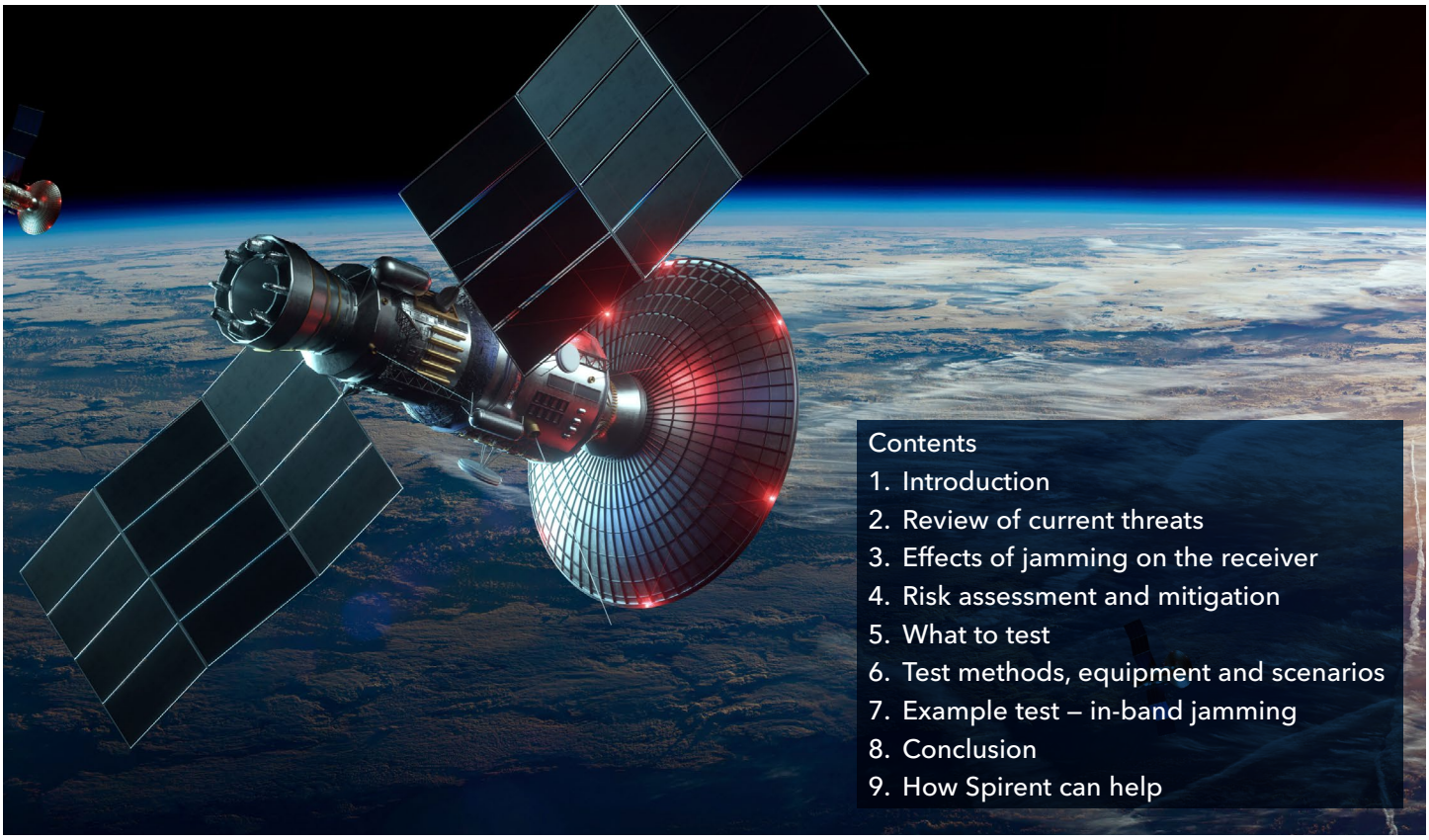
White Paper



Contents

1. Introduction
2. Review of current threats
3. Effects of jamming on the receiver
4. Risk assessment and mitigation
5. What to test
6. Test methods, equipment and scenarios
7. Example test – in-band jamming
8. Conclusion
9. How Spirent can help

GNSS Jamming

How to test the risks to safety-critical and liability-critical systems

A Spirent white paper for developers and integrators of GNSS receivers

1. Introduction

As industries rely more heavily on GNSS signals for positioning, navigation and timing (PNT), radio frequency (RF) interference from signal jamming is a growing threat.

Whether intentional or unintentional, jamming can have a significant impact on the performance of GNSS receivers – including those used for safety-critical and liability-critical operations.

