Simulating NAVWAR

Creating ultra-realistic PNT test scenarios in the lab

eBook

KEYSIGHT

NAVWAR Developments Demand a New Approach to Testing

Navigation warfare (NAVWAR) is evolving, with the emergence of new threats, new mitigation techniques and new defensive capabilities.

In terms of threats, recent years have seen a significant increase in the use of radio frequency (RF) jamming and spoofing techniques to disrupt enemy operations. On the mitigation side, encrypted global navigation satellite systems (GNSS) signals like M-CODE, MNSA, Galileo PRS, and the forthcoming GPS Regional Military Protection (RMP) signals provide greater threat protection, while new low Earth orbit (LEO) and ground-based services provide alternative or enhanced navigation capabilities.

Positioning, navigation, and timing (PNT) user equipment (UE) is also advancing with the development of more sophisticated antennas and signal processing algorithms to detect, reject, and avoid spoofed signals and jamming waveforms. New sensor fusion capabilities also allow user equipment to blend navigation signals.

What is NAVWAR?

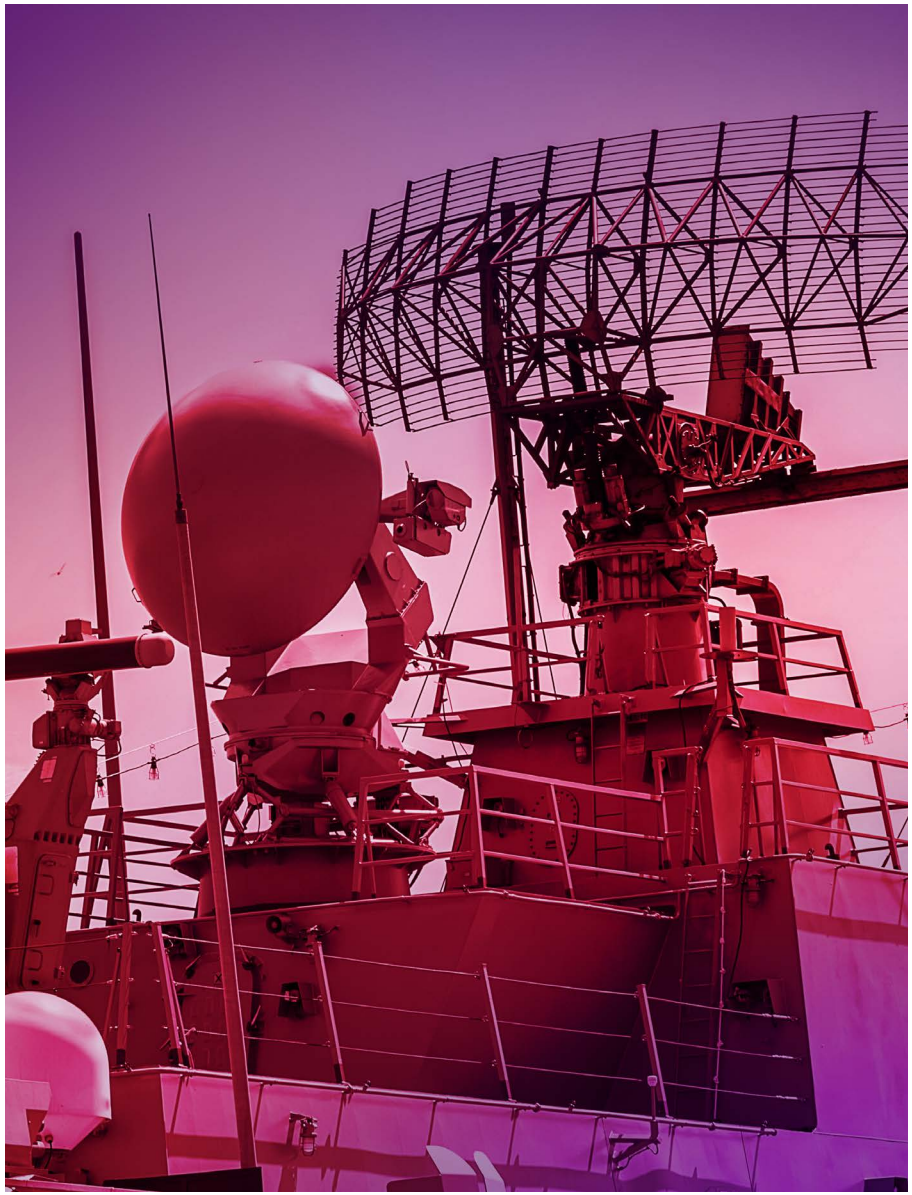
Navigation warfare (NAVWAR) is a type of electronic warfare (EW). It refers to the deliberate disruption of an adversary's ability to navigate accurately and reliably. Offensive NAVWAR tactics typically include signal jamming and signal spoofing, while defensive measures typically involve hardening PNT equipment against jamming and spoofing threats. Read more on the Keysight blog.

