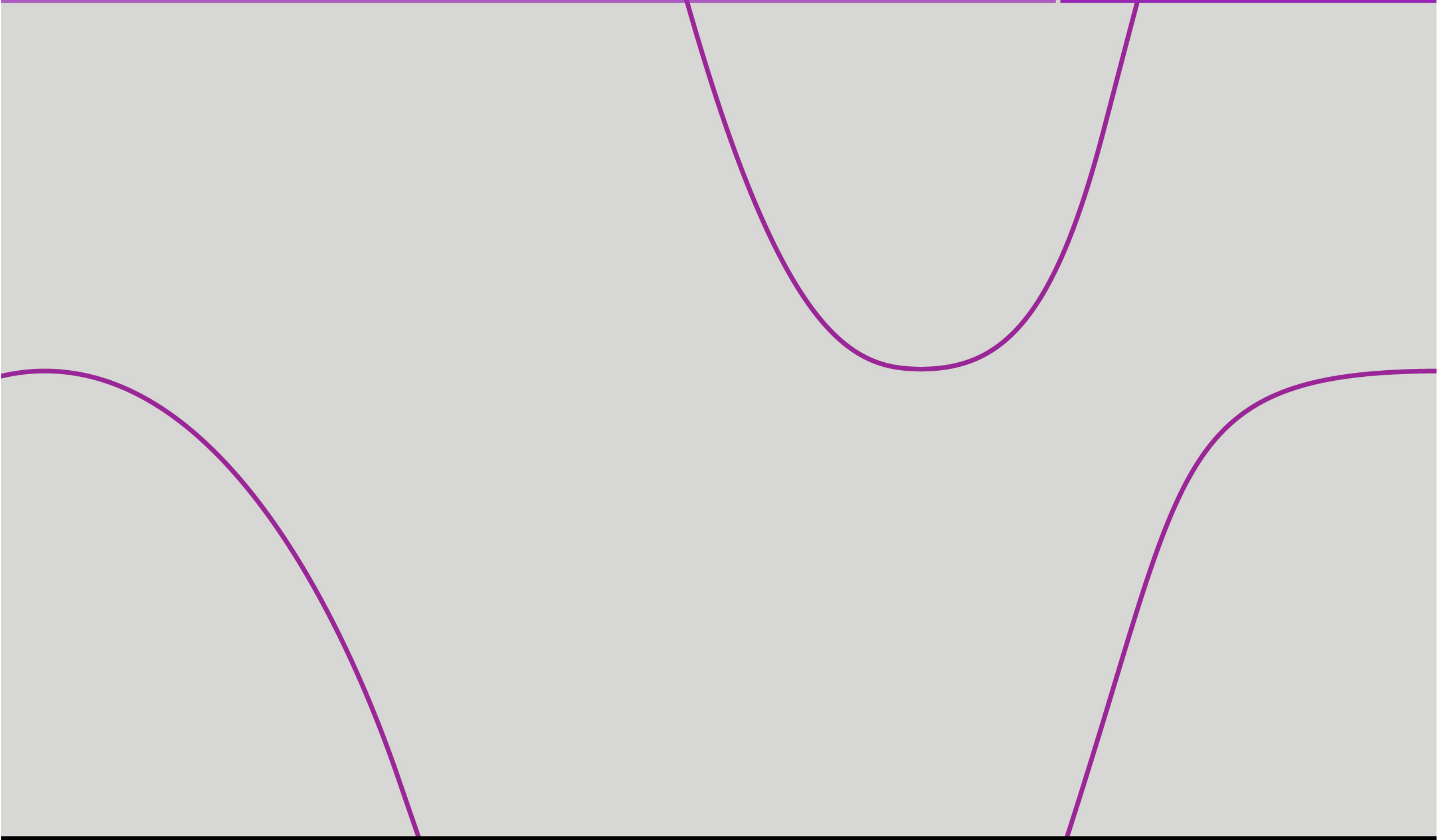
WHITE PAPER



Characterizing CRPAs and Other Adaptive Antennas

How to Test CRPAs and Other Advanced GNSS Antenna Designs

KEYSIGHT

Table of Contents

Introduction....3
How Adaptive Antenna Systems Work....4
Challenges of Testing Adaptive Antennas....5
Defining What to Test....6
Defining the Test Requirements....8
Choosing a Test Method....9
Choosing the Test Equipment....17
Sample Test Walkthrough: Conducted Test....20
Future Considerations....24
Conclusion....25
How Keysight Can Help....25
Contributors....30
Glossary of Abbreviations....31

Introduction

Anti-jamming and anti-spoofing capabilities are becoming essential features of mission-critical Global Navigation Satellite Systems (GNSS) receivers and dependent systems.

Threats from signal jamming and spoofing are increasing; both from civilian sources (e.g. illegal personal privacy devices (PPDs) intended to mask a commercial vehicle's whereabouts) and from the use of radio frequency interference (RFI) as an electronic warfare (EW) method deployed by nation states to disrupt an adversary's operations.

GNSS Jamming on the Rise

The International Civil Aviation Organization (ICAO) received 174 reports of GPS disruption in the Eastern Mediterranean region in 2018, compared to just 32 between 2015 and June 2018.[1]

In the military domain, the need to protect mission-critical PNT systems led to the development of adaptive antennas that can be retrofitted to a wide range of GPS receivers. Now, adaptive antennas are also increasingly used in commercial applications such as surveying, mining, and autonomous vehicles.

Adaptive antenna systems need to be thoroughly tested, particularly if they are to be used in safety and liability-critical contexts. In this paper, we will explore the challenges of reliably testing adaptive antennas and provide guidance on establishing test requirements, selecting test equipment, and conducting a test using a radio frequency constellation simulator.

Finally, we'll set out how Keysight can help with any aspect of adaptive antenna testing — from providing future-proof simulators and software to designing a zoned chamber solution for over-the-air (OTA) testing.

How Adaptive Antenna Systems Work

Adaptive antenna systems come in a number of forms, with lesser or greater degrees of sophistication. The fundamental principle of operation, however, is that the antenna is designed to maximize reception of genuine GNSS signals while mitigating the impact of interfering signals.

Developers can achieve mitigation through the physical design of the antenna as well as through algorithms that control the antenna's behavior. Adaptive antenna technologies include:

Fixed radiation (or reception) pattern antenna (FRPA)

A single-element antenna can be hardened against interference with the addition of a choke ring or "horizon nuller": a device that blocks radio frequency (RF) signals arriving from a low elevation.

Controlled radiation (or reception) pattern antenna (CRPA)

This is a multi-element antenna that can steer its reception pattern in real time toward genuine signals and away from interfering signals.

CRPA design is typically planar, with several antennas arranged in a circular pattern around a central reference element. Studies have shown that a convex design offers an additional advantage of being able to steer the radiation pattern vertically as well as horizontally.

The steering algorithms work by assigning and modifying "weights" for each antenna element based on the received phase shifts of each signal. By modifying these weights, it is possible to change the radiation pattern of the array to steer nulls in the direction of the unwanted signals or gain in the direction of genuine signals. The combined output from the antenna electronics is output to the GNSS receiver for further processing to provide position, velocity, and time (PVT).

Steering algorithms can be embedded in the GNSS receiver or driven by a separate antenna electronics unit. The best performance is usually achieved when the algorithms are embedded in the receiver (Rx) and the system is integrated with one or more inertial measurement units (IMUs).