Developers and integrators of GNSS receivers must fully understand the risks presented by jamming, and design mitigation measures that ensure receivers and their users are adequately protected. Understanding receiver performance in a wide range of realistic jamming scenarios is an important part of that process, and simulation is essential to characterise and compare performance in repeatable conditions.

This paper is written for designers and developers of GNSS chipsets and modules, as well as organisations selecting or integrating a GNSS receiver for a safety-critical or liability-critical system. It reviews the growing threat from GNSS signal jamming, and the unpredictable effects it can have on GNSS receivers. It sets out the methods by which receivers can be thoroughly tested to understand how they behave in different jamming scenarios, and provides an example test description from Spirent's library of interference test packs.

2. Review of current threats

Jamming interference to GNSS receivers is a growing threat as more systems and devices rely on GNSS for PNT. The European GNSS Agency (GSA) estimated there were 6.4 billion GNSS-enabled devices in use worldwide in 2019, and forecasts this will rise to 9.5 billion by 2029 – equivalent to 1.1 devices for every person in the world.

Many of those receivers are used in safety-critical and liability-critical systems. In the US, 13 of the 16 sectors of critical national infrastructure rely on GNSS, according to the Department of Homeland Security. The more the world relies on GNSS, the greater the threat presented by RF interference – whether intentional GNSS frequency jamming by malicious or mischievous actors, or unintentional interference from radio transmissions in bands close to the GNSS frequencies.

The impact of jamming is being felt worldwide. In the maritime sector, jamming traced to the Syria conflict has been disrupting shipping in the Eastern Mediterranean since 2018. In aviation, the number of reports of suspected GPS signal jamming made to NASA's Aviation Safety Reporting System (ASRS) has been steadily rising (Figure 1). And in road transport and logistics, illegal jammers are widely used to disrupt employer telematics, as well as for criminal activities.

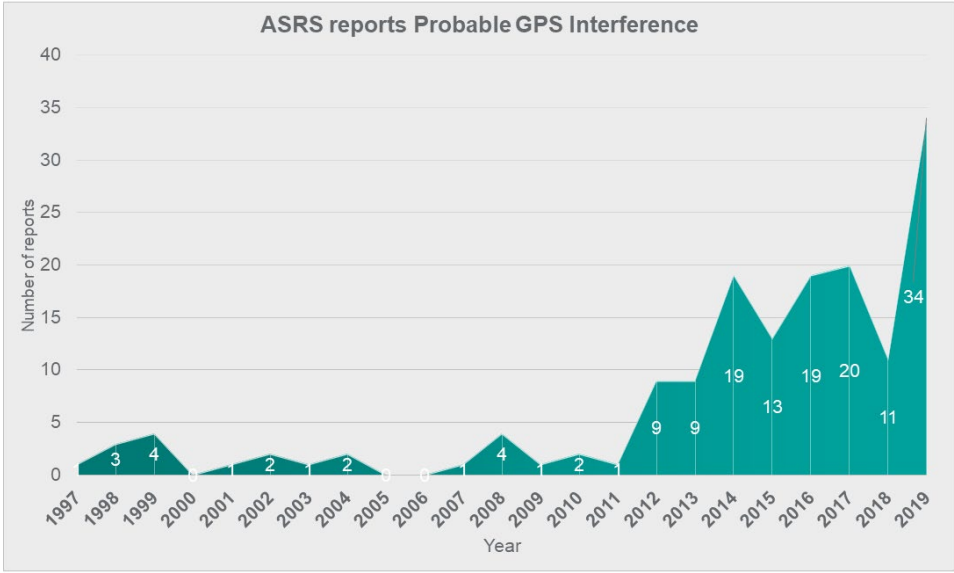


Figure 1: Reports of GPS interference made by pilots to the NASA Aviation Safety Reporting System

Types of GNSS jammer and jamming signal

The equipment used for signal jamming varies, as do the characteristics of the jamming signals. Small, cigarette lighter-type jammers are designed to disable tracking devices in cars, vans or lorries, and broadcast white noise on the GPS L1 frequency at power levels of 10 mW or similar.

More sophisticated 'hedgehog' jammers, favoured by criminals, are designed to jam multiple radios simultaneously, including Wi-Fi, cellular and GNSS. Recently, GNSS frequency jammers have started to appear online that broadcast white noise at a power of around 10 W (Figure 2). Marketed as anti-drone weapons, they are capable of causing interference over a very wide range.

