Fundamentals of GPS Threats

How the growing threats to satellite navigation signals can impact your critical systems, and what to do about it

Executive summary

Satellite navigation signals from space are precariously weak, and can easily be blocked, damaged or compromised by a growing array of threats - including solar activity, man-made interference, malicious faking of GPS signals, and the manipulation of position and timing information.

As we come to rely more and more on GNSS signals and data across a wide range of industries, understanding and mitigating against these threats will become a critical risk management activity for manufacturers, systems and applications providers, and end-users.

This white paper is for people responsible for understanding the risk factors affecting GNSS-reliant systems, and for ensuring that appropriate steps are taken to mitigate them. In it you will find:

- An introduction to the different threats to GNSS, and how these are evolving
- Some guidance on evaluating the susceptibility of your systems to GNSS threats
- An overview of some of the most effective techniques available to mitigate the risk of GNSS outages, errors and/or cyber-attacks on your critical systems
- An introduction to Spirent's GNSS threat assessment and mitigation services

GPS or GNSS?

The Global Positioning System (GPS) was once the only global navigation satellite system in operation. Today, there are numerous satellite systems dedicated to providing time and location signals for both military and civilian use. They include Russia's GLONASS, China's BeiDou and Europe's Galileo, as well as a number of regional systems. Collectively, these systems are known as Global Navigation Satellite Systems (GNSS). We will use this term in this white paper, except where we are referring to a specific system.

Fundamentals of GPS Threats

Introduction: our growing dependence on GNSS

Almost unnoticed, global navigation satellite systems (GNSS) have begun to exert enormous influence on the way we live and the world we live in.

A vast array of devices and systems rely on data from GPS and other satellite systems to provide services we have come to rely on.

For example:

In the world's **container ports**, automated cranes are often guided by GNSS to pick up the right container and move it to the right place.

In the **maritime industry**, ships use GNSS for navigation and as the basis for the Automatic Identification System (AIS), which is used to track shipping movements and location worldwide.

In **3G mobile networks**, the precise time derived from GNSS signals is used to achieve successful call signal hand off over IP and to transport real time data, while in **4G networks** it's also used to ensure uninterrupted streaming video.

Farmers rely on automated, GNSS-based systems to plant, water and fertilise their crops.

The **commercial aviation** sector uses GNSS to assist with landing at remote airfields, while the next generation of Air Traffic Management Systems will require precise time from GNSS to implement 4D trajectory management.

Government agencies variously rely on GNSS for tasks like monitoring fishing activity, directing emergency services and tracking stolen vehicles

In Europe, Russia and the United States, some **models of cars and trucks increasingly** use GNSS to alert emergency services automatically in the event of an accident.