Algorithm-based CRPA technologies include:

Null generation/null steering	Steering negative antenna gain toward a source of RFI to try to cancel out the interference. The number of interferers that can be neutralized increases with the number of elements in the antenna array: For example, a seven-element array can deal with six interference vectors. There is, however, a trade-off in terms of antenna size and cost. A military-grade antenna typically has seven elements, while a commercial antenna may have four.
Beamforming/beam steering	Steering positive antenna gain toward signals that are not jammed or spoofed to minimize the impact of the interference.
Space-time and space-frequency adaptive processing (STAP and SFAP)	Advanced algorithms that further increase the antenna's ability to steer a null toward sources of interference. STAP and SFAP can adapt the weights of individual outputs to create multiple beams or nulls at the desired directions and to switch the adaptive antenna pattern steering at faster rates.
Adaptive CRPA	The newest CRPAs allow each beamformer to track one specific satellite while forming a null in the direction of one or more interferers.

Aiding with Inertial Navigation Systems (INS)

High-end, dynamic, safety-critical PNT systems using adaptive antenna technology often also make use of IMUs to provide additional anti-jamming capabilities.

These sensors provide the attitude of the system, allowing control algorithms to take accurate attitude into consideration for PVT calculation and for beamforming to suppress interference. It is important to ensure that test coverage of an adaptive antenna system also takes any associated IMUs and sensor fusion algorithms into account.

The Importance of Antenna Design

Note that it is not possible to compensate for a poorly designed or implemented antenna array anywhere else in the system or by the use of improved algorithms. Characteristics of good GNSS antenna design include:

- Visibility of as many satellites as possible
- High carrier-to-noise (C/N_0) ratio of strongest satellite signals
- High directivity (radiation pattern optimized for higher gain in direction of satellites)
- High gain performance
- Good filtering of out-of-band signals
- Low coupling between elements (for multi-element antennas)
- Good match between antenna and connecting RF cables

Achieving these characteristics can be challenging, as the size of aperture required for optimum signal gain can conflict with the size requirements for the antenna system.

Challenges of Testing Adaptive Antennas

The sophistication of adaptive GNSS antenna systems creates some intricate test challenges.

Firstly, **antenna and receiver capabilities** need to be tested in realistic scenarios and ideally with the ability to repeat the same test conditions many times over.

This requires an initial **risk assessment** to understand the breadth of interference scenarios that the system may encounter — including possible future scenarios — and the desired behavior of the system in response to those scenarios.

It then requires the drawing up of a **test regimen** incorporating these scenarios to understand their impact on the system's performance.

Next, the appropriate **test method** must be chosen at each stage of the product development and selection cycle. There are a number of options, with some requiring a significant investment of time and budget.

Suitable **test equipment** — hardware and software — must be chosen, so tests can be conducted accurately and reliably in a lab, chamber, or open-air environment, and so that future test requirements can also be accommodated. Equipment must be properly installed and configured, which can require significant specialist knowledge, especially for more complex chamber-based tests.

The tests must be **set up and run** correctly, and the results accurately monitored and recorded. Extensive testing may require a degree of test **automation**, which must also be set up correctly.

In the next sections, we'll look at each of these challenges in turn and provide guidance on choosing an appropriate approach to adaptive antenna testing throughout the product lifecycle.

Defining What to Test

The test approach will be largely guided by which antenna and receiver capabilities need to be tested, to what degree of rigor, and in which types of scenarios. That requires a risk assessment to be carried out first, followed by requirements gathering for the test scenarios.

Risk Assessment and Analysis

An important part of test planning is to develop test scenarios based on the threats the system or device is likely to encounter during operational use. A risk analysis should be carried out to understand how likely it is that the system will be exposed to harmful levels of GNSS interference and / or spoofing, and the likely operational impact if it is. Scenarios can then be developed to test the system's response to those threats.

Types of interference a system may encounter — individually or in combination — could include:

Jamming: Both intentional GNSS frequency jamming by malicious actors and unintentional interference from radio transmissions in bands close to the GNSS frequencies are on the increase. Frequency jamming is becoming more common, as vehicle owners purchase illegal jammers to override in-vehicle telematics, and as nation states increase the use of RF signal jamming in conflict zones or contended geographical areas. Adjacent-band interference (ABI) is becoming more common as spectrum adjacent to the GNSS bands is allocated to other services, including most recently the 5G services offered by Ligado Networks in the US.

Spoofing: Once an arcane disruption technique, GNSS spoofing (broadcasting of fake GNSS signals) has become significantly easier and cheaper with the rise of software-defined radio (SDR). A low-cost spoofing device can be easily built from components sourced on the internet and downloaded open-source code. Notable spoofing incidents include multiple ships affected in the Black Sea in 2017, and ships in Chinese ports being spoofed in a distinctive circle pattern in 2019. State actors with sophisticated equipment may be responsible for incidents of this type.

Obscuration: GNSS signals, which work on a line-of-sight basis, are blocked by objects on the ground such as tall buildings, hillsides, and dense foliage. A GNSS-reliant system is not only vulnerable while it is unable to receive satellite signals, but also as it exits an area of obscuration, such as a tunnel or underground car park. As it attempts to reacquire a signal, it can be subjected to a spoofing attack, causing it to lock on to the fake signal rather than a genuine one.

Multipath: In addition to direct (line-of-sight) signals from satellite, signals can take multiple paths: reflected or diffracted by buildings or other objects in the environment. These signals have slightly further to travel and so arrive at the receiver slightly later than line-of-sight signals. Without mitigation, multipath signals can cause the receiver to output an inaccurate range measurement that translates into an erroneous position.

If a system is likely to encounter interference that could have a material impact on safety of life, national security, financial liability, or market success, extensive testing will be required to assure the system's performance.

At the R&D stage, these findings can inform the design of the system's mitigation capabilities. In later stages of the product cycle, the findings can help evaluate a PNT system's robustness in the face of jamming and spoofing interference.

Further Reading

For more detail on evaluating the risks of interference and spoofing, read our white papers:

GNSS Jamming: How to Test the Risks to Safety-Critical and Liability-Critical Systems

GNSS Signal Spoofing: How to Evaluate the Risks to Safety-Critical and Liability-Critical Systems

Defining the Test Requirements

It is important to define the requirements in detail before investing in test instruments and other equipment. Gathering the requirements may encompass knowledge of the following:

Purpose of the testing	Testing could be required for one or more purposes, including: • Evaluation of early-stage adaptive antenna algorithms • Internal quality control and qualification procedures • Benchmarking and vendor selection for adaptive antennas or PNT systems equipped with adaptive antennas • Understanding and quantifying possible operational impacts resulting from exposure to interference • Carrying out a risk assessment of real-world threats including jamming and spoofing attacks Any potential future requirements should also be considered to avoid having to invest in further equipment.
Scope of the testing	Should the physical antenna be tested along with the antenna electronics unit, GNSS receiver and other hardware in the loop (HIL)? This will determine whether OTA tests are needed as well as conducted tests.
Geographic location(s)	Should the simulations be carried out for more than one location, or is simulation for a single location sufficient?
Satellite geometries	Do tests need to be repeated with identical satellite geometries, and are there any ”worst case” satellite geometries that need to be included in the test regimen?
Vehicle motion	Are the device under test (DUT) and interference source(s) stationary, or is there any relative motion?
Spoofing vector profile	This will encompass: • Profiles for relative power, code / carrier phase and Doppler offsets of spoofing signals with respect to (if required) authentic signals • Code / navigation data attack: A selection of likely target messages has to be made (e.g. health status of space vehicle (SV), clock correction messages, ephemeris data) • Pseudorange ramp: At what pace should the spoofer move the position from truth? (If done over a long period of time, this type of attack can deceive the receiver and ”sneak under” alarm / alert thresholds) • RFI profile if ”jam then spoof” attacks need to be considered. See below.
RFI power profile	This will encompass: • Boundary conditions (e.g. min / max jammer / spoofer power levels) • How rapidly the jammer / spoofer power levels change (e.g. the slope of a first order power ramp) depending on the dynamic output range and update rate of the test instrument (e.g. every 1ms) • The power resolution (e.g. at least 0.1 dB) • Supported bandwidths: For GNSS receiver testing it is essential to support the GNSS frequency bands (e.g. L1, L2, and L5 for GPS) as well as the adjacent bands, which may affect the DUT performance