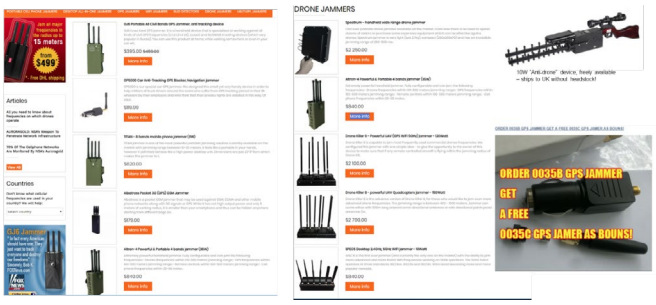


Figure 2: Illegal jammers are readily available to buy online

Most of these jammers are of the CHIRP type, and operate across the band 1565 – 1585 MHz. The jammer changes frequency rapidly over time and sweeps across the frequency, overpowering the GNSS signal. The use of frequency sweeping means that a narrowband jammer can be used to overpower a frequency range which would otherwise have required a broadband jammer. Some of these jammers operate with a sawtooth waveform (Figure 3), while more sophisticated devices use frequency burst techniques in addition to CHIRP.

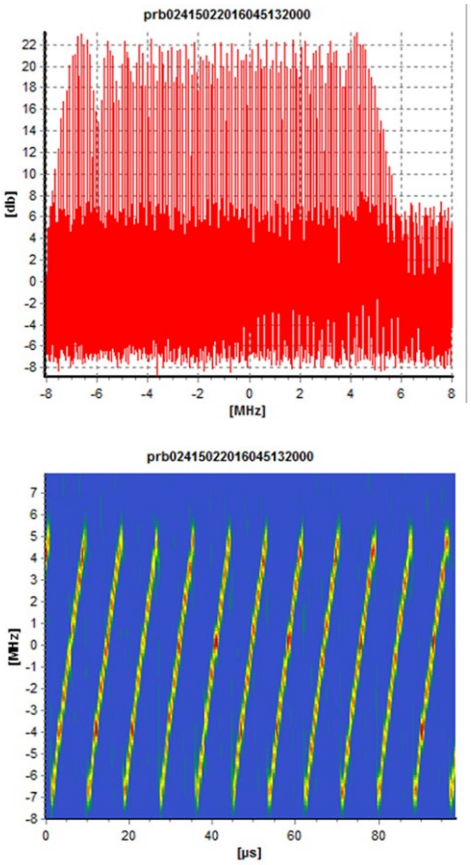


Figure 3: Sawtooth jamming waveform detected by Spirent near an airport in Germany

As well as in-band interference from jammers, receivers may also encounter interference from RF equipment broadcasting (legally or illegally) on frequencies close to GNSS. ABI is a growing threat as the available radio spectrum is increasingly squeezed, leading to regulations like the EU's Radio Equipment Directive (RED), which requires electronics equipment manufacturers to ensure RF emissions from their products do not cause harmful interference to other spectrum users.

Faulty radio equipment can also transmit erroneously on the GNSS bands, and receivers may also encounter in-band interference from poorly housed or sited circuitry within the same system.

3. Effects of jamming on the receiver

Understanding the impact of jamming on the receiver is a critical first step to designing mitigation measures. The effects can vary dramatically, depending on variables like the type of jammer, its distance from the receiver, and the surrounding physical and RF environment.

The manufacturer's spec sheet will often provide information on a receiver's performance under interference conditions. However, a lack of standardised metrics means that relying on information provided in these is not advisable. Test parameters, conditions and environments vary between manufacturers, and it would be near impossible to cover the comprehensive range of interference conditions. Our own tests at Spirent have found that receiver performance can vary significantly from the spec sheet: sometimes exceeding and sometimes falling short of the stated values.

Integrators comparing multiple receivers during a selection process will find that identical jamming conditions affect different receivers in different ways. It is often assumed that exposure to GNSS jamming invariably means a loss of signal, but extensive testing in the Spirent laboratory has shown that the effects vary from:

- **No effect at all –** if the jammer is out of range, or its centre frequency is not aligned with the target GNSS frequency
- **Degradation of GNSS signals –** as the carrier-to-noise (C/N_0) ratio of received signals drops, affecting the dilution of precision (DOP) value (often lower-elevation signals are affected first)
- **Complete loss of tracking of GNSS signals and saturation of the receiver front end –** meaning the receiver will need to re-acquire the signals

Degradation of signals

Of these three effects, degradation of signals is often the most dangerous because it can cause the receiver to output significant position or timing errors. Our tests have shown that if a receiver is moved slowly towards a jammer, a gradual degradation in performance can be observed as the C/N_0 of received GNSS signals starts to deteriorate.

