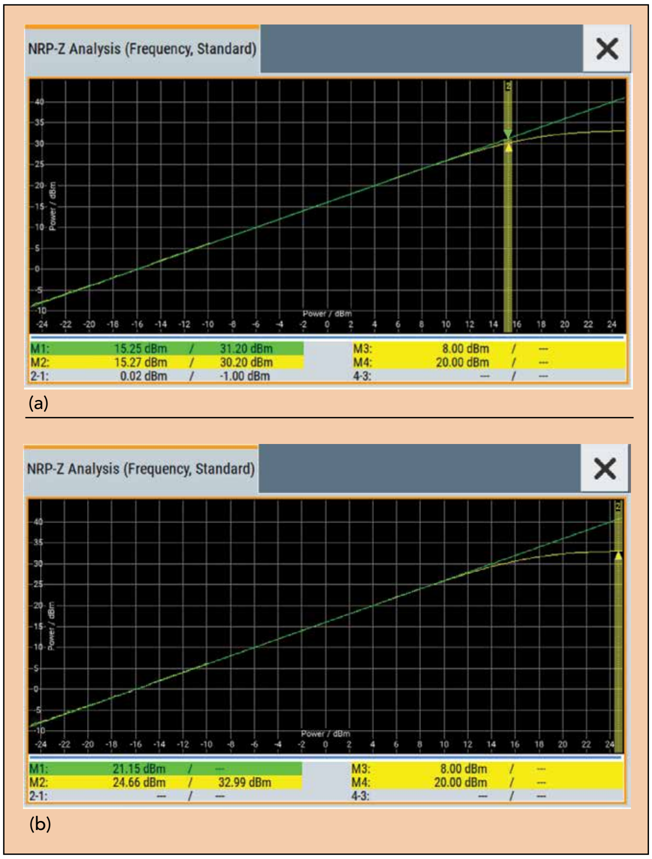


Fig. 10 P_{1dB} (a) and P_{sat} (b) measurements using the suitable signal source.

GaN PAs have higher saturated output power capability than GaAs PAs. Assuming the same gain, the GaN PA will require higher input power to reach P_{1dB} and the maximum or saturated output power, designated P_{sat} (see ***Figure 7***). For measuring the P_{1dB} and P_{sat} of a PA, the signal source must have suitable output power. Addressing this need, Rohde & Schwarz designed the R&S SMA100B to have four output power options (see ***Figure 8***). From 20 GHz to approximately 38 GHz, the R&S SMA100B provides more than 30 dBm—compared to the 16 dBm available from traditional signal sources. Higher output power from the signal source may eliminate the need for an external amplifier at the output of the source to drive the PA into compression.

To illustrate this, ***Figure 9*** shows a typical test setup for measuring P_{1dB} and P_{sat}. The power sensor measures the PA output power and feeds back the measurement result to the signal generator via USB, where it can be graphically displayed on the signal generator's display. The 20 dB attenuator after the PA ensures the power sensor is not overdriven. The DUT is a GaN PA covering 27 to 41 GHz with P_{sat} = 33 dBm and 16 dB gain. The input power (P_{in}) is swept from -25 to +25 dBm at a carrier frequency of 30 GHz. ***Figure 10*** shows the P_{in} versus P_{out} measurements of the PA using a suitable signal source, the yellow trace reflecting the output power and the green trace the linear

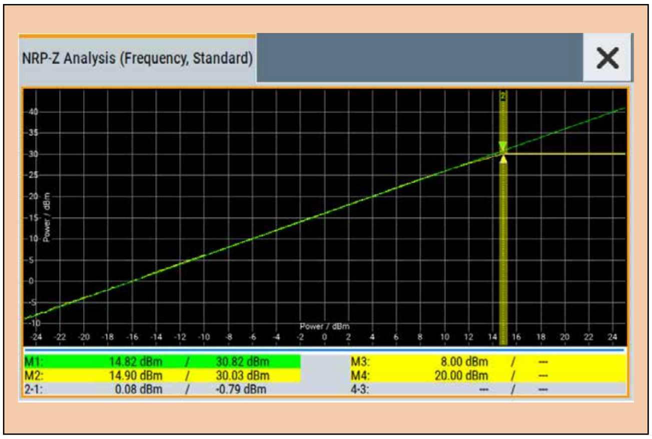


Fig. 11 P_{1dB} **measurement using the unsuitable signal source.**

gain. The y axis accounts for the 20 dB attenuator following the PA. Figure 10a shows a P_{1dB} measurement of 30.2 dBm, and Figure 10b shows a P_{sat} of 33.0 dBm. To measure the P_{sat} of the GaN PA requires P_{in} = ~25 dBm at 30 GHz, which is more power than the capability of many signal sources (see ***Figure 11***). Using a signal source with lower output power, P_{1dB} and P_{sat} cannot be measured directly without an additional amplifier. Figure 11 shows 30.0 dBm maximum output power from the PA, which reflects the shortfall of the signal source rather than the performance of the PA.