Building ultra-realistic NAVWAR test scenarios

Developing robust PNT solutions for today's NAVWAR environments requires a comprehensive test approach. This eBook will review five complex requirements of NAVWAR PNT testing in the lab and detail how developers can meet these requirements through realistic, repeatable simulation.

Read on to learn about key lab testing considerations and how these support the development of robust and resilient systems.

- High-dynamic trajectories and responsive vehicle models
- Controlled reception pattern antenna (CRPA) system modeling and evaluation
- Encrypted GNSS signals and complementary PNT
- Complex jamming and spoofing threat evaluation
- Modeling environmental obscuration, diffraction, and multipath effects



Contents

CHAPTER 1

High-Dynamic Trajectories

High-Dynamic Trajectories

Because of the nature of the NAVWAR environment and the platforms operating within it, scenarios often involve high speeds, rapid acceleration and deceleration, jerk, and rapid spinning. Such platforms may include missiles, crewed aircraft, or drones.

Remaining true to the defined trajectory and dynamics is critical in providing a realistic evaluation of the performance of the device under test (DUT). With the elevated demands of highly dynamic platforms, this requires a high simulation iteration rate. In addition, in hardware-in-the-loop (HIL) environments, low latency between all equipment in the loop is integral to following precise trajectories and delivering actionable data.

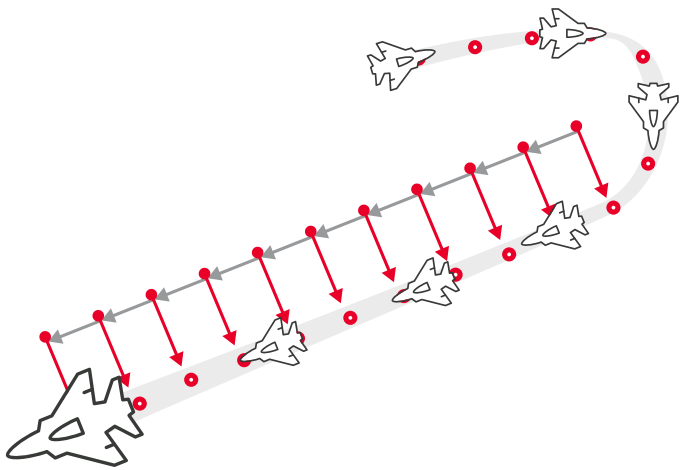


Figure 1. Illustration of trajectory sampling

Update rates

The most obvious limiting or enabling factor when it comes to simulating high-dynamic trajectories is the update rate of the simulation system.

As with all digital systems, simulated trajectories are made up of a series of single-position iterations. Unless a vehicle moves at a consistent speed in a straight line throughout the scenario, there will inevitably be deviations from the true trajectory. For instance, if a military jet performs a smooth bank, the simulator will plot a series of points (referred to as samples) on that turn, and the simulated vehicle will effectively move in a straight line between each sample. The fewer the samples — the lower the update rate — the more angular the turn will be represented in the test. Conversely, a high iteration rate will sample the plotted trajectory more frequently, more closely following the correct path.

A 2 kHz update rate — as is standard with the Keysight PNT X simulation system — delivers the most realistic trajectories available in test. Without high update rates for dynamic vehicles in NAVWAR test environments, assessing the impact of NAVWAR attacks on the vehicle-under-test (VUT) becomes significantly less precise and representative. Errors in trajectory could be accountable to the attacks, or they could represent the inherent errors in the original plotting of the course by the test equipment.

Spinning vehicles

Spinning vehicles create a further headache for testers in accurately modeling PNT solutions. As the vehicle rotates on its axis, the GNSS antenna (or antennas) experience rapid and continuous changes in pseudorange. The faster the vehicle spins, and the greater the diameter of the vehicle, the greater and the faster these changes will be. For hypersonic projectiles, even a 2 kHz update rate may not be able to render the most realistic trajectory.