A well-accepted parameter for assessing the point after which increased interference is likely to result in reduced performance and erratic receiver behaviour is the 1-dB Interference Protection Criterion (IPC). Once this point has been passed, a measurable loss of performance in terms of Horizontal Positioning Error (HPE) can be observed.

The chart on the following page shows the observed effect on a GPS receiver that is gradually exposed to adjacent-band interference (ABI) at the levels specified in the EU's RED. Gradually increasing the power level of the ABI can be thought of as analogous to the receiver moving gradually closer to the source of the interference.

As the power of the RF signal increases, there is a point at which the C/N_0 of the received signals drops by greater than 1 dB. Until this point there is no measurable effect on the HPE of the receiver under test. This test was conducted using the following assumptions:

- The power of the interference reduces with range according to the Friis free space propagation equation, which assumes a clear line of sight between the receiver and the interference source:

$$P_r = P_t + G_t + G_r + 20\log_{10}\frac{\lambda}{4\pi R}$$

- The received level of GPS signals at the antenna should be at a nominal level of -158.5 dBW for GPS L1 C/A signals, as set out in the relevant GPS Interface Control Document (ICD)

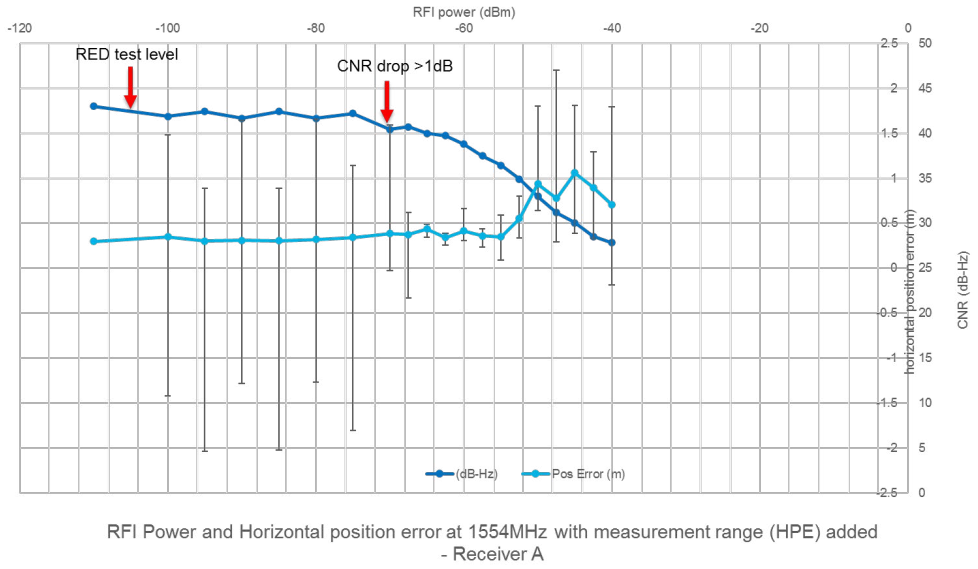


Figure 4: Observed effects of adjacent-band interference on HPE in a GPS L1 receiver

4. Risk assessment and mitigation

Given that receivers can behave erratically under some jamming conditions, thorough risk assessment is essential. Receiver developers and integrators will want to assess the impact on the operation of the receiver, as well as the secondary impact of impaired receiver performance on functional safety and business liability.

Appropriate mitigation mechanisms should be built in, commensurate with the levels of risk determined. Mitigation technologies tend to take one of two forms: detection mechanisms and excision mechanisms. For developers, appropriate measures could include:

Use of a multi-constellation, multi-frequency (MCMF) receiver: This is a widely used measure to make a system more robust, as it is less likely that accidental/unintentional interference will affect different frequencies equally. In the case of intentional interference, an MCMF receiver makes it harder for the attacker to disrupt the target system to the extent where it stops tracking altogether, since many low-cost jammers only attack the GPS L1 C/A signal.

However, vulnerability testing is still essential, as many MCMF receivers use GPS L1 to acquire signals when initialising. If L1 jamming is present, they will not be able to acquire and track signals from any constellation. More sophisticated jammers are capable of jamming multiple frequencies simultaneously, including all known GNSS frequency slots.

Active notch filtering: Notch filters can be configured in the receiver firmware or by the user to filter out signals in narrow frequency bands that are susceptible to interference. It is especially important to test the impact of adaptive notch filtering, as the use of notch filters can result in a bias to horizontal position data that could be larger than the effect of the interferer.

Improvements to digital signal processing (DSP) and logic: The receiver logic can be tuned to detect GNSS jamming or other interference events and alert the user.

Firewalls: Firewall-type systems can be positioned between antenna and receiver to detect and mitigate against jamming and spoofing.