	• Accuracy required (e.g. calibrated power levels, static and run-to-run biases, non-linearities). Note that there are inherent trade-offs in any signal generator between supporting a wide effective bandwidth against the achievable power level magnitude and accuracy. This trade-off must be well understood before investing in vulnerabilities testing equipment. For example, some manufacturers re-purpose generic SDRs for testing within the GNSS frequency bands. Although these generic SDRs can generate waveforms over a wide spectrum of frequencies (e.g. cellular, digital TV, Wi-Fi), they essentially sacrifice performance in terms of calibrated power level, signal fidelity, and spectral purity
DUT testing states	This is very important to ensure test repeatability, especially if testing is conducted in chronically divided phases, or by different operators, sometimes located at different test sites. Typically, the DUT is cold-restarted between test runs, erasing any previous data stored in the volatile memory, but invoking the testing state configuration parameters (e.g. last-used, user-saved, or factory-set) from the non-volatile memory — enabling testing of the DUT from an identical initial test state. These configuration parameters may contain essential information (e.g. which atmospheric model the Rx may employ) or whether to enable or disable any multipath / interference mitigation algorithms.

Choosing a Test Method

Having decided on which capabilities to test, and defined the test requirements, a test campaign must be planned to show that the new system is providing the expected benefits.

This may require repeating tests carried out in quantitative risk assessment to prove that the technology is now able to provide an adequate defense against expected threats. It is also worth considering some "worst cases" that may not have been considered in the original risk analysis, but which could help to future-proof the system against the evolving GNSS threat landscape.

There are numerous ways to validate the performance of an adaptive antenna system. The method chosen will likely depend on the nature of the DUT and the specific purpose of the testing.

At the highest level, there are two options:

- **Conducted testing:** playing simulated or recorded signals and interference directly to the receiver of the DUT via coaxial cable, bypassing the physical antenna. This kind of testing is typically done at the receiver R&D stage and does not evaluate the performance of the antenna hardware.
- **Radiative or over-the-air (OTA) testing:** transmitting real or simulated RF signals over the air to the DUT, to evaluate the performance of the antenna and antenna electronics. This kind of testing is typically carried out later in the product cycle, to validate the performance of the whole system including the physical antenna subsystem.

For radiative testing, there are two broad options: testing on an open-air range with real GNSS signals or testing with simulated signals in a closed (anechoic) chamber. With a chamber, there are broadly two types of possible configuration: using a fixed antenna to represent each GNSS SV or using a "zoned chamber" to simulate SV movement in orbit.

A "system of systems" approach is required when developing a test plan for complex systems using a GNSS receiver in conjunction with adaptive antenna technology. The plan will typically combine elements of both conducted and OTA tests to verify and validate system performance.

In a typical "system of systems" test plan, conducted testing will provide assurance of the receiver and associated electronics performance. OTA testing will then allow the performance of the antenna system to be considered as an additional variable.

It should be noted that conducted and OTA testing are not equivalent techniques. Each has advantages and disadvantages that must be considered when making decisions on the most effective combination of tests, methodology, and analysis.

A summary table of the test methods is included at the end of this section.

Illustration of a simulated test environment incorporating GNSS, multipath and jamming in a zoned chamber

Conducted Testing with Simulated Signals and Interference

In a conducted test, all relevant elements of the RF environment are transmitted directly to the antenna electronics (in devices where the electronics are in a separate unit from the antenna) via coaxial cable.

Signals from a single or multiple satellite constellations are generated by an RF constellation simulator (RFCS), optionally including multipath interference and signal obscuration effects, as well as atmospheric interference. Interference waveforms can be generated internally by the GNSS signal simulator or an external interference generator.

For single-element antennas, the combined single RF output from an RFCS and interference generator can be used to generate the required signals. For multi-element antennas, a signal wavefront is required from the multiple individual outputs of the simulator, to simulate the phase changes across the antenna elements.

The signals from the multiple individual outputs of the simulator can be used as a combined RF signal input to a GNSS receiver requiring a single input, or as individual antenna feeds to an antenna electronics unit or GNSS receiver that is capable of receiving individual antenna array inputs.

Advantages

Control: The test conditions are fully controllable, including power levels of satellite signals, jammers, and spoofers. Multipath, obscuration, and atmospheric effects can be modeled to a greater or lesser degree, depending on the simulation equipment used.

Time and cost: Tests can be conducted at will in the lab, allowing for faster test timescales than waiting for permission and dates to conduct field trials on an open-air range. The cost and logistics of open-air testing are removed. Tests can also be automated, further accelerating timescales.

Repeatability: The test environment is fully repeatable, allowing reliable iterative testing. For example, to compare the performance of different CRPAs, to assess the impact of different interference waveforms, or to evaluate iterative modifications to anti-jamming and anti-spoofing algorithms.

Disadvantages

Coverage: Conducted testing bypasses the physical antenna, so the effect of antenna behavior on the receiver is not evaluated.

Realism: Depending on the equipment used, the simulated signals, multipath / obscuration and atmospheric effects may lack the depth and richness (such as lack of resolution of angle of arrival) of the real-world environment. The level of jamming signal that can be applied will be limited. Tests may therefore not provide a detailed characterization of real-world performance.

“Live Sky” Testing on an Open-Air Range

Testing is conducted on an open-air range with live satellite signals and using real jamming and spoofing equipment (with the relevant regulatory permissions) to disrupt the signals from space.

Advantages

Authenticity: The richness and authenticity of the real environment provides a reliable guide to the real-world performance of the antenna and receiver in the presence of RF interference.

Disadvantages

Risk: Open-air testing carries the risk of collateral damage to GNSS-dependent systems in the vicinity of the test range. To mitigate the risk, the power level of the jammers and spoofers must often be scaled down. The performance of the antenna and antenna control systems can still be assessed, but because the scale of the setup is compromised, angular measurements may be less accurate than is desirable.

Logistics: The equipment under test, the interference-generating equipment, the test recording equipment, and any record and playback systems (RPS) must be transported to a dedicated open-air test range, often in a geographically remote area.

Time and cost: Open-air field trials can incur significant costs in terms of time, resources, and equipment. That can delay the availability of new CRPAs and may be less cost-effective than using a chamber (see below). The permissions required to gain access to test ranges can make it impossible to carry out testing at short notice.

Repeatability: The real-world RF environment is constantly changing, and conditions like the satellites in view, multipath effects, and temperature can’t be controlled, meaning test conditions can never be exactly repeatable. That creates issues of accuracy and reliability if tests are run iteratively.

Limited environment: There is a lack of control over the environment. Devices will be tested only for operation in the designated test range. This will, generally, not be urban, or have other equipment operating nearby, meaning the scope of the testing is far more limited. Test conditions are also limited to the satellites and constellations in view at the test location.

Anechoic Chamber with Fixed Antenna Array

The traditional method of configuring an anechoic chamber for CRPA testing is to place a transmit (Tx) antenna at the same azimuth and elevation as the individual SV it is to emulate. The antenna then broadcasts that SV’s signals using one single-channel GNSS signal simulator per antenna. Interference sources such as jammers and spoofers can be placed anywhere in the chamber.

For additional realism in dynamic scenarios, the Rx antenna can be mounted on a rate table / 3D positioner that replicates the attitude changes of the simulated vehicle platform. For units such as handheld devices, items such as reflectors, and signal attenuators (for example, a dummy human head) can be physically placed adjacent to the DUT to emulate a realistic environment.