These measurements show that using a signal source with sufficient output power simplifies the test setup, enabling higher power P_{1dB} and P_{sat} measurements without requiring an external amplifier that could introduce measurement errors.

SSB PN MEASUREMENTS

Analog and digital circuits rely on pure clock signals. Typical clock signal performance indicators are PN, jitter, wideband noise and spurs. Similarly, a low PN signal source is needed for measuring DUT performance. The residual PN of the DUT determines the PN added by the DUT to the PN of its input signal. Phase-locked loops in high speed digital applications require an input signal with excellent PN performance, i.e., negligible compared to the residual PN of the DUT.

How can designers ensure the signal source meets the requirements for SSB PN? First, the requirements for the DUT should be defined. Next, the data sheet of the signal source should be reviewed to determine whether the SSB PN performance meets the requirements with enough margin to minimize the contribution from the signal source. We illustrate this with measurements showing how suitable and unsuitable signal sources affect SSB PN measurements. The R&S SMA100B is used as the suitable source, with the option for a maximum SSB PN of -128 dBc/Hz at 10 kHz offset from a 10 GHz carrier and typically providing -132 dBc/Hz. The unsuitable signal source has a speci-

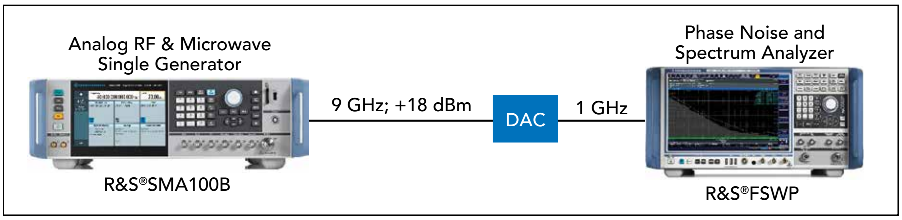


Fig. 12 **Test setup for measuring the SSB PN.**

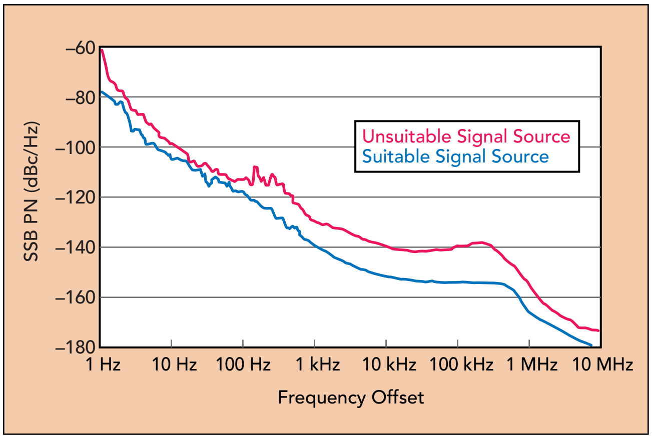


Fig. 13 **Comparing the SSB PN measurements using the two signal sources.**

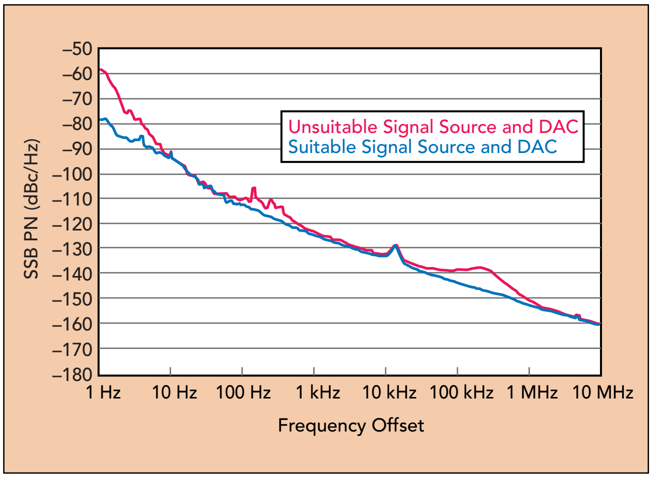


Fig. 14 **Comparing the SSB PN performance of the DAC using the two signal sources.**

