WHITE PAPER

Fundamentals of GPS Threats

How the Growing Threats to Satellite Navigation Signals Can Impact Your Critical Systems, and What to Do about It

KEYSIGHT

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
- 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 cyberattacks on your critical systems
- An introduction to Keysight'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.

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 **automotive sector**, GNSS enables connected vehicle services such as eCall, automatically providing vehicle location information to emergency responders after a collision. GNSS is also fundamental to navigation, fleet tracking, advanced driver assistance systems (ADAS), and emerging autonomous vehicle technologies.

In the **maritime sector**, GNSS is fundamental to vessel navigation, positioning, route optimisation, and port operations. It also provides the positioning and timing data that underpin the Automatic Identification System (AIS), enabling global vessel tracking, collision avoidance, maritime safety, and efficient management of international shipping traffic.

5G networks depend on highly precise GNSS-based timing to support massive MIMO, beamforming, ultra-low-latency communications, and synchronized operation across dense, distributed radio networks.

In modern **precision agriculture**, GNSS positioning and timing are used to guide autonomous and semi-autonomous farming equipment with centimeter-level accuracy, enabling precision planting, fertiliser and pesticide application, automated steering, field mapping, and yield monitoring. By improving operational efficiency and reducing overlap, GNSS helps farmers optimize resource use, lower costs, and increase crop productivity while supporting sustainable farming practices

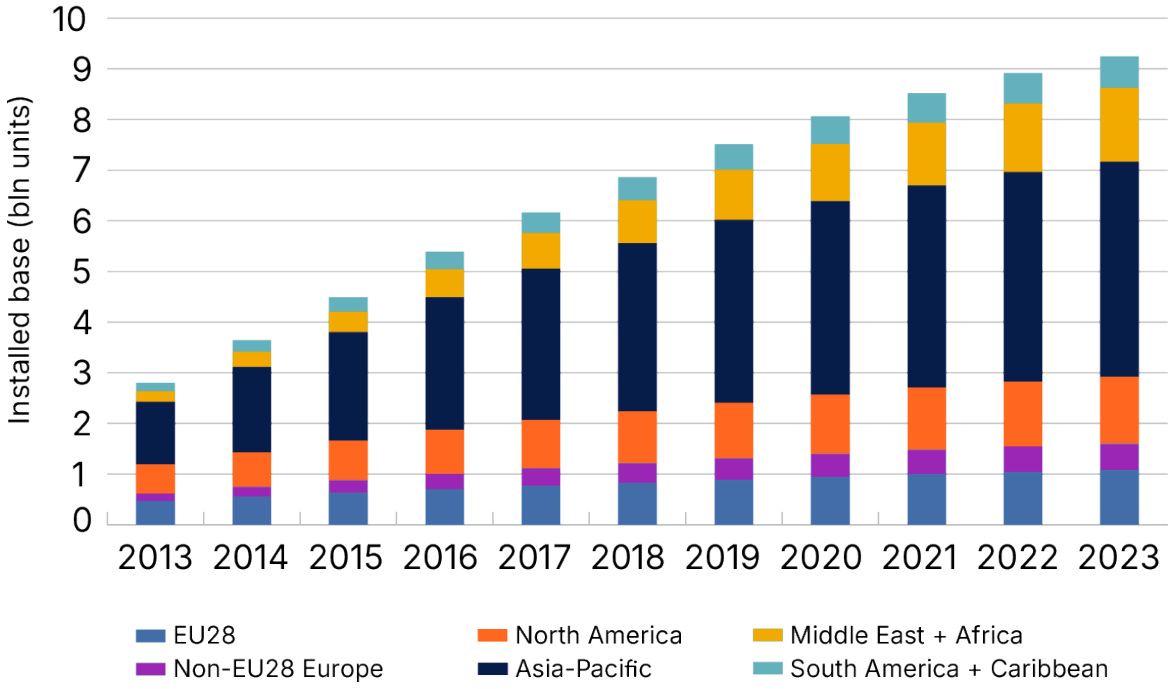
The **commercial aviation** sector relies extensively on GNSS for navigation, performance-based navigation (PBN), precision approach and landing procedures, and aircraft surveillance. Next-generation Air Traffic Management (ATM) systems also depend on precise GNSS-derived timing and positioning to enable 4D trajectory management, improved airspace efficiency, and safer coordination of increasingly dense air traffic.

Government agencies rely on GNSS to support a wide range of public safety, security, and regulatory functions, including emergency response coordination, disaster management, law enforcement operations, border and maritime surveillance, critical infrastructure monitoring, and the tracking of vehicles and assets.

Wearable devices including smartwatches and fitness trackers use GNSS to provide accurate location, navigation, fitness tracking, and safety services, supporting applications such as exercise monitoring, route guidance, emergency assistance, and location sharing in connected consumer ecosystems.

The list goes on and on, because GNSS is everywhere.

Installed Base of GNSS Devices by Region



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 is 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 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
- 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 cyberattacks on your critical systems
- An introduction to Keysight's GNSS threat assessment and mitigation services

Keysight's GNSS Threat Mitigation Expertise

Keysight works with commercial, government, and military organizations 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.