To support the testing of these highly demanding, high-dynamic vehicles, Keysight has introduced a dedicated 100 kHz update rate for spinning vehicles with PNT X. This enables position and navigation modeling with the level of precision needed for mission-critical projectiles. Again, without the assurance of such a level of precision, NAVWAR testing will be conducted from an unstable baseline.

Hardware-in-the-loop (HIL)

While update rate remains of great importance in HIL testing, developers also need to consider system latency — small delays in data transfer between different pieces of equipment in a test setup or between different electronic components within a piece of equipment.

In an HIL environment with real-time inputs and feedback loops, latency is an inevitability. It manifests in test results as uncertainty — and the greater the latency, the greater the uncertainty. In terms of plotting trajectories, maintaining low and consistent latency means the truth data provides the most accurate possible baseline for assessing the impacts of NAVWAR attacks on the vehicle-under-test.

For more information about latency in simulation, read our white paper.

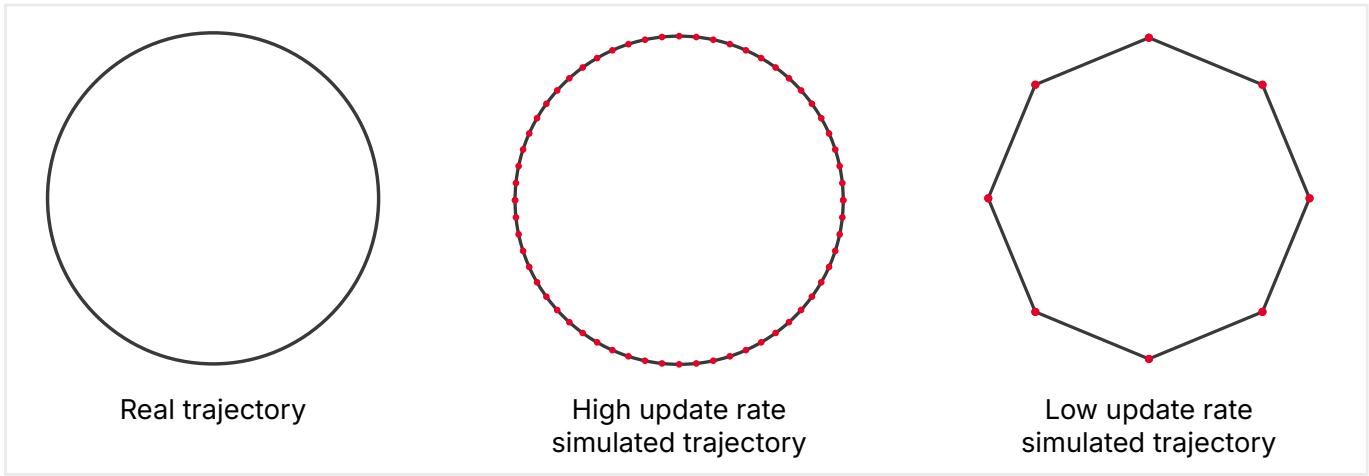


Figure 2. Example of plotting a circular course with differing update rates

CHAPTER 2

Testing Controlled Reception Pattern Antenna (CRPA) Systems

CHAPTER 2

Testing Controlled Reception Pattern Antenna (CRPA) Systems

With multiple independent antenna elements and null-steering and beamforming capabilities, CRPAs are an essential part of the defense toolkit for mitigating RF jamming and signal spoofing threats. However, these adaptive antenna systems require advanced simulation capabilities for realistic lab testing — both in conducted testing and over-the-air (chamber-based) testing.

In conducted testing, a key challenge is defining and controlling the antenna in the simulator. Antenna elements must be correctly defined and positioned to reflect their real-world characteristics. Depending on the use case, the antenna system may also need to be defined as part of a larger vehicle.

The simulator must also be able to realistically and repeatedly simulate the propagation of a jamming wavefront, or a spoofing attack, across the antenna elements — with precise phase alignment and without introducing unwanted test artifacts. Adding high dynamics also necessitates a simulator architecture that generates predictably repeatable and precise signals.