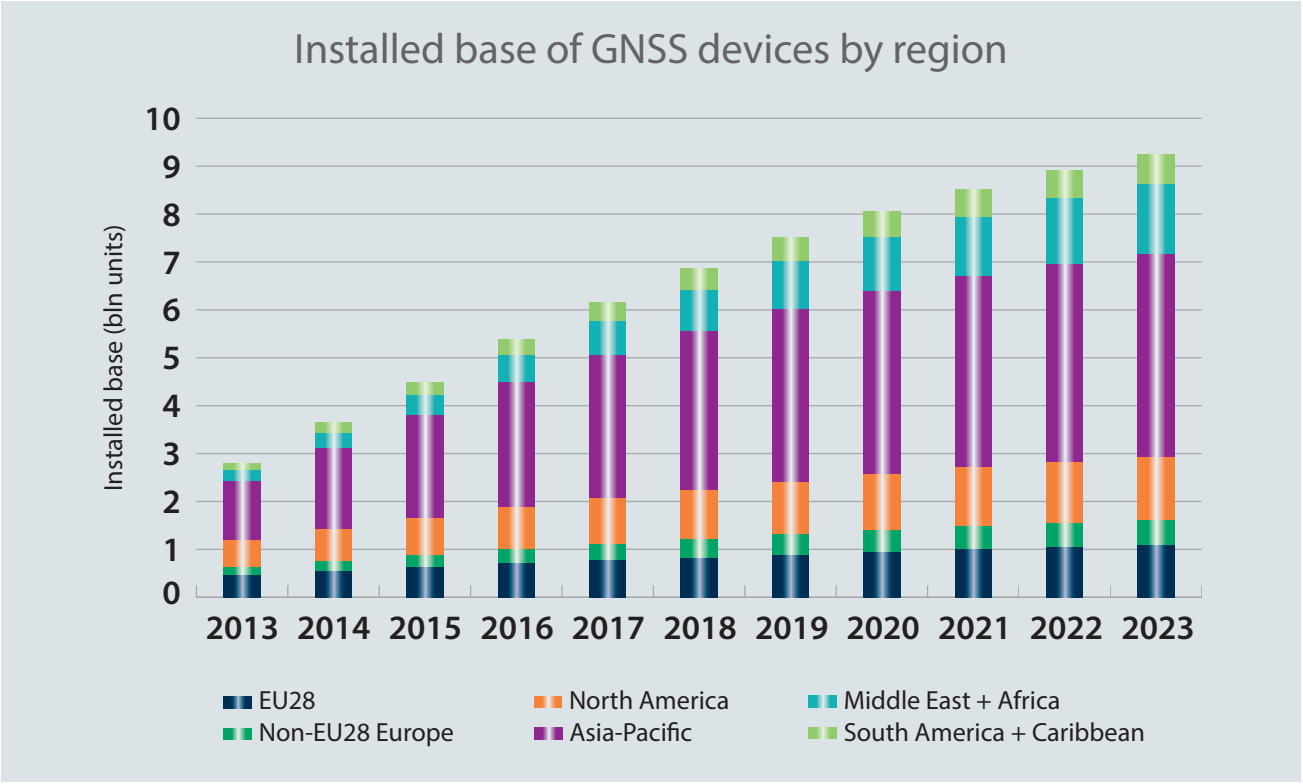
Banks and financial institutions depend on GNSS for precision timestamping of transactions.

In the **logistics and transportation industries**, GNSS is used in fleet management/telematics applications and is an important factor in Just in Time management of supply chains.

In the **building and construction** industries, GNSS is used for surveying and for guiding autonomous or highly automated construction machinery.

The list goes on and on, because GNSS is everywhere. The European GNSS Agency (GSA) estimates that 3.6 billion GNSS devices were in use worldwide in 2014. That figure is forecast to double to over 7 billion by 2019, as GNSS functionality finds its way into ever more vehicles, mobile devices, networks and control systems[1].

1 European Global Navigation Satellite Systems Agency, GNSS Market Report Issue 4, March 2015



Source: GSA GNSS Market Report 2015 Issue 4_0, March 2015

Fundamentals of GPS Threats

GNSS signals are highly vulnerable to a growing array of threats

For the people who use these systems every day, GNSS is simply there, guiding them and their machines to do the right thing in the right place at the right time.

But for the people whose job it is to ensure these systems work, it's not so straightforward. Satellite signals from space are precariously weak, and can easily be blocked, damaged or compromised by a growing array of threats. Those threats include solar activity, man-made interference, malicious faking of GPS signals, and the manipulation of position and timing information.

As we come to rely more and more on GNSS signals and data, understanding and mitigating against these vulnerabilities will become a critical risk management activity for manufacturers, systems and applications providers, and end-users.

In this white paper: Threats affecting GNSS-reliant systems, and how to address them

This white paper is for people responsible for understanding the risk factors affecting GNSS-reliant systems, and for ensuring that appropriate steps are taken to mitigate them. In it you will find:

- An introduction to the different threats to GNSS, and how these are evolving
- Some guidance on evaluating the susceptibility of your systems to GNSS threats
- An overview of some of the most effective techniques available to mitigate the risk of GNSS outages, errors and/or cyber-attacks on your critical systems
- An introduction to Spirent's GNSS threat assessment and mitigation services

Spirent: 30 years of GNSS threat mitigation expertise

Spirent has been working with commercial, government and military organisations for 30 years to help them understand the threats to GPS and other satellite navigation systems, and to address those threats through the use of professional testing and measurement.