Additionally, realistic multipath, obscuration, and atmospheric interference effects can be introduced with the use of advanced 3D environment modelling and ray tracing.

Advantages

Control: Full control over the test environment, ensuring the same conditions can be repeated to test different antennas, antenna designs, or antenna placements.

Coverage: The antenna hardware is brought into the test, along with the potential for differing angles of arrival of signals on the hardware.

Disadvantages

Realism: The constraints of the chamber design make it challenging to accurately recreate the geometry of any particular GNSS constellation, or to emulate a multi-constellation environment.

Test duration: Fixed Tx antennas are unable to represent the movement of satellites in orbit, but rather represent a given fixed location, time, and date. Only very short test scenarios are possible (around 30 minutes), as the environment quickly becomes unrealistic. While this can be useful for evaluating the receiver’s ability to lock on to and track GNSS signals, and can help with assessing the CRPA’s beamforming capabilities, it is not an effective method for testing an active or responsive antenna system.

Zoned Chamber

A zoned chamber also makes use of fixed antennas distributed in a regular pattern of azimuth and elevation angles. However, unlike configurations that require one fixed Tx antenna and one single-channel simulator per SV, the zoned chamber employs one Tx antenna per zone, from which all the signals in that zone are broadcast (see Figure 1).

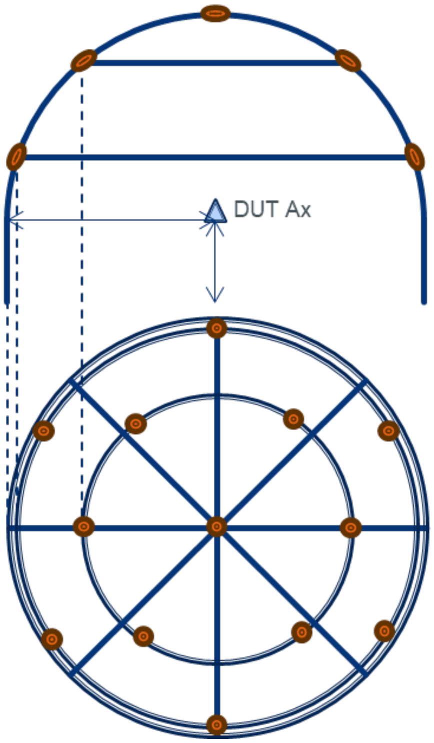


Figure 1. Configuration of 13 Tx antennas in an anechoic chamber

Signals from a specific SV are broadcast in one zone before being switched off in that zone and transitioning instantaneously to the next, emulating the pattern of satellite movement in orbit. By enabling realistic simulation of specific satellite constellations orbiting the earth, the zoned chamber approach represents the state of the art in OTA CRPA testing.

Zone sizes can be modified to suit the test requirements and the dimensions of the chamber. Keysight's work with commercial organizations has indicated that 31 zones is the optimum configuration (see Figure 2). A reduced number of zones at lower elevations and a higher density of zones above 10° may offer a better representation of the orbital paths.

A smaller zone size should offer a better representation of the orbital paths. This is because the signal angle becomes less accurate as the orbit progresses toward the edge of the zone, and a smaller zone size shortens the distance between the bore site (located at the center of the zone) and the zone edge. However, the trade-off of having smaller zones at the higher elevations is an increase in transitions or handovers from zone to zone.

Note that each satellite signal is assessed independently. While there is a small signal interruption when signals move zones due to an inevitable discontinuity in carrier phase, this will only impact the satellite signal concerned. This might cause brief loss of carrier lock on the affected SV, but these events occur infrequently and are unlikely to affect more than one satellite at any one time. Consequently, they can generally be considered to be insignificant.

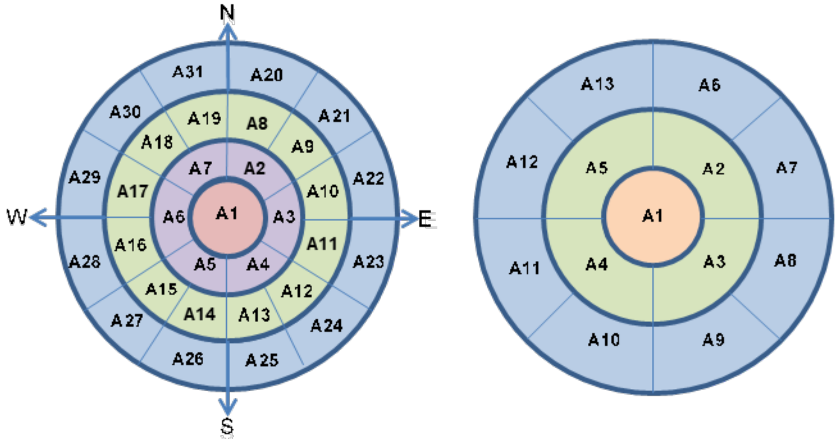


Figure 2. Configuration for a 31- and 13-zone setup in a Keysight zoned chamber

As with the fixed chamber, interference sources such as jammers and spoofers can be placed anywhere in the chamber, and a rate table / 3D positioner, reflectors, and signal attenuators can be used to provide additional realism. Realistic multipath, obscuration and atmospheric interference effects can be introduced with the use of advanced 3D environment modeling and ray tracing that takes into consideration, and manipulates accordingly, the angle of arrival information for the signals.

Advantages

Realism: A zoned chamber makes it possible to simulate the movement of real GNSS constellations in orbit. Individual constellations (e.g. GPS, Galileo, GLONASS) can be simulated, as well as combinations of constellations (e.g. GPS + Galileo + GLONASS).

Test duration: Test scenarios can play out for longer without losing realism, making the zoned chamber effective for validating all aspects of the CRPA system, including beamforming, null steering, and SFAP / STAP processing.

Accurate angle of arrival: The azimuth and elevation of each satellite can be realistically recreated, allowing direction-finding and anti-spoofing capabilities to be reliably assessed.

Disadvantages

Phase calibration challenges: Depending on the system's hardware update rate, there may be a small signal interruption when signals move between zones. Since signal generation is tied to carefully defined time epochs, a discontinuity in carrier phase is inevitable, the magnitude of which is dependent on the quality of the calibration. This might cause loss of carrier lock, but this is inevitable in any switched system. The frequency of change increases with the number of zones; with a 31-zone system a typical rate would be every 2–3 hours for a static vehicle.

Summary of Test Options for Adaptive Antenna Systems

Test method	Key advantages	Key disadvantages	Product cycle stage
Conducted			
Simulated signals	Conditions are fully controllable and repeatable Multiple constellations (including future signals) can be simulated	Signals bypass the physical antenna, making it unsuitable for testing an active or responsive antenna system	Receiver testing during R&D and integration
Over the air			
Live sky	Real-world environment; CRPA performance can be validated More cost-effective than building a dedicated chamber	Restricted access area required; environment is not repeatable in a controlled manner; jamming signal may affect other GNSS users, and spoofing may not be authorized. Some constellations may not be in view for global system testing Resource intensive	Verification testing of the CRPA elements and CRPA electronics unit
Fixed chamber	Relatively simple to configure Test environment is fully controllable and repeatable Jamming and spoofing can both be introduced	Satellite movement is not simulated, therefore scenario signal geometry is only valid for a short duration	Receiver validation and validation of CRPA beamforming capabilities during R&D and integration testing
Zoned chamber	Test environment is fully controllable and repeatable Jamming and spoofing can both be introduced Longer duration for testing Azimuth and elevation of received signal are realistic Each constellation can be simulated together or in isolation	Hardware intensive solution Each RF output requires careful phase calibration so lock is not lost during zone transitions	R&D, integration, and conformance testing of all aspects of the CRPA system