The key to the power of a CRPA is not all in the antenna hardware (though it is highly significant); it is also in the signal processing algorithms and electronics that control the null steering and the beamforming. These must be refined and validated in the lab in order to ensure performance in the harshest NAVWAR environments, and this necessitates testing that incorporates both realism and diversity of attack vectors.

CHAPTER 3

Encrypted GNSS Signals and Complementary PNT

CHAPTER 3

Encrypted GNSS Signals and Complementary PNT

NAVWAR test scenarios for defense applications must incorporate the increasingly diverse array of signals used by military vehicles and equipment to navigate in challenging environments. Understanding the performance and the limitations of each of these, and how they can work in concert, creates unique challenges for labs. The test equipment used must be able to generate all of the required signals, sometimes concurrently, and the system must deliver the security required by secure lab environments.

For authorized users, encrypted signals may include GPS M-Code, Regional Military Protection (RMP), MNSA, and Galileo PRS. In addition, complementary PNT might include the LEO PNT systems under development, such as Xona Space Systems' Pulsar constellation. Furthermore, the ability to incorporate new planned and proposed signals into the environment without sacrificing performance or realism can be a critical enabler in the fight to stay ahead of NAVWAR adversaries.

From an alternative standpoint, these flexible capabilities can also help in the development of offensive NAVWAR vectors. The ability to model signals, to generate them in dynamic scenarios with uncompromised realism, and the ability to evaluate the impact on hardened PNT equipment creates a powerful iteration and validation toolset to help win in the NAVWAR domain.

CHAPTER 4

Complex Jamming and Spoofing Threats

CHAPTER 4

Complex Jamming and Spoofing Threats

In NAVWAR scenarios, equipment may encounter jamming and spoofing threats both individually and in complex combinations. Equally, jamming and spoofing, individually or in combination, may be used defensively to protect key assets. Organizations need to be able to create complex threat conditions realistically in the lab to understand how equipment will perform in an infinite variety of scenarios.

Even a typical spoofing scenario might incorporate jamming as a means to trick the receiver into accepting the spoofed signals. In addition, with highly dynamic vehicles under test, it is necessary to assess the impacts of these varying threats as the vehicle moves through an environment. This means test equipment not only needs to support the generation of a wide range of attacks, but also to be able to model these situationally within the test environment.

From an alternative viewpoint, organizations could use this capability to play custom waveforms from predefined I/Q files to model how they might impact an adversary in different scenarios. The ability to apply spatial realism to custom waveforms in the simulator, and to model them within a customizable 3D environment, could allow users to develop situationally effective measures.

A key consideration with jamming and spoofing scenarios is dynamic range. This is best understood as the maximum power of the jamming signal in relation to GNSS signals in a scenario. As RF threats grow in power and sophistication, this is highly important, but is not the only consideration with regard to dynamic range.

In the real world, vehicles are typically in motion relative to the source of a jamming or spoofing signal. As the vehicle approaches the interference source, the noise from that source increases relative to the GNSS signals in the environment, resulting in a progressively higher jammer-to-signal (J/S) ratio. A realistic scenario needs to be able to model the changing J/S ratio as the vehicle moves toward and away from the jammer or spoofer, ideally from a start point where the interference signal is not yet in range of the receiver, and is thus lower than the noise floor. In order to qualify receivers in these dynamic scenarios, dynamic range must be both high and continuous.

