# GNSS Signal Integrity Monitoring

With a world that is more and more reliant on the Global Navigational Satellite Systems (GNSS), it is critical that the integrity of the signals, especially position and time accuracy, remain uncompromised. There are over 4 billion GNSS receivers in various applications around the world that are highly susceptible to having the GNSS signal quality being compromised. Applications that could have serious consequences are:

**Financial Services.** Demand very stringent requirements of time synchronization. GNSS spoofing attacks can cause a timestamp shift that influences the security and integrity of banking transactions.

**Power Grid System Phasor Measurement** is critical in synchronization to ensure flawless Network Monitoring and Automatic Protection. Time synchronization distortion of a Phasor Measurement can lead to cascading faults and large-scale power blackouts.

**Autonomous Machines.** Coordinate or speed manipulations can lead to undesired damages, and even human loses.

**5G.** 5G time synchronization accuracy is critical and mandatory. Maintaining precision from GNSS in difficult jamming conditions, or an inferior GNSS antenna placement, and even under spoofing, is mandatory.

**DVB-T/T2.** Digital broadcasting in Single Frequency Networks (SFN) mode like DVB-T/T2, T-DMB, DAB, or DRM requires precise and reliable synchronization. In case of low accuracy of the PPS phase, the service falls.

**Data Centres** require sub-millisecond precision time stamping for transactions and distributed data processing, log file accuracy, auditing, and monitoring. GNSS spoofing may cause SSL certificates to fail.

**Marine.** GNSS is currently applied to diverse marine applications such as navigation, seafloor mapping, underwater exploration, dredging, offshore drilling, and pipeline routing. At the same time, thousands of GNSS spoofing incidents at sea are recorded all over the world.

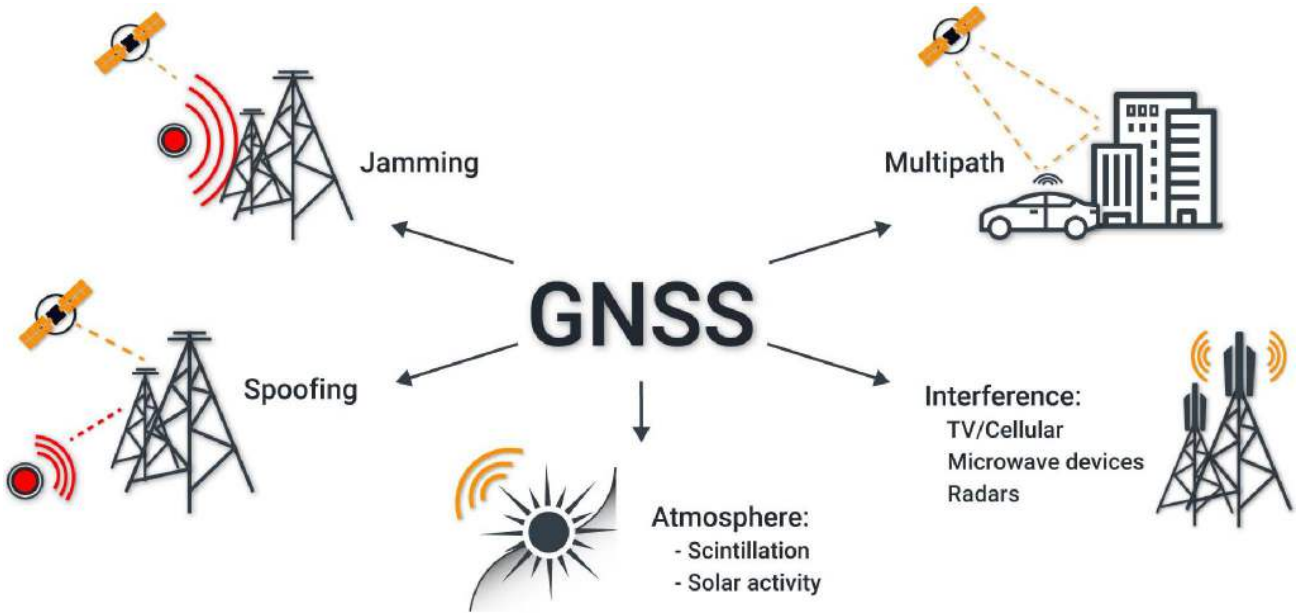
**Railway.** GNSS is utilized to track trains on low-density line networks. Automatic Train Control Systems use GNSS to determine speed and position. The GNSS should work in any conditions: under the GNSS spoofing/jammingattack, high RF interference level.

**Airport.** According to ICAO Annex 10 requirements, airports need to implement GNSS monitoring and recording systems to ensure a quick response to the degradation of accuracy and to conduct incident investigations.

**Network RTK**is a critical part of many applications with precise, real-time positioning requirements. RTK base station must have reliable GNSS spoofing protection. Incorrect data can be detrimental to thousands of users.

The quality of GNSS signals is affected by signal reflections from various objects, RF interferences from communication systems, terrestrial TV, etc. In densely populated cities many systems require accurate synchronization, but often it is not possible to mount a GNSS antenna high above buildings, trees, billboards, construction cranes. This adversely affects the accuracy of determining time, which is critical for some applications like 5G. If the antenna is unfittingly positioned, the accuracy of the PPS signal can drop to 500 ns.

Factors that impair GNSS signals quality:




Since GNSS is a critical component in many systems today, it is essential to provide timely capture and analysis of signal parameters for fast identification and response. For example, if your network of GNSS RTK reference sites fails every so often, or you have many random errors during autonomous vehicle tests, a tool should be used to monitor the status of the GNSS data.