Choosing the Test Equipment

The equipment required for testing adaptive antenna-based systems throughout the development cycle may encompass the following:

- GNSS RFCS or wavefront simulator
- Interference generator (if an interference-enabled wavefront simulator is not being used)
- Calibrated cabling / adaptors, connecting the GNSS RFCS to the antenna DUT
- Access to an anechoic chamber or open-air test range
- 3D positioner / rate table to emulate DUT motion and attitude
- Jamming / spoofing device (for chamber-based or open-air testing)
- RF RPS (for testing with recorded real-world signals)
- The device under test
- Monitoring equipment for data collection and analysis, typically via the Rx control user interface, and / or other custom / third-party tools interfacing the Rx output

Test scenario considerations

The choice of equipment for conducted testing may encompass requirements for the following scenario elements:	
Nominal GNSS signals	• Constellations, frequencies, signal geometry (including orbit definitions) • Open, classified signals, or custom-defined codes / nav data and waveforms with specific RF characteristics
Interference	• High jammer to signal (J/S) ratio, e.g. above 130 dB (corresponding to absolute power of 0 dBm or above) • Maintain carrier-phase coherence with nominal GNSS signals and performance specs, e.g. less than 0.5 mm of phase alignment between generated signals • Maintain high performance specs in all given test conditions, e.g. do not compromise signal fidelity when in high-dynamic conditions or at maximum output power • Ability to modulate custom-defined waveforms (I/Q data streaming) into the test scenario
Overlaid errors and other effects	May include: • Proven mathematical models for ionospheric / tropospheric error modeling, and other physical phenomena affecting GNSS receiver performance, e.g. scintillation; this type of modeling may encompass orbital perturbations and the capability to inject any other custom-made error models via an open remote API • Signal-in-space errors and custom-defined signal failure modes • Multipath interference with appropriate 3D environment modeling • Fusion with inertial sensors, emulating the IMU outputs, and support a range of proprietary high-end INS / GNSS receiver interfaces
Power output	• Modeled (dependent on simulated range between DUT and GNSS / interference transmitters) or fixed
Additional considerations	• Calibrated / characterized cables (phase matched) are essential • Maintain coherence between nominal GNSS signals (+overlaid effects / errors) and interference signals • Ensure the simulated antenna pattern and CRPA elements geometry is reflected accurately in the scenario definition parameters • Ensure that any vehicle dynamics are modeled faithfully and are injected into the scenario at the highest possible update rate (as per application requirements), e.g. 1 kHz or above

CRPA and GNSS receiver (DUT) considerations

The detailed CRPA and GNSS receiver design is out of the scope of this paper; however, the following aspects must be considered:	
Number of CRPA elements	This will impose a physical limit to the number of adaptive beamforming and null-steering lobes that can be generated
Characterization of individual antenna elements	Aspects to consider include cross coupling, gain / phase patterns, impedance / group delay responses, and their relative geometry to reduce phase noise and correlation, producing robust phase outputs to the antenna electronics unit Ideally, all elements' phase outputs must be coherent, with 0° and 180° relative phase, when a signal wavefront is perpendicular or horizontal, respectively, relative to the antenna array
Antenna electronics unit circuitry and adaptive algorithms	These can range from simple to more sophisticated implementations, to meet corresponding application requirements in terms of: • Adaptive patterns, e.g. null depth, directionality • Beams / nulls switch rate (typically less than 50 ms for civil applications)
Test state of the antenna array and GNSS receiver	Initial settings may differ among tests Ideally the DUT will provide a utility to configure these settings easily and in a repeatable manner, e.g. via injecting remote commands or scripts

Simulator considerations

The following aspects should be considered when selecting an RFCS with multiple phase outputs for conducted or radiated testing:	
GNSS nominal signals	Open + classified (if needed)
Custom-defined waveforms	For example, GNSS signals in pre-operational / experimental stage or without a published interface control document (ICD), called "non-ICD signals" for brevity in this paper, or secure signals with classified modulated codes and nav data, bespoke RF characteristics and power modeling, e.g. fixed or range-dependent Non-ICD signals and injected custom-defined waveforms may encompass different modulation types, sub-carriers, primary, secondary code, and nav data rates, etc.
Number of RF outputs	These must be equal to or greater than the number of CRPA elements under test, e.g. 16 or above
Support for number of signals	Including combinations of constellations and frequencies, plus multipath, as required by the number of CRPA elements under test and application (e.g., 1,000 or above)
Control of output RF signals	Output signals must be precisely carrier-phase aligned and controllable to recreate a realistic incipient wavefront on the CRPA under test Precise power control is an important consideration (especially for dynamic scenarios), requiring accurate signal propagation modeling between the simulated receiver position and satellite positions
System upgradeability	The RFCS may comprise a standalone single chassis or synchronously connected multiple chassis to scale up the test system capabilities Careful consideration is required when deciding about future system upgrades, as they may require compromises on other aspects (e.g., hardware update rate or number of simultaneously simulated channels)
Interference generation (via the RFCS or a separate interference generator)	Key considerations include: Interference specs must allow tight carrier-phase alignment with the nominal GNSS signals and employ high quality spectral properties, e.g. negligible spurious signals/harmonics, even at high output power levels of more than 0 dBm (i.e., >130 dB J/S referenced to the nominal ICD GPS L1 C/A level of -130 dBm) It must be noted that typically, external interference signal generators (ISGs) can be more powerful than embedded ones, but they cannot provide the same precision in terms of the carrier-phase alignment level required for CRPA testing applications

	The simulator user interface must provide a user-friendly utility to define the interference radiation field, e.g. a map that shows the positions of ground interference transmitters (static or dynamic) with respect to the simulated vehicle representing the receiver under test The interferer must support many different — and easily defined, types of waveforms — e.g. additive white Gaussian noise (AWGN), FM, AM, PM with appropriately defined RF characteristics, e.g. bandwidth, update rate, frequency resolution, etc. This capability may encompass injection of custom-defined interference waveforms (I / Q data)
Additional support for scalable requirements	For example: Multipath interference with 3D dynamic environment modeling, e.g. static buildings, trees, and moving vehicles / pedestrians Integration with inertial sensors, to test equipment and algorithms using inertial / GNSS sensor fusion
Test automation capabilities	Ideally, the RFCS should offer the option of an open application programming interface (API) which enables automation of the whole testing process and real-time test progress monitoring, ensuring repeatability over multiple test runs This facilitates testing in many ways, for example: • Different testing sites with different test operators • When a series of identical tests (or “golden scenarios”) need to be repeated at a future time, e.g. in a modified / upgraded design of the DUT for comparative performance analysis • When the DUT or testing equipment is upgraded, e.g. by adding more CRPA elements, this typically requires minimal modification of the automated testing scripts by a test engineer, rather than allocating precious engineering resources on redesigning and updating entire testing processes

Further reading

For more information on how to characterize simulator performance, read our eBook:
How to Choose a GNSS Simulator

Chamber test considerations

The following further requirements should be considered when selecting a chamber for OTA testing:	
Chamber design	Typically, this will be a dome that can be assembled just in time according to testing needs and resource availability
Power control of RFCS and interference generator	A key challenge with an anechoic chamber is the scale factor and the inherent restrictions it imposes on the signal propagation properties — such as artificial reflections (which can be mitigated by careful placement of RF-absorbing materials) and different power propagation models It is key that the test equipment allows for precise control of the carrier phase and power level of GNSS and (optional) interference signals to maintain realism, especially in the presence of high dynamics in the simulated scenario
RF isolation	The chamber should be RF-isolated from the external environment to prevent accidental leaking of signals Typically, the control room is also RF-isolated from the chamber with RF and data inputs linked from the control room to the chamber If the controllers of the radiating equipment are inside the chamber, remote access from the control room is allowed Tests involving classified signals may require additional access provisions, which are out of the scope of this document

Transmit antennas	Typically supporting multiple GNSS frequencies, e.g. in the L1 and L2 frequency bands Calibrated cables / adaptors will be needed to connect the RFCS with the transmit antennas
Rate table/3D positioner	Optionally, a rate table / 3D positioner may be required to emulate physical rotations undertaken by the CRPA host vehicle

Sample Test Walkthrough: Conducted Test

This is a conducted test, designed to measure C / N improvement in the presence of interference for a 7-element CRPA DUT.