CHAPTER 5

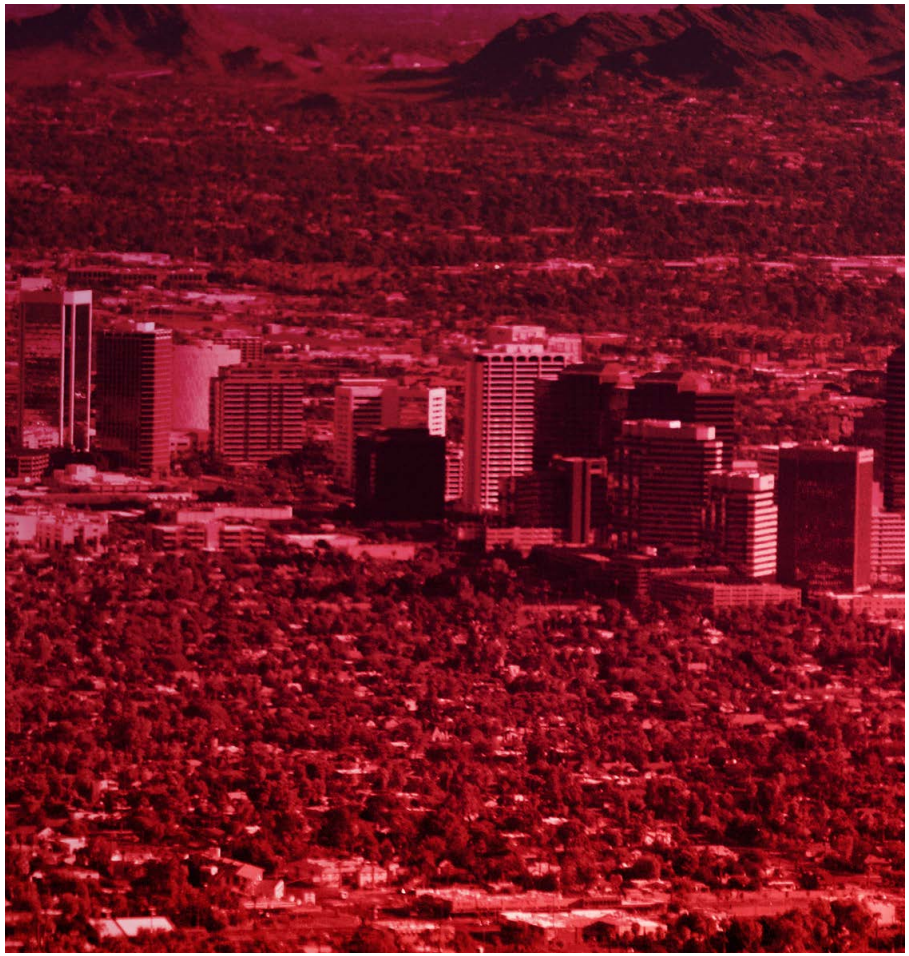
Obscuration, Diffraction, and Multipath Effects

CHAPTER 5

Obscuration, Diffraction, and Multipath Effects

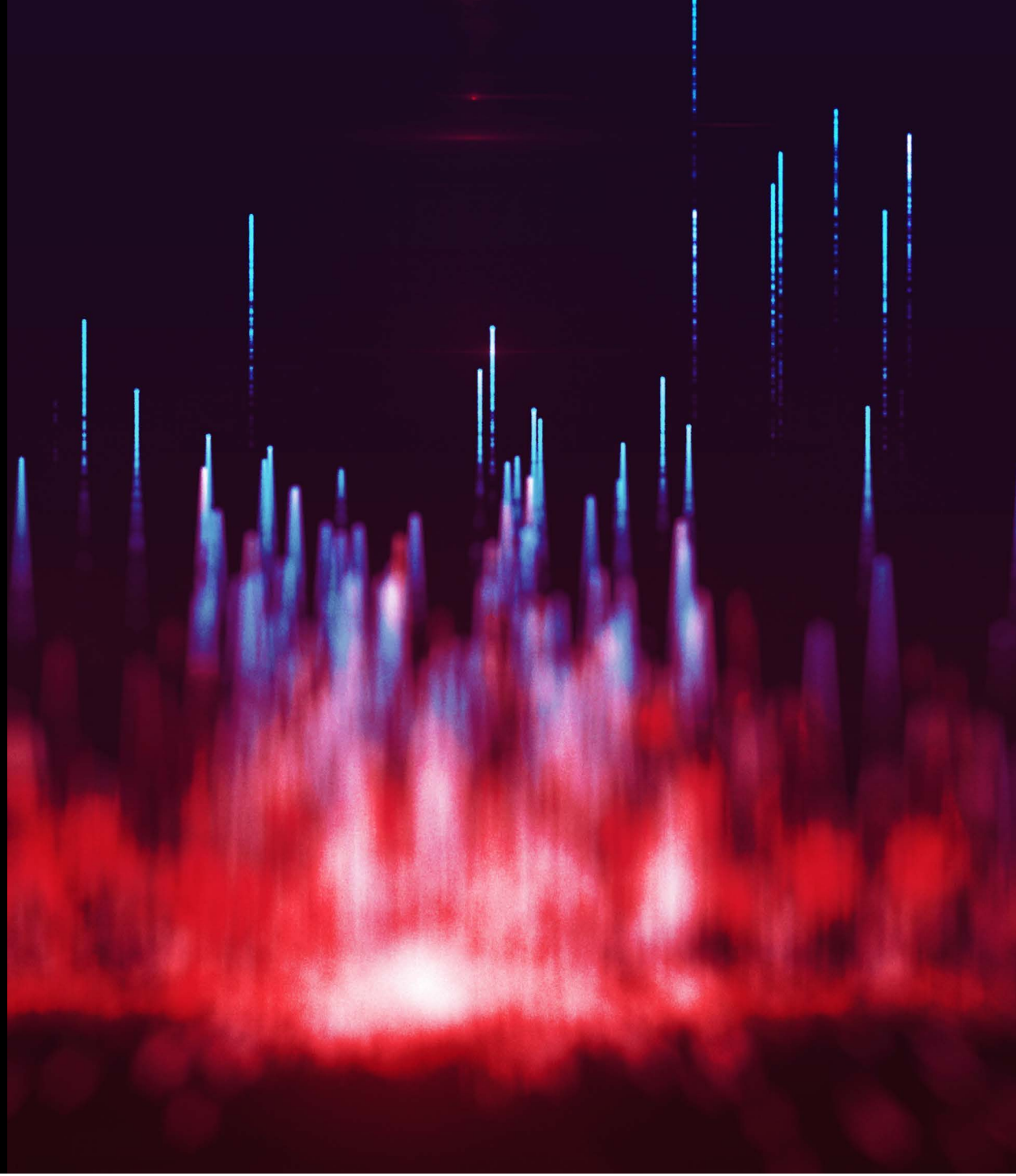
Understanding receiver or transmitter performance in real landscapes is key to the development of effective equipment. Signal obscuration, diffraction, and reflection (multipath) caused by obstacles in the environment can significantly affect performance. The full impact of these artifacts can sometimes not be realized until late in the development cycle, when testing is carried out on a physical test range.