RF front end: Improvements can be made to the antenna by moving it to a location that is less vulnerable to interference, shielding it from line-of-sight signals from lower elevations, or using a nulling or beamforming antenna to cancel out the jamming signal.

It is vital to evaluate the performance and characteristics of detection and correction systems when connected to user equipment. Unless tested against relevant scenarios, it is difficult to assess their performance and to understand whether there are missed detections or false positives that can cause more harm than good.

5. What to test

A number of receiver capabilities can be affected by jamming, and these should be thoroughly tested in realistic and relevant jamming scenarios to determine their levels of vulnerability and thus the level of risk exposure.

Key performance characteristics to test are:

- **Cold Start Time to First Fix (TTFF):** The time taken by the receiver under test to acquire the signals and perform the initial position fix
- **Hot Start TTFF:** Same as cold start, but where the receiver already knows position (within 100 km of last fix), time, ephemeris and almanac
- **Horizontal Position Accuracy (HPA):** The accuracy of the simulated position, which can be evaluated with Circular Error Probable (CEP) or Root Mean Square Error (RMSE) measurements
- **Acquisition Sensitivity:** The minimum received power level at which a first fix can occur
- **Tracking Sensitivity:** The minimum power level at which the receiver can continue to maintain lock

For integrators, it is vital to perform these tests both before and after the receiver is connected to user equipment, as the placement is likely to affect the receiver's response to jamming.

6. Test methods, equipment and scenarios

Testing should be conducted in controlled, repeatable conditions to adequately assess the performance of the receiver and any mitigation measures implemented. This requires an appropriate test method to be selected, as well as access to the appropriate equipment and scenarios to conduct all relevant testing.

Choosing a test method

There are two fundamental methods of testing a receiver (Rx) and antenna (Ax) against in-band and adjacent-band interference:

Conductive testing of the Rx electronics only, by connecting the relevant simulation equipment to the device under test (DUT) via coaxial cable – ideally using calibrated cables to characterise the absolute power level incipient to the antenna.

Over-the-air (OTA) testing of the whole system (Rx and Ax), using broadcast simulated GNSS signals and interference – ideally inside an anechoic chamber, with appropriate RF absorbing materials surrounding the testing area to eliminate external interference from outside the chamber and unwanted multipath effects within the chamber. Outdoor testing on a designated test range is also possible but can be difficult and costly to organise and conduct.

Depending on the objectives of the test programme, an assessment may include both conductive and OTA tests, as well as testing with hardware in the loop (HIL). As OTA testing can be difficult to organise, requiring access to an anechoic chamber or outdoor test range, a good understanding of the available options and required test scenarios is needed from the outset. It must be noted that a careful cost/benefit analysis is essential to justify this approach.

Configuring test equipment – conductive testing

The equipment and configuration required for a basic conductive test may encompass:

- A GNSS RF constellation simulator (RFCS)
- An interference signal generator (ISG) if the RFCS does not have the capability to generate the embedded interference required by the test
- Calibrated cabling/adaptors, connecting the GNSS RFCS (and optional ISG) to the antenna DUT
- The Ax/Rx 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

In some configurations, the RFCS (and ISG) may be replaced by an RF Record & Playback System (RPS). The RPS can record real-world signals and interference for playback in the lab, rather than generating them in real time from first principles.

It should be noted that any RPS used should have a sufficiently high dynamic range to capture effectively both signals and interference (e.g. without clipping effects), and represent realistically to the DUT the jammer-to-signal (J/S) ratio which occurred at the time of the recording.

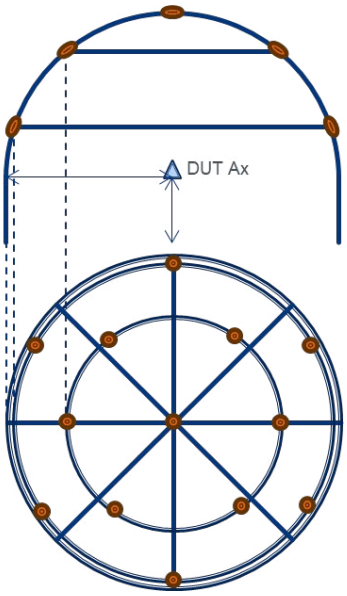


Figure 5: Configuration of 13 Tx antennas in an anechoic chamber

Configuring test equipment – OTA testing

Similarly, a basic OTA test configuration may encompass:

- One (or a group of synchronised) RFCS, depending on the number of transmit (Tx) antennas in the anechoic chamber. The diagram shows an anechoic chamber with 13 Tx antennas above the DUT Ax (Figure 5)
- Optional ISGs as for the conducted test
- Calibrated cabling/adaptors, connecting the RFCS(s) (and ISG) to the Tx antennas
- The Ax/Rx 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

The use of RPS in place of RFCS/ISG is prohibitive in the case of OTA testing in an anechoic chamber, as it is impossible to filter and split the pre-recorded signals into different Tx antennas corresponding to their line-of-sight direction at the time of the recording.