Scenario

This table summarizes key simulated parameters in the scenario:

Simulated parameter	Notes
Start date / time and duration	It can be in the past (noting that some DUTs prohibit that), real time, or future, and last from a few seconds to weeks, as per application requirements, but a typical scenario duration is a couple of hours
Vehicle position	Static or dynamic (with pre-defined or real-time induced external motion) in WGS84 coordinates
CRPA elements relative positions (on vehicle)	Fixed for the duration of the scenario run Different antenna array configurations can be changed / saved / uploaded in-between runs
CRPA elements antenna patterns	Via user-friendly gain and phase 3D editors, with capability to switch antenna patterns during the scenario run
Satellite signals	GPS L1 (the number of which depends on satellite visibility in the scenario)
Satellite geometry	Default parameters propagated by the RFCS control software or induced via RINEX / SP3 orbital files, with optional curve-fitting function to realistically represent the satellite ephemerides parameters' propagation during the time of validity of a given upload period Additional effects (satellites rising / setting) may be simulated
Jamming signals	6 static or dynamic jammers, to exercise the full capabilities of the DUT (7-element CRPA)
Motion and geometry of jamming signals	The jammers can be placed in absolute positions, or relative to vehicle, and move during the scenario Jamming signals can be of various types, e.g. AM / FM / AWGN / pulsed, they can be switched on / off as required, and their transmission power and motion can be controlled in real time (either interactively via the GUI or via remote commands), or via pre-loaded scripts
Atmosphere and errors	Default ICD models, or custom-defined with additional errors, e.g. scintillation
Other errors	For example, multipath, signal-in-space (SIS), and nav data failure modes

Test Method

The scenario is executed and DUT timestamped output parameters (e.g. C/N_0, J/S from jammers and antenna pattern characteristics) are collected by the monitoring equipment (either via real-time data streams, or by logging files for post-processing).

The C/N_0 deterioration can be tested in the absence and presence of a given interference waveform from a simulated jammer to allow performance comparison and analysis.

In addition, the scenario can be executed multiple times to enable statistical evaluation of any DUT performance variability.

Equipment Required

- 1x Keysight C50r host controller
- 2x Keysight PNT X chassis (one used to generate GNSS and the other for interference signals)
- An external RF combiner matrix, e.g. a Keysight GSS9768 microcontroller unit (MCU)
- Cables and adaptors
- DUT (7-element CRPA + Rx)

The test configuration is illustrated in Figure 3. It is assumed that the test system is factory-calibrated, so no additional equipment is required for calibration. The host controller is running SimGEN, Keysight's proprietary software suite for GNSS testing scenario definition. Once the test parameters have been configured, the user can play the scenario in real time. The host controller communicates with the signal generators, which provide the real-time GNSS / interference signals.

In this example, each signal generator provides either nominal GNSS or interference signals to each of the seven elements of the CRPA via separate RF outputs. The GNSS and interference RF outputs (14 in total) from the signal generators then become inputs to an external combiner (GSS9768 MCU), which provides seven combined (calibrated and phase-aligned) RF signals; one for each antenna element.

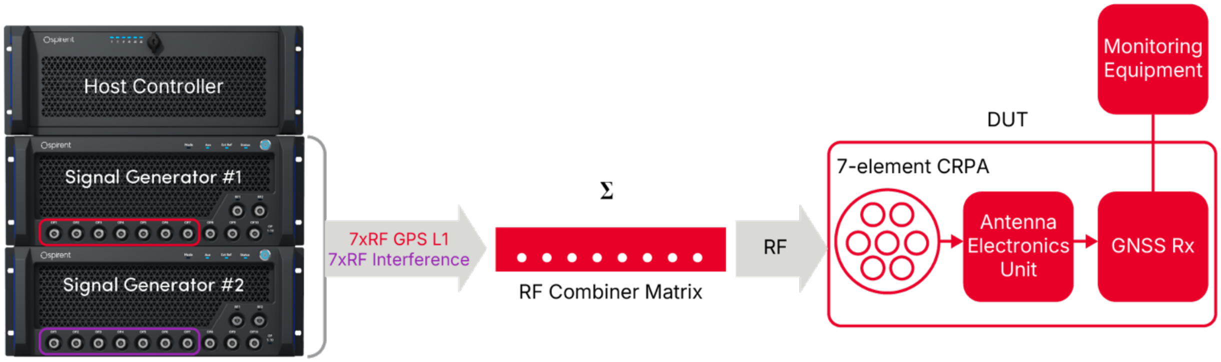


Figure 3. Example of a 7-element CRPA test configuration

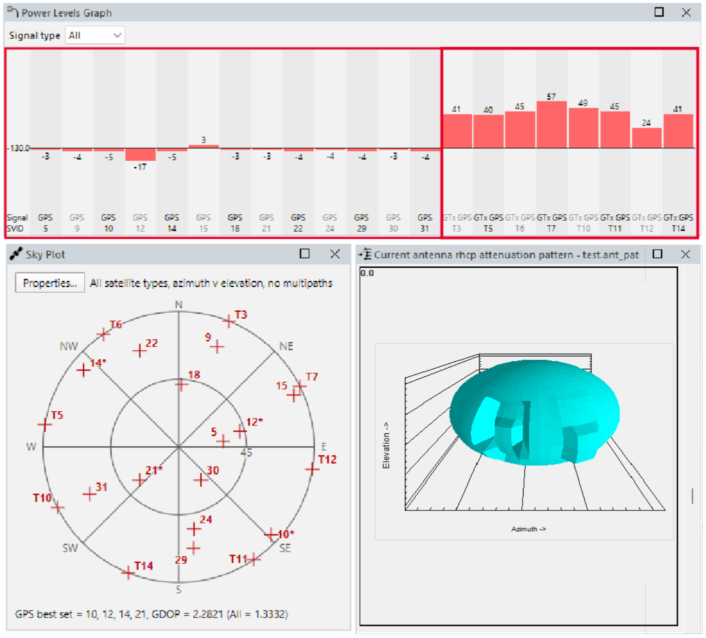
What Does the Test Do?

The scenario defines six ground-based jammers around the DUT, as shown in Figure 4. This is the maximum number of jammers that an adaptive 7-element CRPA can null by design at any given time. The example test can be split into three stages as shown in the table below.

The first stage is the DUT initialization with interference off, so that the DUT can provide a nominal navigation solution. In the second stage, the interference is turned on without turning on the CRPA adaptive algorithms. This is to quantify the deterioration of the C/N_0 and DUT performance and use it as a worst case scenario benchmark. In stage 3, the adaptive CRPA algorithms are switched on and the improvement in DUT performance can be observed in the test parameters, e.g. C/N_0, 3D accuracy, etc.