Applying a 3D terrain model to a simulated scenario enables the use of each of these effects within a NAVWAR context, adding another layer of realism that would be extremely difficult to replicate in the field. It should be considered that this capability would need to be complemented by a signal capacity that can support reflected as well as line of sight (LOS) signals.



CHAPTER 6

Overcoming NAVWAR Threats with PNT X



CHAPTER 6

Overcoming NAVWAR Threats with PNT X

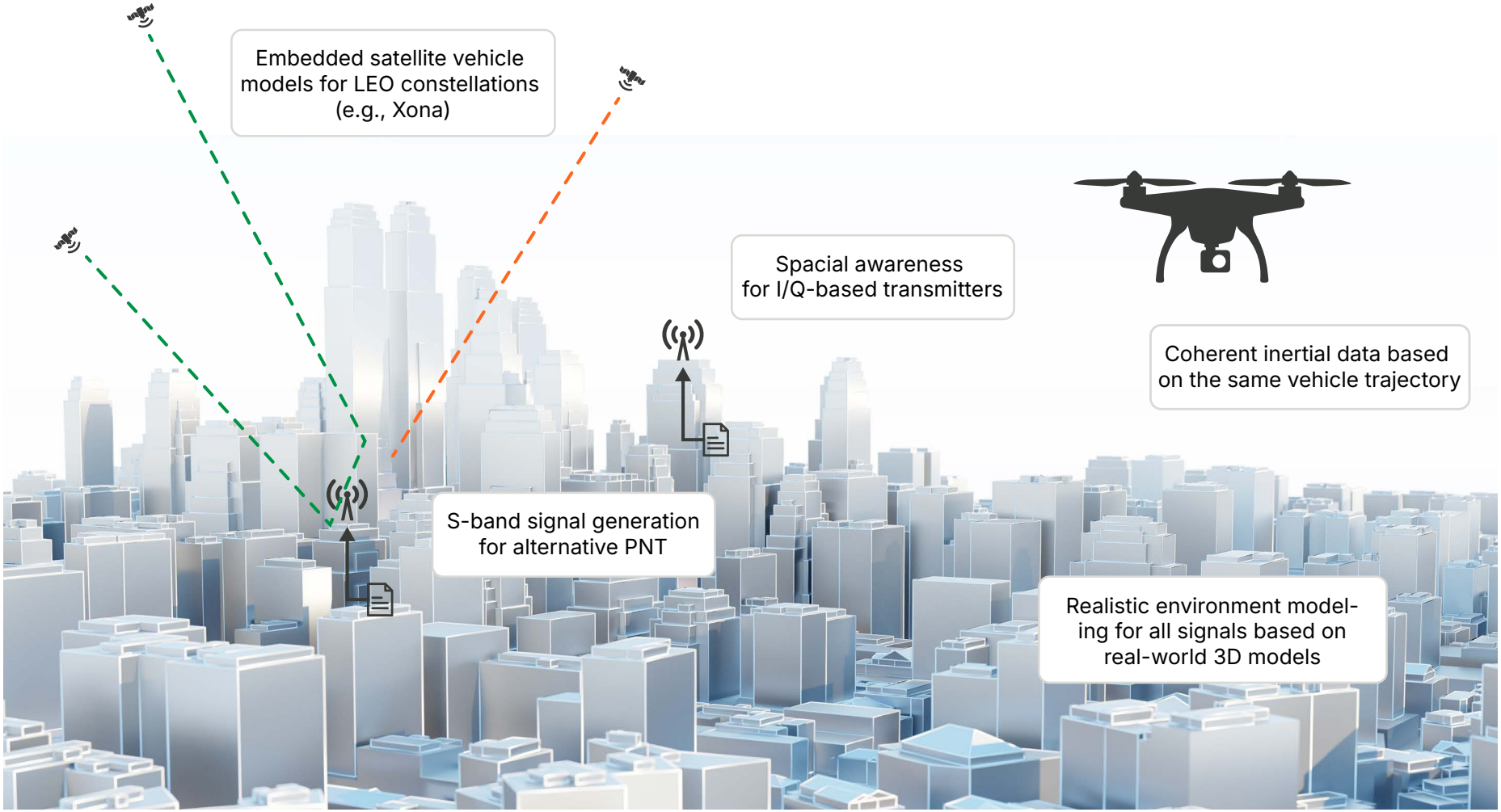
As NAVWAR threats and techniques evolve, scenario testing equipment must evolve too. Keysight has designed PNT X to be the most