Although cumbersome, it is essential to calibrate path losses and characterise the gain/phase patterns of the Tx antennas and the DUT Ax in order to ensure test repeatability, for all applications requiring either relative or absolute incipient power measurements at the DUT.

An example of such a relative power test could be to compare the relative performance of two different controlled reception pattern antennas (CRPAs), e.g. with different numbers of elements or other hardware components, in order to select one for integration.

An example of an absolute power measurement is when we need to know the sensitivity of the DUT in absolute figures, and characterise the power ranges within which it can acquire GNSS signals, re-acquire after loss of lock or keep tracking them, in the presence – or not – of RF interference.

Selecting a simulator

When selecting a GNSS RFCS for vulnerabilities testing, the following features are key:

Signal accuracy: The signal generator must be more accurate by at least an order of magnitude than the DUT, otherwise it may mask the DUT performance. It is important to generate a test input signal eliminating artefacts, by ensuring maximum specs for the following key parameters:

- **Signal fidelity –** the RF output represents faithfully what has been configured in the simulated scenario.
- **Spectral purity –** eliminating spurious signals, harmonics and other products that may occur in the process of generating the GNSS RF signal output, as well as providing sufficient isolation between signals of different frequencies.
- **Low noise floor –** ensuring that the noise inherently generated by the RFCS (which is additive to the ubiquitous environmental thermal noise), is kept to a minimum (at least an order of magnitude lower than the DUT) so as to be conducive to a realistic representation of real-world signals – as if the test was taking place under live-sky conditions.
- **High J/S ratio –** the ratio of interference power over the nominal GNSS signal power, typically measured in dB. Usually -130 dBm is the reference power level which corresponds to the ICD GPS L1 frequency C/A code. J/S is a commonly used parameter to benchmark the performance of a DUT in the presence of interference. An RFCS must provide maximum J/S (ensuring low noise floor specifications are maintained).

Accurate signal and error models: The nominal GNSS signals must truthfully represent the live-sky signals (as defined in their respective ICDs) and ensuing errors, e.g. due to multipath, atmospheric or potential signal-in-space (SIS) failure modes. Both the implementation of ICDs and error models can be highly complex, requiring advanced expertise. It is therefore important to invest in testing equipment that is calibrated to an accredited standard, with performance verified by experts in industry-leading organisations.

Flexibility to add new test cases: The RFCS must be able to expand to accommodate future test requirements, e.g. by adding spoofing generation and monitoring capabilities; multipath interference simulation tools for the specific operational environment of the DUT; remote motion input for HIL testing configurations; or integration of generated GNSS RF signals with emulated inertial sensors for simulation testing of INS/GNSS equipment.

Automation capabilities: If vulnerabilities testing becomes a regular part of ongoing operations, it is essential for the RFCS to support internal or external automation control tools, e.g. via sharing a public application programming interface (API). Automation can help to maximise the return on the initial RFCS investment. This is something that Spirent has done successfully for many of its customers over the past 30+ years; however, it is out of the scope of this publication.

Further reading

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

Defining the test requirements

There are many reasons to conduct interference testing, including:

- Testing conformance to an industry standard, e.g. RTCA DO-229 for aviation receivers
- Internal quality control and qualification procedures
- Vendor selection for receivers and antennas

It is therefore important to understand the purpose(s) of the testing and to define the requirements in detail before investing in test instruments and other equipment. Any future changes in requirements should also be considered, to avoid incurring extra costs.

Gathering the requirements for interference testing may encompass knowledge of the following parameters within the test scenario(s):

RFI power profile, involving:

- Boundary conditions, e.g. min/max interference power levels
- How rapidly the power levels can 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 1 ms
- 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, and 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.

Types of interference waveforms: e.g. carrier wave, FM/AM, pulsed modulation and additive white Gaussian noise (AWGN).

DUT testing state: This is very important to ensure test repeatability, especially if the testing campaign is conducted in chronically divided phases or by different operators. 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 ones) from the non-volatile memory. These configuration parameters contain essential information, e.g. which atmospheric model the Rx may employ or enabling/disabling any multipath/interference mitigation algorithms.

Defining appropriate test scenarios

Receivers and systems should be tested using scenarios that are highly representative of real-world interference conditions. Their responses will indicate what kind of mitigation techniques may be necessary to allow them to function as expected in the real world. The broadest possible range of scenarios should be tested, to minimise the risk of unexpected effects in the field.