Example test stages

Test stage	Scenario time into run (hh:mm:ss)	Scenario configuration	DUT configuration	Expected result on DUT
1	00:00:00 – 00:15:00	Interference off	Initial testing state, CRPA adaptive algorithms off	DUT initialization, signal acquisition and tracking lock, nominal navigation solution output
2	00:15:00 – 00:16:00	Interference on (static jammers)	CRPA adaptive algorithms off	C/N_0 deteriorates, possible loss of code tracking lock, navigation solution outages
3	00:16:00 – 00:20:00	Interference on (static jammers)	CRPA adaptive algorithms on	C/N_0 improves, possible recovery from loss of code tracking lock and navigation solution outages



All satellite types, azimuth v elevation, no multipaths

GPS best set = 10, 12, 14, 21, GDOP = 2.2821 (All = 1.3332)

Received GPS signal levels at antenna/element

Received GTx signal levels at antenna/element

GPS & GTx transmitters in-view of antenna/element

Create antenna patterns for each antenna/element

Figure 4. Example of CRPA test scenario configuration with 6 ground-based jammers

Figure 4 shows an example of the scenario configuration with received signal strength from the GPS satellites and interference from ground transmitters (GTx) in the top window, the skyplot with nominal GPS signals (green) and ground-based jammers (red) in the lower-left window, and an antenna element 3D gain pattern in the lower-right window.

Note that it is possible to define each element antenna pattern (gain and phase) response to different carrier frequencies, e.g. L1 and L2.

Variants of this test may also be executed, for example:

- Simulate a rotating DUT at various angular rates to test how fast it responds to a changing interference environment
- Initialize the DUT with interference and CRPA adaptive algorithms on, to reflect a use case where the DUT starts operating in an environment where significant interference already exists
- Initialize the DUT at different states, to simulate cold / warm /hot starts; this is also useful when the GNSS receiver needs to be initialized via another navigation system, e.g. INS, not susceptible to RFI

Expected Results

C/N_0 and J/S vs. time diagram (static case)

A C/N_0 and J/S vs. time diagram can show the observed C/N_0 for selected satellite(s) under nominal conditions (in the absence of interference) and when interference is on.

When the interference is on, the diagram will typically show a deterioration in the observed C/N_0 measurements, e.g. a decrease or sudden drop in C/N_0, and, in extreme cases, loss of signal tracking lock (if the C/N_0 falls below a pre-defined threshold — determined by the Rx code discriminator pull-in range), especially if the angle of arrival of satellite signals is near to the direction of the jamming signals.

Note that null-steering algorithms attenuate all signals arriving from a given direction (not distinguishing between nominal satellite and jamming signals).

C/N_0 and J/S vs. time diagram (dynamic case)

Like the static case, but this test run provides additional evidence of how quickly the null-steering algorithms respond to relative dynamics between jammers and the CRPA.

For example, a jammer moving at an angular rate of 20°/s against the antenna array frame will be easier to be nulled than one rotating at 200°/s. This is equivalent to having static jammers at e.g. 3° elevation with respect to the local horizon, and the CRPA array rotating about its vertical body axis (i.e., perpendicular to the local horizon) at equivalent angular rates.

Depending on the user application, it could be either or both of the CRPA host vehicle and the jammer sources that exhibits motion dynamics.

Faster response times may be traded off with other design parameters, e.g. the null depth, or the additional processing load requirements.

Final Notes

In addition to the parameters investigated in this test, a user may wish to investigate additional parameters, for example:

- Adaptive null-steering parameters, e.g. directionality, depth and width
- Impact of back lobes on signal tracking, e.g. by artificially amplifying satellite signals

The test setup described in this section can support testing of all these parameters and more. Reliable characterization of DUT performance requires repeated experiments and analysis via appropriate metrics and statistics.

For military / defense and commercial aviation applications, this will typically encompass environmental factors (e.g., temperature range, humidity) to qualify or certify a DUT for specific operations. Detailed discussion of such test methodologies is beyond the scope of this paper.

Future Considerations

As this paper has discussed, testing of PNT systems that incorporate an adaptive antenna array can require significant investment in test equipment and resources.

To extract the full value from those investments, test teams should take into account possible future developments, both in the evolution of threats and the evolution of adaptive antenna technologies.

Evolution of Real-World Threats

Incidences of real-world GNSS jamming and spoofing continue to increase in number, magnitude of impact, and sophistication — a trend that is likely to continue as the equipment needed to build powerful jammers and spoofers becomes progressively cheaper and more powerful.

The authorized use by 5G operators of frequencies adjacent to the GNSS bands means that adjacent band interference (ABI) is also likely to become an important part of the threat landscape. While older, high-precision GNSS receivers will be most significantly affected, ABI is still likely to present a challenge for some critical safety-of-life applications.

Evolution of Antenna Technologies

New materials and design techniques will shrink the footprint of antenna arrays while retaining high levels of performance. Adaptive antenna technologies such as CRPAs and beamformers will continue to become more advanced and compact.

While the antenna electronics used to be a separate unit, it will be increasingly integrated into the antenna itself or directly into the receiver, creating new system configurations for testing.

The cost of adaptive antenna technology is also likely to reduce, along with government restrictions on the use of the technology, making it more cost-effective and accessible for commercial applications.

Conclusion

RF interference and spoofing are growing threats to safety and liability-critical PNT systems, which can be partially mitigated through the use of adaptive antenna technologies. The increasing use of adaptive antennas for commercial and military use will see a growing number of models being developed in the coming years for different industry markets.

Testing those antennas presents unique and sometimes complex challenges, which we have reviewed in this paper. Therefore, careful consideration must be exercised to select the most appropriate testing equipment for specific application needs.

Keysight stands ready to help developers, integrators and buyers of adaptive antenna-based systems to address those challenges with a comprehensive suite of solutions and services that is set out in the next section.

How Keysight Can Help

Keysight can help with every aspect of adaptive antenna system testing, drawing on our deep experience developing and implementing GNSS and inertial testing solutions.

We continuously evolve our hardware and software to address the PNT testing needs of leading organizations in the military, government, space, and commercial sectors. We generate our GNSS signals implementing the latest ICDs, using dedicated hardware and software that we develop in-house for better support and maintainability.

Keysight’s mathematical models have been proven and optimized, and we work in partnership with the leading experts in the GNSS industry. Our simulated GNSS signals are generated from first principles, via full implementation of each relevant and current ICD, and fidelity is assured through verified mathematical modeling of the signal characteristics and errors as well as relevant aspects of DUT behavior.

For adaptive antenna testing in particular, Keysight offers the following solutions and services:

Hardware

Keysight GNSS simulators cover all GNSS testing needs from receiver algorithm design to the PNT validation of the device, system, or vehicle under test. Integrating these capabilities in the same hardware unit makes it easier for designers, developers, and testers to exchange test results and share resources. Simulator solutions for antenna system testing include:

PNT X CRPA Test System

PNT X is Keysight’s 6th generation PNT simulation system and is the most powerful and capable PNT test system available today. PNT X offers an intuitive and configurable approach to define CRPA systems, easily facilitating changes and data analysis based on specific user needs.

Capable of supporting CRPA systems of 16+ elements, the 10 individual outputs can generate the most precise phase-aligned wavefront. With extensive spoofing capabilities and high J/S interference, PNT X is the ideal partner for both conducted and OTA testing.

Find out more

PNT GSS7000 GNSS Signal Simulator

The PNT GSS7000 is a multi-frequency, multi-GNSS simulator that delivers reliable results faster. Built on Keysight’s industry-leading architecture, the PNT GSS7000 combines high channel density and precision performance with the affordability to be accessible for a range of applications. Proven multi-chassis capability and in-field upgradability, powerful onboard interference availability, and dual composite RF outputs make the PNT GSS7000 an ideal solution for complex conducted and OTA CRPA test methodologies.