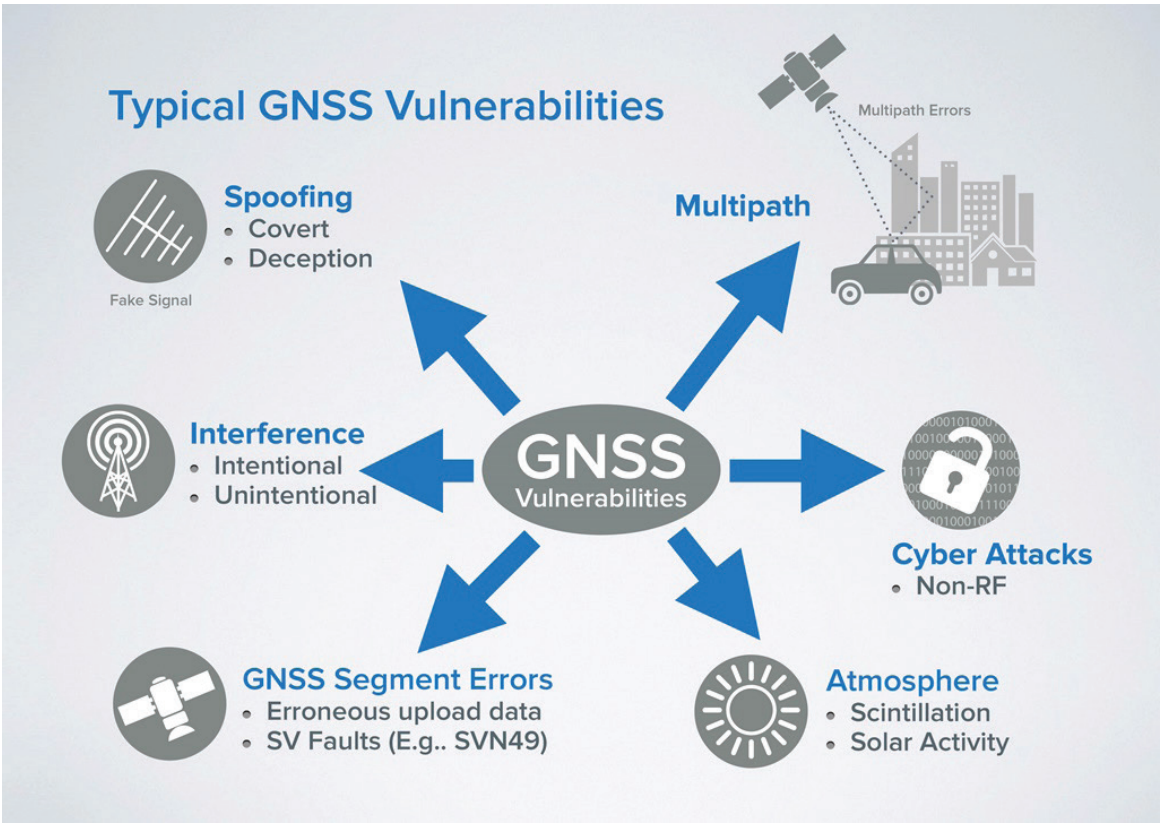
If you have a question about the resilience of your GNSS-dependent products or systems, please do get in touch at www.spirent.com/ContactSpirent.

The threats to GNSS-dependent systems

The GNSS signals used by commercial devices are precariously weak, with a power no greater than that of a 40-watt light bulb. They are also freely available, and – unlike signals reserved for military use – are usually unprotected by encryption.

These two factors mean that civilian satellite signals are relatively easy to block, disrupt, manipulate and tamper with, whether intentionally or unintentionally.

There are many types of threat that can interfere with a GNSS receiver's ability to receive and process GNSS signals, giving rise to inaccurate readings, or no reading at all.