powerful, capable, and realistic NAVWAR test platform available today, drawing on our years of expertise and innovation in PNT test and measurement. Essential NAVWAR features in PNT X include:

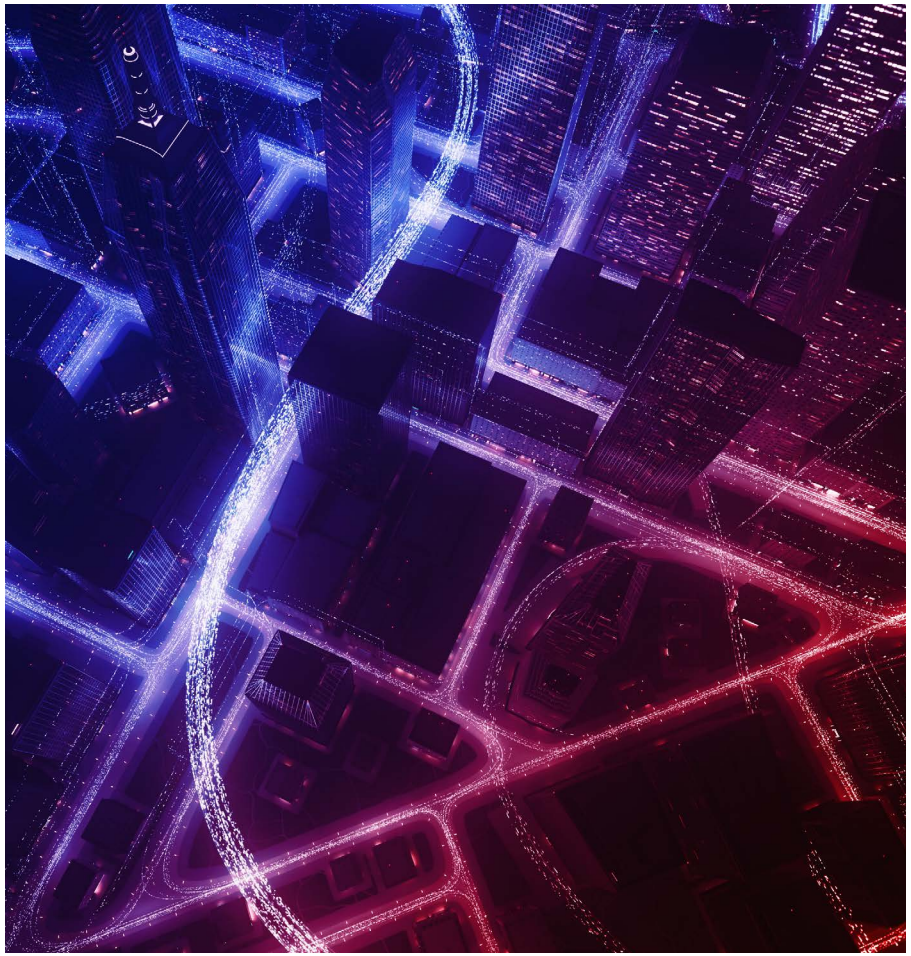
Unprecedented signal capacity: PNT X is the first simulator to enable up to 640 independent signals to be generated simultaneously from the same unit with no loss of performance. PNT X supports all GNSS constellations and frequencies as standard, as well as LEO PNT signals, S-band signals, inertial sensor outputs, interference signals and waveforms, reflected and diffracted signal paths, and I/Q-defined transmitters.