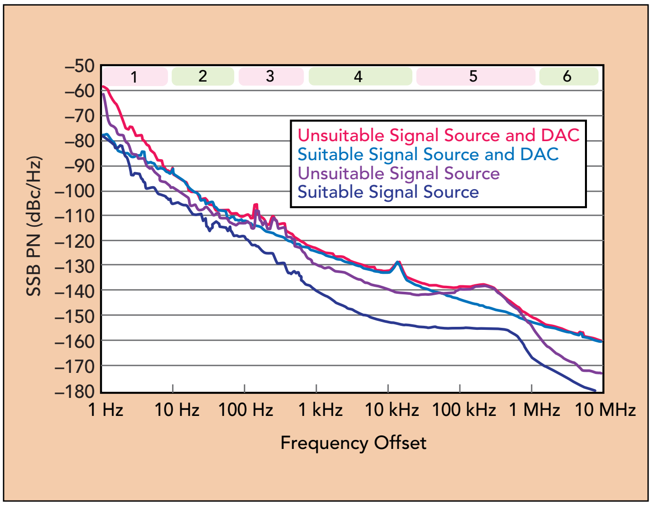


Fig. 15 **1 GHz SSB PN comparisons.**

fied SSB PN performance of -115 dBc/Hz at 10 kHz offset from a 10 GHz carrier. Although usable for many applications, this signal source may no longer be sufficient to for testing current generation analog-to-digital (ADC) and digital-to-analog (DAC) converters.

In this example, the DUT was a test board with a DAC. The best way to measure the residual SSB PN of the DAC is to generate a sinusoidal signal at its output, where the digital input is I = Q = 1. The DAC used here has a digital signal processing unit with a digital up-converter, enabling the digital input data to be resampled and shifted in frequency. The numerically-controlled oscillator of the DAC was set to $f_{out} = f_{sample}/9$, with f_{sample} = 9 GHz, so the DAC output signal was a 1 GHz sine wave.

As with the previous measurements, the setup comprised the two signal sources and the DUT; an R&S FSWP was used to measure the SSB PN (see ***Figure 12***). The SSB PN was measured with the suitable signal source, with and without the DAC, and the unsuitable signal source, with and without the DAC. ***Figure 13*** shows the SSB PN measurements of both signal sources at 9 GHz with +18 dBm output power and "downscaled" to 1 GHz by subtracting 20log(9 GHz/1 GHz) in dB. Downscaling is necessary to compare the SSB PN performance of the signal sources and the DAC.

Comparing the SSB PN performance of the DAC with the two signal sources, the difference in specific frequency ranges was high (see ***Figure 14***), with the lower curve the SSB PN performance of the DAC measured with the lower PN source. The SSB PN measurement using the unsuitable signal source adds significant contributions to the DAC's residual SSB PN. To show where the poorer signal source influences the SSB PN measurement, the offset frequency range was split into six bands (see ***Figure 15***). In ranges 2, 4 and 6, the measured DAC SSB PN performance was nearly same with both signal sources, as the SSB PN of the unsuitable signal source was better than that of the DAC. In frequency ranges 1, 3 and 5, the SSB PN of the unsuitable signal source was worse than the DAC's performance, so the SSB PN measurement reflects the performance of the unsuitable signal source, not the DAC.

These measurements show the importance of using a low PN signal source. To ensure accurate measurements, follow this process:

1. Measure the SSB PN performance of the signal source using the same frequency and power level as will be used for the DAC measurement. In this example, the DAC output frequency was 1 GHz, so the DAC clock input signal of 9 GHz was divided by 9 in the DAC.
2. Calculate the SSB PN performance of the signal source at 1 GHz to compare it with the DAC output frequency of 1 GHz: SSB PN (1 GHz) = SSB PN (9 GHz) − 20log (9 GHz/1 GHz) in dB.
3. Ensure sufficient margin between the DAC measurement and the calculated SSB PN of the signal source.

TABLE 1

SSB PN MEASUREMENT DEGRADATION

Δ SSB PN: Signal Source vs. DAC (dB)	Degradation (dB)
+10	10.4
+6	7.0
+3	4.8
0	3.0
−3	1.8
−6	1.0
−10	0.4

Table 1 shows how the SSB PN of the signal source will degrade the measurement of the DAC's performance. The table shows if the SSB PN of the signal source is 10 dB better at a certain offset frequency than the DAC's performance, the measurement will be degraded by 0.4 dB.

The instrument used to measure the SSB PN is another potential source of measurement error. Although not assessed in this article, a phase noise analyzer with low SSB PN should be used for these measurements to minimize any degradation.