Fundamentals of GPS Threats

Understanding the different types of threat and how likely they are to occur is key to conducting an accurate risk assessment. Broadly, the threat types break down as follows:

Threat Source	Threat Type	Description	Prevalence	Impact on The User
Solar Storms	Natural	Electromagnetic interference from solar flares and other solar activity "drowns out" the satellite signals in space.	Common across wide geographic areas during periods of intense solar activity.	Loss of signal, or range errors affecting the accuracy of the location or timing information.
Scintillation	Natural	The satellite signal is refracted or diffracted in space by irregular ionospheric activity.	Effects of scintillation are most pronounced in tropical latitudes and at high latitudes.	Impact on the receiver can include inaccurate location information.
Obscuration	Natural	An insufficient number of satellites are in view to be able to provide an accurate position – due to structures obscuring the antenna's view of the sky.	Occurs mainly indoors, underground, in built-up areas, in wooded areas, mountain gulleys or deep cuttings.	Loss of signal, or range errors affecting the accuracy of the location information.
Multipath	Natural	Signals from one or more satellites reflect off nearby structures, fragmenting their path to the receiver.	Commonly occurs in "urban canyons" where streets are surrounded by tall glass buildings.	Range errors affecting the accuracy of the location information.
Poor Installation	Man-made	The device's antenna is installed in a position where it can't obtain a clear view of the sky or clear signals from satellites, or is improperly matched to the receiver, which can result in RF leakage that looks like an interference source.	Can be due to poor product design, or to fixed antennas being obscured by new, taller buildings being built nearby.	Sub-optimal satellite geometries can result in a receiver unable to resolve its position, inaccuracies affecting location and timing information. Leakage from a poor installation could cause a complete loss of signal.
Jamming	Man-made	Locally-generated RF interference is used to "drown out" satellite signals.	Jamming is predominantly (but not solely) caused by "personal privacy devices" fitted to company vehicles to prevent tracking of movement. Illegal use of PPDs is increasing significantly.	Loss of signal (if the jammer is blocking out all satellite signals) or range errors affecting the accuracy of the location or timing information (if the receiver is at the edge of the jammer's range).
Spoofing	Man-made	Fake satellite signals are broadcast to the device to fool it into believing it is somewhere else, or at a different point in time.	Spoofing was once extremely hard to do, but recent demonstrations have shown it is now easy to build a GNSS spoofer from open-source software and low-cost components.	False location and time readings, with potentially severe impacts on automated and autonomous devices and devices that rely on precise GPS timing.
Hacking	Man-made	Manipulation of the software layer of the device to alter its interpretation of satellite signal data.	Widely carried out today in personal devices such as mobile phones and tablets. The Operating System is jailbroken and the user installs an application that allows the GPS receiver information to be substituted by manually edited information in a separate application. There is evidence that this is also prevalent with AIS data manipulation in the maritime segment.	False location and time readings, with potentially severe impacts on automated and autonomous devices and devices that rely on precise GPS timing.
RF Interference	Man-made	Noise from nearby RF transmitters (inside or outside the device) obscures the satellite signals.	Prevalent in areas with heightened RF noise (e.g. near cell towers) or inside devices where the GNSS receiver is not appropriately shielded from other components.	Loss of signal (if the transmitter is blocking out all satellite signals) or range errors affecting the accuracy of the location reading (if the receiver is at the edge of the transmitter's range).
User Error	Man-made	Users over-rely on the GNSS data they are presented with, ignoring evidence from other systems or what they can see.	Prevalent in any scenario where the user becomes too reliant on information from their navigation system.	Can lead to poor decision-making in a range of scenarios (e.g. lorries driving down too-narrow lanes, ships steering too close to hazardous objects).

Understanding the risks to your critical systems

Given the increasing number and prevalence of the threats outlined in the previous section, manufacturers of GNSS-reliant systems and related applications need to be aware of the potential impact on their products, customers and end-users.

This highlights the need to conduct a thorough assessment to map the following factors:

- The importance of accurate GNSS location and/or timing information to the overall functioning of the system
- The extent to which users rely on precise, accurate and continuous GNSS signal data
- The likelihood of the system being affected by one or more identified GNSS threats
- An understanding of the most likely behaviour of the system when stressed by relevant threats and the impact of this behaviour on the end-user applications
- The risk to the business, its customers, its end-users and other parties if one or more threats impair the proper functioning of the system

The risk profile is application-dependent and will differ significantly from organisation to organisation, and from device to device. For example:

If an **automated crane** at a container port can't receive a GNSS signal for a prolonged period of time, the port and its customers may incur financial losses.