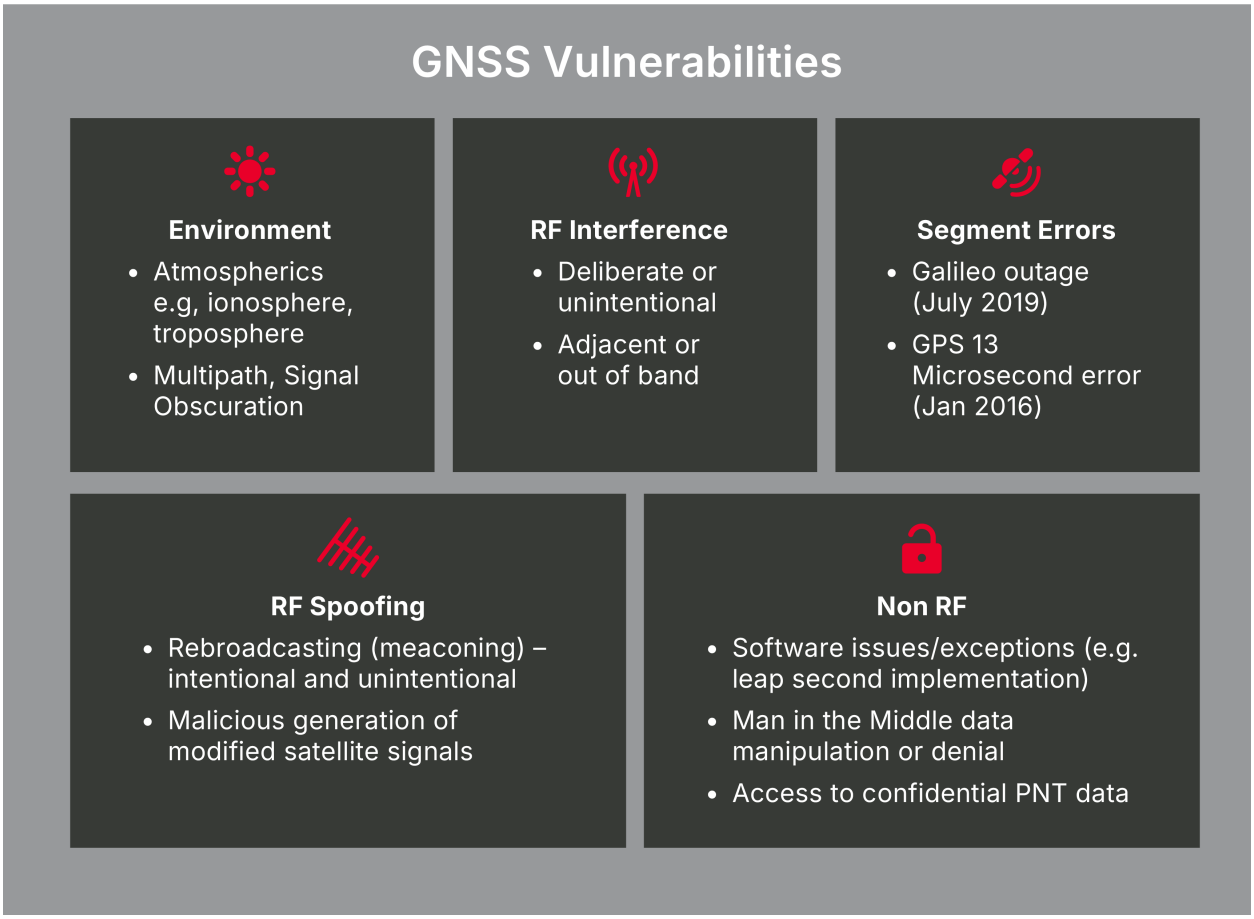
If you have a question about the resilience of your GNSS-dependent products or systems, please get in touch.

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.



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	False location and time readings, with potentially severe impacts on automated and autonomous devices and

Threat source	Threat type	Description	Prevalence	Impact on the user
			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	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 behavior of the system when stressed by relevant threats and the impact of this behavior 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 organization to organization, and from device to device. For example:

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 cannot get accurate distance and time calculations from their **fitness tracker**, they may defect to another brand 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.

Find out how to test the risks to safety-critical and liability-critical systems in this white paper.

Find out what GNSS signal spoofing is, how a spoofing attack works, and what you can do to protect your product or system in this white paper.

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 are not 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: Many advanced antenna designs are 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 maximize 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, Wi-Fi / 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).

Received signals with a ground-based reference source: Compare these to identify any anomalies. Reference data technologies include differential GPS and real-time kinematic (RTK).

Receiver autonomous integrity monitoring (RAIM) techniques: Use these in the receiver to identify and reject spurious signals or interference.

Innovative digital signal processing technology in the receiver: Use these to intelligently monitor signal parameters and excise interfering signals.

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

Encrypted GNSS signals (if authorized): 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 is 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 to update them accordingly.

Help with GNSS Threat Identification, Risk Assessment, and Risk Mitigation

For many organizations, 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.

Simulation Solutions and PNT Test Services

Keysight's powerful and flexible hardware and software has been at the forefront of GNSS interference testing, delivering the performance needed to mitigate the most advanced GNSS jamming and spoofing events.

From onboard interference in the PNT GSS7000 and PNT X GNSS simulators to specialized services offered by the expert global services team — and including the capability to build composite systems with no impact on performance — testing for GNSS receivers and anti-jamming systems has never been so comprehensive.

Keysight's services team brings decades of experience to your operations, helping you to accelerate and de-risk product development and verification. Whether you need recordings or scenarios delivered to order, resident engineering support, consultancy, team training, analysis, benchmarking, or any other support inside and outside the lab, Keysight services is the ideal partner. To find out more about the range of capabilities and how they could help you to deliver world-leading products, see our website.

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

Conclusion

As the world becomes 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 is an urgent need to keep pace with emerging threats and ensure appropriate risk mitigation measures are taken.

Keysight 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.

https://www.keysight.com/us/en/products/positioning-navigation-and-timing-emulators.html

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.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2026, Published in USA, June 1, 2026, 3126-1204.EN