Find out more

Software

SimGEN: The World's Leading GNSS Simulation Software

SimGEN is the world's leading GNSS simulation software for test scenario definition, execution, data management and GNSS RF constellation simulator command and control. SimGEN supports all the GNSS test parameters and control capabilities needed for comprehensive GNSS testing for research, development, and design of GNSS systems, services, and devices across any application. SimGEN provides the following key features:

- Fully automatic and propagated generation of precise satellite orbital data, ephemerides, and almanac
- Multiplicity of mechanisms for applying declared and undeclared errors and modifications to navigation data, satellite clocks, and orbits
- SimREMOTE: comprehensive simulation control and 6-DOF trajectory delivery capability
- Data logging and streaming of signal, time, control, vehicle, and trajectory data over a variety of interfaces in real time and to file
- Range of models for multipath reflections
- Terrain obscuration models
- Independent satellite / channel signal power control
- Signal modulation and code control
- Multi-copy constellations for spoofing testing
- Multi-vehicle to 1RF for trajectory spoofing
- Vehicle personalities and motion modeling for aircraft, spacecraft, marine vessels, and land vehicles
- Antenna reception gain and phase patterns
- Satellite transmit antenna pattern control
- Clock g-sensitivity
- Antenna lever arm effects
- INS aiding data
- Ionosphere and troposphere effects including ionospheric scintillation
- DGPS / RTK corrections
- Pseudorange ramps (for RAIM testing)
- Leap-second and week roll-over event testing

Find out more

Sim3D: Realistic Environment Modeling

Sim3D is Keysight's integrated 3D signal propagation environment modeling tool. Combining OKTAL's SE-NAV with Keysight's GNSS simulation systems, Sim3D enables the creation or import of a wide range of realistic environments, attenuating simulated GNSS signals and modifying angle of arrival according to the calculated multipaths.

Sim3D can be used for testing and characterizing a nulling / beamforming algorithm using simulated GNSS and interference signals that are representative of real-world effects.

This test can be carried out in conducted mode or in a chamber environment. In conducted mode, the user can import their own RHCP / LHCP antenna pattern to the simulation. Sim3D will ensure the gain and phase of the signal is adjusted based on the polarization of the signal.

Find out more

SimINERTIAL: Emulation of Inertial Sensor Outputs

For adaptive antenna-based systems that also include IMUs, Keysight's SimINERTIAL software can emulate inertial sensor outputs in sync with GNSS RF signals. Supporting a wide range of sensor types, and many of the leading integrated GPS / inertial systems (IGIs) and embedded GNSS / inertial systems (EGIs), the SimINERTIAL series dramatically reduces the need for costly and time-consuming field trials in the development stages.

Find out more

Zoned chamber solutions

For a zoned chamber configuration, Keysight can offer a unique solution of synchronous transmission of L1, L2, and L5 signals with angle of arrival in the anechoic chamber, which is a critical testing factor for high-end CRPAs.

Interference testing to exercise null-steering CRPA algorithms can also be integrated, by adding physical jammers (beacons) in the Keysight chamber solution that are synchronous to the generated GNSS signals.

All these readily available options are built on the world-leading performance of the Keysight simulators, with up to 1 kHz update rate and external motion input, signal fidelity, and spectral purity to support the most demanding high-dynamics applications and enable a thorough and reliable performance analysis of the system under test.

Chamber solutions are built on the leading performance of Keysight simulator platforms; GSS7000 for civil aviation automotive testing, and PNT X for high-end testing applications, for example an aircraft maneuvering at high speed. Keysight can synchronously combine tens of chassis to simulate 1,000+ independent channels simultaneously with multi-frequency, multi-constellation support for 16+ CRPA elements.

In addition, Keysight chamber solutions can offer support for 3D environment modeling to overlay multipath interference for more realism.

Keysight chamber solutions cover all CRPA testing requirements, ranging from civil, commercial, R&D to military and defense applications.

Services

Keysight has a dedicated team capable of delivering a range of services, from identifying your CRPA testing requirements to turn-key system installation and calibration. Services you may require as part of the system delivery, during subsequent use, or as a standalone evaluation include:

Consultancy: Keysight experts can provide a range of consultancy services, from requirements definitions, advice, and guidance to help with testing and evaluating results. Defined goals and timelines will help you deliver better systems ahead of time.

Receiver audit: Keysight will run a test suite to assess the performance of your GPS or multi-GNSS receiver and provide a report. The test suite can be run at a Keysight services lab or at your own site.

Training: Keysight representative(s) can deliver training at your site following successful completion of system installation and acceptance tests. It can involve classroom-style training / presentation sessions as well as "hands-on" demonstrations with the CRPA test system where appropriate.

Scenario generation: Keysight has the expertise to deliver scenarios bespoke to any agreed customer use case — whether OTA, conducted, or a combination of the two. Our services team of engineers will deliver pre-defined scenarios that can easily be loaded and played for comprehensive, expert CRPA testing.

Additionally, Keysight offers a global technical support network, with experienced test engineers and consultants available to resolve any technical questions and advise on how to achieve and maintain the best calibrated performance from your system.

To discuss any aspect of your PNT vulnerabilities testing, please contact us.

Contributors

Guy Buesnel, CPhys, MInstP, FRIN, RNTF

Guy has more than 20 years' experience protecting GNSS receivers from emerging threats, having started his career as a systems engineer involved in the development of GPS adaptive antenna systems for military users. Guy holds a BSc honors degree in physics with atmospheric physics and a master's degree in communications engineering.

Guy is a member of the Institute of Physics, a Chartered Physicist, a Fellow of the Royal Institute of Navigation, and in 2019 was appointed as a member of the International Advisory Council for the Resilient Navigation and Timing Foundation.

Kimon Voutsis, PhD, AFRIN

Kimon is responsible for providing high-end GNSS test solutions to military, government, GNSS, and space organizations. He is interested in all aspects of GNSS vulnerabilities and threats, with a particular focus on spoofing and jamming. He has authored and co-authored many technical reports and publications. He is an Associate Fellow of the Royal Institute of Navigation and holds a master's degree and a doctorate in positioning, navigation, and timing applications, both from University College London (UCL).

Ajay Vemuru, MSc

Ajay Vemuru is a product manager who helps the robotics community build safer and more reliable location-aware platforms.

Ajay has worked as a software engineer and research engineer at two of the leading semiconductor companies in Silicon Valley, with a successful career researching advanced location algorithms and developing software for improving location-based services on mobile devices, as well as launching new solutions to automotive and robotics customers.

Glossary of Abbreviations

The following abbreviations have been used in this paper:

ABI	Adjacent-band interference
AoA	Angle of arrival
API	Application programming interface
AWGN	Additive Gaussian white noise
Ax	Antenna
C/N_0	Carrier-to-noise
CRPA	Controlled radiation (or reception) pattern antenna
DUT	Device under test
EGIs	Embedded GNSS/inertial systems
EW	Electronic warfare
FRPA	Fixed radiation (or reception) pattern antenna
GNSS	Global navigation satellite system
GPS	Global Positioning System
GTx	Ground transmitter
HIL	Hardware in the loop
ICD	Interface control document
IGIs	Integrated GPS/inertial systems
IMU	Inertial measurement unit
INS	Inertial navigation system
ISG	Interference signal generator
J/S	Jammer/signal
LHCP	Left hand circularly polarized
MCU	Microcontroller unit
OTA	Over-the-air
PNT	Positioning, navigation and timing
PPD	Personal privacy device
PV	Position, velocity and time
RF	Radio frequency
RFCS	Radio frequency constellation simulator
RFI	Radio frequency interference
RHCP	Right hand circularly polarized
RPS	Record and playback system
Rx	Receiver
SDR	Software-defined radio
SFAP	Space-frequency adaptive processing
SIS	Signal-in-space
STAP	Space-time adaptive processing
SV	Space vehicle
Tx	Transmitter

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

Published in USA, June 1, 2026, 3126-1203.EN