If a GPS-disciplined clock at an **electricity substation** has its time signal "spoofed", it could disrupt the distribution of energy across the grid.

If a running enthusiast can't get accurate distance and time calculations from their **fitness tracker**, they may defect to another brand, and/or complain about the product on social media.

The key is to understand the specific risks present today, and to gain insight into how the threats are evolving and developing, with a view to anticipating and mitigating future threats.

For example, malicious jamming and spoofing are both evolving fast, as hackers increasingly gain access to low-cost equipment that enables them to interfere with GNSS signals for personal gain, mischief-making, or potentially more sinister purposes.

Fundamentals of GPS Threats

An overview of GNSS threat mitigation techniques

Once you have mapped the risks to your systems, products and customers, you will want to ensure that appropriate risk mitigation measures are in place to counter them.

Depending on the nature of the device, the system and the risk profile, there are many threat mitigation options to choose from. These include, but aren't limited to:

Multi-frequency receivers: It is much harder to jam or spoof a GNSS receiver that has the capability of receiving signals on multiple frequencies.

Multi-constellation GNSS receivers: Receivers that can process signals from multiple satellite constellations (e.g. GPS, GLONASS, BeiDou) are more resistant to all kinds of interference, from obscuration to jamming and spoofing.

Improved antenna: There are many advanced antenna designs available to counteract the effects of jamming and spoofing – with a range of form factors and prices. The antenna is a vital component of a satellite navigation system and investing a relatively small amount of money here can make a large difference in performance.

Advanced military users rely on multi-element antennas that use beamforming techniques to modify the radiation pattern of the antenna to maximise the strength of GNSS signals, while reducing the effect of interference, but this type of antenna is not available for civilian use today.

Alternative or backup sources of position, navigation and timing data: There are many options to explore here, including dead reckoning sensors, WiFi/cellular-based positioning, assisted GPS, and industry-specific, ground-based backup/augmentation systems (e.g. eLoran for UK maritime use, WAAS or EGNOS for aviation).

Comparing received signals with a ground-based reference source to identify any anomalies. Reference data technologies include differential GPS and Real-Time Kinematic (RTK).

Using Receiver Autonomous Integrity Monitoring (RAIM) techniques in the receiver to identify and reject spurious signals or interference.

Using innovative Digital Signal Processing technology in the receiver to intelligently monitor signal parameters and excise interfering signals.

Advanced multipath mitigation techniques that can make it harder for a spoofer to successfully take control of the receiver using a fake signal.

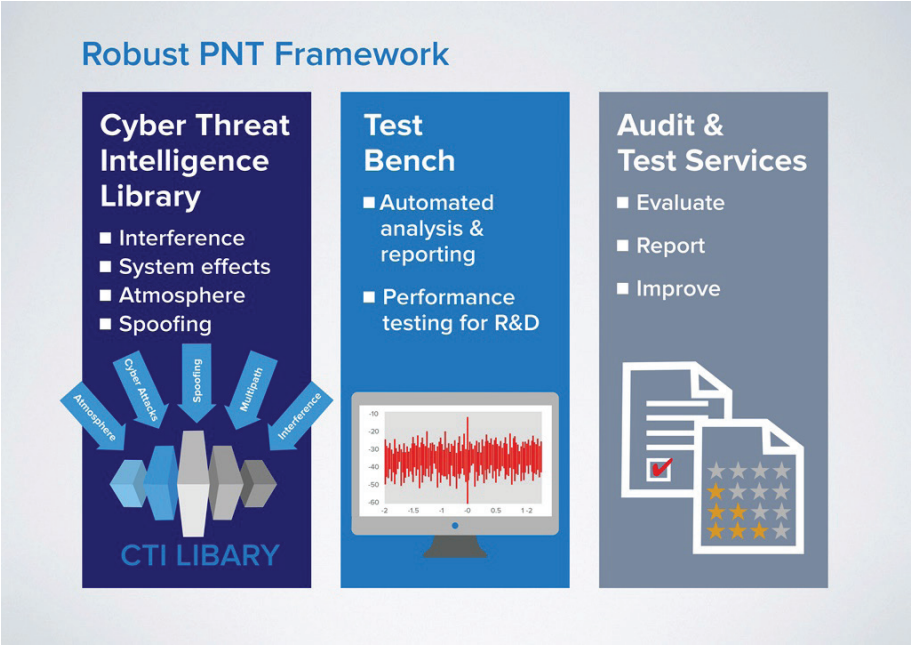
Use of encrypted GNSS signals (if authorised): Encrypted signals are available for military use in the US with the GPS Precise Positioning Service (PPS) and for critical infrastructure in Europe using the Galileo Public Regulated Service (PRS).