2 kHz update rate (optional 100 kHz for spinning vehicles): With motion data represented at RF unlike any other platform, PNT X can realistically model the highly dynamic trajectories of projectiles, drones, and warfighters, generating a true representation of real-world performance. A standard 2 kHz update rate allows dynamic applications to be tested with unprecedented realism, including in hardware-in-the-loop (HIL) testing, while an optional update rate of 100 kHz allows users to better model the pseudorange changes of fast-spinning vehicles of different diameters. A faster update rate also reduces latency for HIL test environments (2 ms in all scenario configurations), enabling trajectory and motion data from third-party hardware and software systems to be processed faster and more precisely.

Simplified CRPA testing: PNT X offers an intuitive, configurable interface for defining controlled reception / radiation pattern antenna (CRPA) systems, easily facilitating changes and data analysis based on specific user needs.

Alternative, complementary, and encrypted signals: PNT X supports a wide range of encrypted, alternative, and complementary PNT signals, including GPS M-Code, MNSA, Galileo PRS, the Xona Pulsar LEO PNT constellation, and S-band and custom L-band signals. It is the first simulator to support planned GPS Regional Military Protection (RMP) anti-jam signals, allowing authorized developers to test modernized GPS user equipment (MGUE) before live signals are available.





Spatial awareness for custom I/Q-defined transmitters: SimIQ Spatial Awareness is a new, patented solution for signal architects and developers seeking to use custom waveforms in simulation scenarios. It automatically applies realistic signal effects, such as power level offsets, signal delays, and Doppler shift, to user-defined signals, for unprecedented realism in NAVWAR scenarios.

Enhanced dynamic range: An enhanced dynamic range allows the maximum output power level to accommodate high-power interference transmitters and spoofers alongside low-power GNSS signals, providing an increased J/S ratio for realistic NAVWAR scenarios. Continuous dynamic range of 140 dBs also enables full power level characterization of the transmitter across the range, mirroring scenarios like a high-velocity vehicle flying by several interference transmitters.

3D terrain modeling: A 3D scenario tool with real-time visualization brings the NAVWAR test range into the lab, allowing test scenarios to be run in spatially realistic environments. The 3D scene is applied to all RF generated signals — including, for instance, geolocated jamming transmitters generating novel waveforms from user-defined I/Q files. Realistic obscuration and multipath signatures can be generated. Users can import their own 3D maps or use pre-loaded maps of cities and landscapes around the world, with the tool visualizing the physical environment for real-time insight into the effects of obstacles on signal transmission and reception.

CONCLUSION

The Ultimate Test Platform for Realistic NAVWAR PNT Scenarios

NAVWAR threats and mitigations continue to grow in variety and complexity, and the use of NAVWAR techniques in conflict situations continues to expand. Developers of equipment and signals need test instruments that can accurately emulate complex RF environments in challenging terrain. The ability to create realistic scenarios in the lab can drastically reduce the time and cost of range testing, improving the robustness and speed of development cycles.

Keysight has made this possible with PNT X, the ultimate test platform for ultra-realistic NAVWAR PNT scenarios, built on Keysight's deep experience at the forefront of PNT test and measurement. If you would like to learn more about PNT X or discuss your specific NAVWAR test requirements, visit our PNT X product page or get in touch.

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.