The following points should be kept in mind when designing realistic test scenarios:

Static and dynamic elements: Both the jamming source and the receiver may be stationary or moving, and should be modelled as such. For example, ABI from a stationary cell tower may affect a moving receiver in a unmanned aerial vehicle (UAV). Conversely, a cigarette lighter-type jammer in a moving vehicle may affect a stationary receiver in a GBAS ground station. Scenarios may also model more than one source of interference.

Interference type: Interference types can range from narrowband continuous wave jammers to CHIRP jammers and out of band interference from radio transmitters. For the latter, the EU's RED specifies a number of tests for GNSS receivers.

Receiver benchmarking: A packaged subset of scenarios can be used as the basis for a receiver benchmarking scheme. Users can compare test results from a wide range of devices and choose the most appropriate receiver for their intended application.

7. Example test – in-band jamming

This section describes an example in-band vulnerabilities test, encompassing scenario definition with pre-set pass/fail criteria, data collection, and analysis to determine if the pre-defined pass or fail conditions have been met. This test is set out in Radio Equipment Directive ETSI EN 303 413.

Overview of the test

The test involves an RFCS capable of generating RFI (either internally or externally connected and synchronised with an ISG), as described in Section 6, and a DUT connected to an RFCS with cables/adaptors of known losses for the test frequencies that will be employed in the test (described later in this section).

The DUT in this example test is assumed to be capable of being cold-restarted via a remote command (to facilitate automated testing – discussed later in this section). The DUT can also provide C/N_0 observed values with 1 dB-Hz resolution, at 1 Hz rate.

Purpose of the test

The purpose of the test is to determine whether, in the presence of specific interference profiles, the carrier-to-noise density ratioo (C/N_0) of a given simulated satellite drops below a threshold value of 1 dB, compared to nominal conditions.

The selected satellite transmits the GPS L1 C/A signal and is visible throughout the duration of the test (20 minutes). The power level on the RFCS output RF port is at the nominal ICD level of -130 dBm throughout the scenario duration, i.e. not modelled depending on its range with respect to the DUT simulated position.

The RFI types employed during the test are described in Table 1, noting that this is a GNSS L1 in-band RFI test.

Simulation time into run (hh:mm:ss)	RFI type	RFI power level (dBm)	RFI spectral properties	Comments
00:00:00	n/a	n/a	n/a	• Interference OFF • The DUT is cold-restarted and initialised to the desired testing state • DUT settles to nominal observed C/N_0 levels • C/N_0 nominal measurement
00:05:00	CW	-93	• Centre frequency: 1,575.42 MHz	Interference ON
00:07:00	CW pulse	-95	• Centre frequency: 1,575.42 MHz • Width: 500 µs • Repetition rate: 3 ms	
00:09:00	FM	-93	• Centre frequency: 1,575.42 MHz • Deviation: ±5 MHz • Rate: 5 kHz	
00:11:00	AM	-99	• Centre frequency: 1,575.42 MHz • Modulation depth: 50% • Rate: 5 kHz	
00:13:00	AWGN	-96	• Centre frequency: 1,575.42 MHz • Bandwidth (3 dB): 20 MHz	• Interference OFF • The DUT is left to settle to nominal C/N_0 levels again • C/N_0 integrity measurement
00:15:00	n/a	n/a	n/a	
00:20:00	n/a	n/a	n/a	End of test

Table 1: Example of interference test points

Glossary

CW	Continuous Wave
FM	Frequency Modulation
AM	Amplitude Modulation
AWGN	Additive White Gaussian Noise

Analysis of test results

It is assumed that the user has logged the timestamped C/N_0 values observed by the DUT for the selected satellite. The pass/fail test criterion is Eq. **(1)**:

$$\Delta C/N_0 \leq 1 \text{ dB}, \textbf{(1)}$$

Where:

$\Delta C/N_0$ – the degradation of the observed C/N_0 (dB-Hz) by the receiver in the presence of interference at a specific Testing Point – TP (C/N_0,iTP), with units in dB. $\Delta C/N_0$ is calculated using Eq. **(2)**:

$$\Delta C/N_0 = \langle C/N_0,n_1\rangle - \langle C/N_0,\text{iTP}\rangle, \textbf{(2)}$$

Where:

$\langle C/N_0,n_1\rangle$ – the average (over a minute, i.e. 60 measurements) of the nominal C/N_0 level in the absence of any interference, with the receiver settled before the interference testing starts (units in dB-Hz).