SUMMARY

This article has examined how the harmonics, output power and SSB PN performance of the signal source can degrade measurement accuracy, often without the user realizing the unwanted effects. In each example, the performance of two signal sources was measured, showing the effect on a PA or DAC measurement. Guidelines for harmonics and SSN PN were provided to quantify the impact of the signal source, enabling users to determine the appropriate signal source requirements to achieve the desired accuracy for the application.■

Sivers Semiconductors and Rohde & Schwarz Collaborate on Testing 5G RF Transceivers up to 71 GHz

Rohde & Schwarz

As 5G networks are being rolled out globally, the evolution of the 5G NR standard continues. With Release 17, 3GPP will extend the frequency support of 5G NR mmWave bands into the unlicensed spectrum up to 71 GHz, a frequency band traditionally used by non-cellular standards like IEEE 802.11ad and 11ay. To address new testing challenges related to this bandwidth extension and to evaluate the performance of the latest generation RF transceiver chipsets, **Rohde & Schwarz** and **Sivers Semiconductors** teamed up to test RF transceivers for 5G NR up to 71 GHz.

With Release 17, 3GPP will extend the frequency support for its 5G New Radio (5G NR) standard to 71 GHz by Mid-2022. This extension requires an adaptation of the physical layer, notably the addition of two new subcarrier spacings (480 kHz and 960 kHz), and the support of wider signal bandwidths of up to 2 GHz. The support of this new frequency band poses new challenges to manufacturers of RF transceivers already targeting cellular applications, but also opportunities to those specialized thus far in the design and manufacturing of transceiver chipsets for non-cellular IEEE standards operating in these mmWave bands.

Rohde & Schwarz and Sivers Semiconductors have jointly tested the performance of the latest generation of RF transceiver chipsets, which so far supported the IEEE 802.11ad and 802.11ay standards, against 5G NR signals up to 71 GHz.

For the joint testing efforts, Sivers Semiconductors provided an evaluation kit as device under test (DUT), powered by the state-of-art RFIC TRXBF01 and the RF antenna module BFM06010. The RFIC supports IEEE 802.11ad/ay modulations up to 64QAM over the full

frequency range from 57 to 71 GHz. The setup consisted of the R&S SMW200A vector signal generator, which supports frequencies up to 67 GHz – 72 GHz in overrange mode – thanks to a new frequency option, and the R&S FSW85 signal and spectrum analyzer, the only one with an integrated signal analysis bandwidth of up to 8.3 GHz and supporting RF frequencies up to 90 GHz. The R&S ATS1800C compact antenna test range (CATR) based 5G NR mmWave test chamber completed the setup for OTA testing.

To validate the transmitter performance of the DUT, the R&S SMW200A provides a differential analog IQ baseband signal to the DUT, which performs the IQ modulation of the signal and up-conversion to the desired RF frequency. The generated signal is compliant to Release 17 of the 5G NR 3GPP standard and uses a subcarrier spacing of 960 kHz and a modulation bandwidth of 2 GHz. The DUT focuses its transmitter beam, which is created by 16 individually controllable antenna elements, in boresight direction towards the CATR reflector of the R&S ATS1800C. It bundles the signal to the feed antenna and provides it to the input of R&S FSW85, which then performs fully 3GPP compliant signal analysis.

To test the receiver performance of the DUT, the R&S SMW200A provides the 5G NR RF signal at 64 GHz (FR2-2), while connected to the feed antenna of the R&S ATS1800C. The feed antenna directs the signal towards the CATR reflector, which creates far-field conditions within a high-quality quiet zone (QZ) of 30 cm diameter. The integrated positioner allows repeatable RF measurements of the DUT within the QZ. The Sivers Semiconductors chipset converts the received signal into baseband, which is captured by an R&S RTP oscilloscope, and processed for individual signal analysis with help of the R&S VSE vector signal explorer software or on the R&S FSW signal and spectrum analyzer.

Erik Öjefors, chief technology officer of the wireless business unit at Sivers Semiconductors, said, "This has been a valuable opportunity for Sivers Semiconductors to be able to provide yet another proof point of our world leading mmWave technology. Together with Rohde & Schwarz, we have demonstrated that the high performance of our mmWave transceiver RFICs provides a pathway for future NR-U deployments in the 60 GHz band based on the upcoming 3GPP Release 17 standard. Early access to test and measurement solutions capable of addressing new and upcoming standards such as 5G NR in the 60 GHz band is critical for our mission to be at the forefront of technology development."

Andreas Pauly, executive vice president Test & Measurement at Rohde & Schwarz, said, "Together with Sivers Semiconductors, we set another milestone for the wireless industry. With our innovative test and measurement solutions we verify new functionalities within the 5G New Radio standard, demonstrating our continuous commitment to our partners and customers. Through this, we enable them to develop cutting-edge technology that will make advanced use cases of 5G for consumers and enterprises a reality."■