Whichever mitigation techniques you adopt, it's essential to keep pace with developments in Position and Timing System threats, to verify that your chosen techniques can counteract new threats as they emerge, or update them accordingly.

Help with GNSS threat identification, risk assessment and risk mitigation

For many organisations, understanding and countering threats to GNSS-dependent systems will be a new and unfamiliar discipline. The remit may fall to CIOs and CISOs who already have a heavy burden keeping pace with rapidly-evolving information security threats. Or it may fall to a risk management department unfamiliar with the intricacies of GNSS signal processing.

For these reasons, Spirent has developed a set of products and services to help organisations assess and combat the threats to their GNSS-dependent systems. Drawing on our 30 years' experience working with governments, military organisations, space agencies and commercial organisations to identify and counter threats, we offer the following services:



Systems audit: A thorough, professional evaluation of the susceptibility and resilience of your GNSS-reliant receivers, products and systems to the threat types outlined in this white paper – with a full report on our findings and recommendations for action.

GNSS threats database: Access to a continually-updated database of existing and emerging threats to GNSS-dependent systems. The database is currently the only one of its kind in existence. The threats database consists of downloadable test cases that can be used to test the response of your receivers, devices and systems to real, observed threats happening in the world today.

GNSS threats testbed: Spirent offers a wide range of market-leading test equipment to enable you to simulate threats and understand your systems' responses to them. Our products include GNSS signal simulators, interference and spoofing simulators, interference detectors, RF record & playback devices and a wide range of test cases and test scripts. For more, visit www.spirent.com/positioning.

GNSS threat test training: We can train your risk management, QA and test teams to use the database and test equipment outlined above.

Outsourced GNSS threat testing service: We can supply any combination of the above services as a fully-outsourced GNSS threat testing capability, tailored to your requirements.

If you have any questions about these services, or would like further information, please get in touch.

Fundamentals of GPS Threats

About Spirent

Spirent provides software solutions to high-tech equipment manufacturers and service providers that simplify and accelerate device and system testing. Developers and testers create and share automated tests that control and analyze results from multiple devices, traffic generators, and applications while automatically documenting each test with pass-fail criteria. With Spirent solutions, companies can move along the path toward automation while accelerating QA cycles, reducing time to market, and increasing the quality of released products. Industries such as communications, aerospace and defense, consumer electronics, automotive, industrial, and medical devices have benefited from Spirent products.

Conclusion

As the world become more dependent on navigation satellite signals to guide systems and machinery, any threat to those signals carries a correspondingly greater risk.

At the same time, our increasing reliance on GNSS signals makes them a more tempting target for hackers, who are perennially ingenious in inventing new ways to disrupt and exploit them.

For any manufacturer producing GNSS-reliant devices or systems, this means there's an urgent need to keep pace with emerging threats and ensure appropriate risk mitigation measures are taken.

Spirent can advise on any aspect of GNSS threat identification, testing and mitigation. Contact us today to discuss your needs or concerns, and to learn more about how we can help.

www.spirent.com/Solutions/Robust-PNT

spirent.com

AMERICAS 1-800-SPIRENT
+1-818-676-2683 | sales@spirent.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979 | emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539 | salesasia@spirent.com

 MCD00226AAA | Issue 1-00