$\langle C/N_0,\text{iTP}\rangle$ – the average (over a minute, i.e. 60 measurements) of the nominal C/N_0 level in the presence of interference at the respective TP (units in dB-Hz).

The TP measurements schedule is shown in Table 2.

Simulation TIR (hh:mm:ss) Start averaging	Simulation TIR (hh:mm:ss) End averaging	Calculated parameter
00:04:00	00:05:00	$\langle C/N_0,n_1\rangle$
00:06:00	00:07:00	$\langle C/N_0,i_1\rangle$
00:08:00	00:09:00	$\langle C/N_0,i_2\rangle$
00:10:00	00:11:00	$\langle C/N_0,i_3\rangle$
00:12:00	00:13:00	$\langle C/N_0,i_4\rangle$
00:14:00	00:15:00	$\langle C/N_0,i_5\rangle$
00:19:00	00:20:00	$\langle C/N_0,n_2\rangle$

Table 2: Testing point measurements schedule

It is worth noting that an additional integrity check measurement is recommended after completing the interference TP measurements. This is to indicate that the DUT has not changed the nominal C/N_0 baseline level during testing, e.g. due to an error in adjusting the automatic gain control (AGC) during the test. This is given by Eq. **(3)**:

$$|\langle C/N_0,n_1\rangle - \langle C/N_0,n_2\rangle| \leq 1 \text{ LSB (dB)}, \textbf{(3)}$$

Where:

$\langle C/N_0,n_2\rangle$ – the average (over a minute, i.e. 60 measurements) of the nominal C/N_0 level in the absence of any interference, after the interference testing is completed and the receiver re-settled (units in dB-Hz).

LSB – the least significant bit (scale factor) resolution of the DUT in providing C/N_0 measurements (in dB-Hz), noting that the difference between the nominal level C/N_0 averages is in dB units. This is because DUTs may report C/N_0 at different resolutions, e.g. in 0.25 dB-Hz or 1 dB-Hz.

Another way to determine if the integrity check condition is met, is to monitor the AGC level of the DUT before and after the interference testing, (during the same measurement periods as $\langle C/N_0,n_1\rangle$ and $\langle C/N_0,n_2\rangle$) and ensure that, again, the absolute difference is within 1 LSB (dB). Note, though, that some DUTs do not readily report AGC level measurements.

8. Conclusion

In this paper we have outlined the threat from RF signal jamming to safety-critical and liability-critical systems that rely on GNSS for their operation, and provided guidance on how to develop and apply the appropriate tests to assess the vulnerability of a GNSS receiver.

It is important to note that the threat from jamming is continuously evolving. Jamming equipment – including high-powered equipment marketed for drone defence – is becoming easier to buy online, and the code to build a jammer from a software-defined radio (SDR) is easy to find.

As more systems and devices rely on GNSS, jamming becomes a more attractive tool for criminals and other malicious actors to disable vehicles and operations to their own gain. It is also increasingly used by nation states to disrupt adversaries or to test their own military equipment, presenting risks to civilian users within the jamming area.

At the same time, there is a growing threat from ABI, as the radio spectrum is sliced ever more finely, and spectrum nearer to the GNSS bands is allocated to terrestrial communications providers.

GNSS receiver developers and integrators should continually monitor how these threats are evolving, carry out regular quantitative risk assessments against prevalent threats and, as far as possible, deploy appropriate mitigation measures to protect the system and its end users.

9. How Spirent can help

Spirent can help with every aspect of PNT vulnerabilities testing, drawing on our 30+ years' experience of developing and implementing GNSS and inertial testing solutions.

We continuously evolve our hardware and software to address the PNT vulnerabilities testing needs of leading organisations in the military, government, space and industrial sectors. Our GNSS signals are generated implementing the latest ICDs, using dedicated hardware and software that is developed in-house for better support and maintainability.

Spirent mathematical models have been proven and optimised for 30+ years, working 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 modelling of the signal characteristics and errors as well as Rx behaviour.

Spirent 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. Our Professional Services team, meanwhile, offers a broad range of services to help you design and conduct appropriate GNSS vulnerabilities tests and analyse the results.

To discuss any aspect of your PNT vulnerabilities testing, please get in touch.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

Contributors

Guy Buesnel, CPhys, MInstP, FRIN, RNTF
PNT Security Technologist, Spirent

Guy has more than 20 years' working 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 is Spirent's specialist PNT Security Technologist covering the areas of PNT threats and mitigation. Guy holds a BSc Honours 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
Product Manager for High-end PNT Test Solutions, Spirent

Kimon is responsible for providing high-end GNSS test solutions to military, government, GNSS and space organisations. 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).

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev A | 05/20