**GNSS Spoofing**

More and more facts of GNSS spoofing are detected around the world. Such a widespread use of spoofers is explained by the fact that GNSS spoofing is used for:

- VIP and mass events protection (Counter-UAV)
- Deception of vehicle tracking systems
- Military exercise

In many countries, security guards have begun to use GNSS spoofing to protect against Unmanned Aerial Vehicle. Unscrupulous drivers of cars and trucks use spoofing and jamming to trick vehicle tracking systems. If GNSS spoofing is used in a densely populated city, then banks, cellular operators, TV broadcasting are all at risk with their GNSS time receivers and servers. An unintended spoofing attack leads to time and coordinates shift and cause unpredictable heavy damages to businesses.

7 years ago, GPS spoofing used to require considerable technical skills and money. Now it can be done with low-cost commercial hardware (SDRs like HackRF) and software downloaded from the GitHub (e.g., osqzss/gps-sdr-sim). So now, any student can organize a spoofing attack on a bank's processing center in 15 minutes.

In early 2019, a non-profit organization C4ADS released a report on the use of GPS spoofing where they found that there were 9883 events registered over a two-year period.

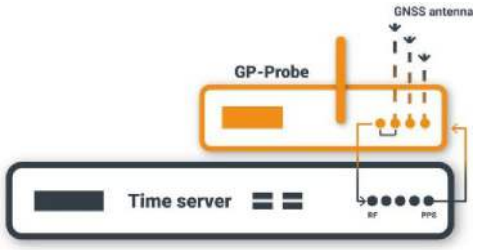
Introducing GPSPATRON, a GNSS quality monitoring system covering the GPS, GLONASS, BEIDOU and Galileo constellations. The system, based upon a neural network, provides monitoring and threat detection of GNSS signal parameters and PPS phase accuracy.

The system consists of affordable three-channel GNSS probes (GP-Probe) and a powerful cloud service (GP-Cloud). GP-Probe conducts GNSS signal measurements using 3 channels with angle-of-arrival estimation and transmits raw data to the GP-Cloud for real-time processing. GP-Cloud uses advanced anomaly detection algorithms for determining any nonlinearities present in the radio frequency signals.


With GPSPATRON technologies you are able to control all your GNSS-dependent entities. Just install GP-Probe on your time/coordinates critical infrastructure and fully control it in one web interface.

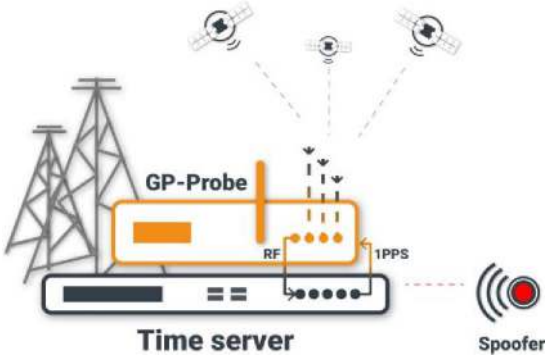
It's an ideal solution for the time-critical applications like 5G, financing services, DVB-T, power grid systems.

**How it works**

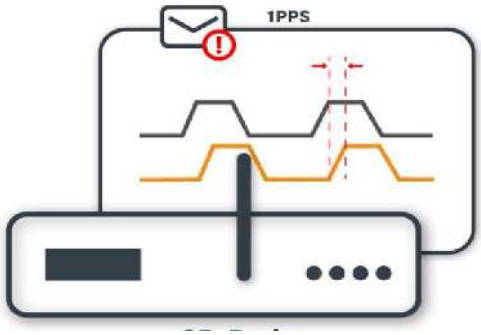



1. Install GP-Probe on your time/coordinates-critical infrastructure, for example, near your time server. The GP-Probe has an output RF port for transmitting GNSS signals to the protected receiver. In case of spoofing or low signal quality, GP-Probe disables the output port.

2. To guarantee uncompromised detection of any type of advanced spoofing, GP-Probe uses 3 spaced antennas for measuring GNSS signals. Every second GP-Probe registers more than 900 parameters for all visible GPS, GLONASS, BeiDou, Galileo satellites.




P +61 3 9551 7334
E sales@stepglobal.com W stepglobal.com
Unit 7, 444 Warrigal Road, Heatherton, Victoria Australia 3202

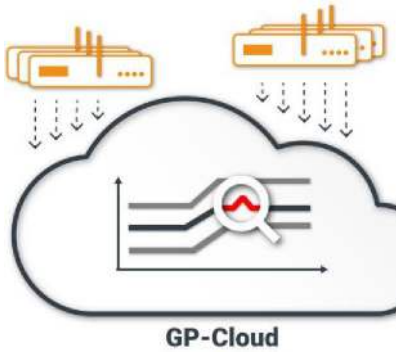


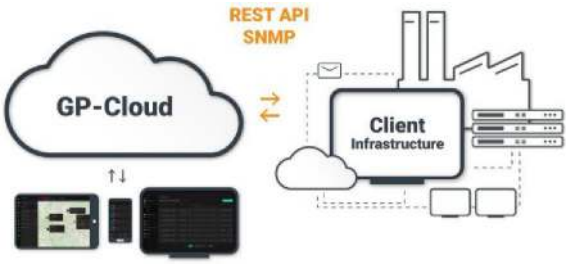

**3.** For advanced time server protection, the GP-Probe can measure the difference between internal and external PPS. In the case of any major mismatch, GP-Probe instantly sends the corresponding alarm to the GP-Cloud.

This functionality helps to improve the overall reliability of synchronization systems.

**4.** GP-Probe transmits raw data to the GP-Cloud for real-time processing. GP-Cloud analyzes data and computes the time/coordinates accuracy and probability of spoofing/jamming.

The spoofing detection algorithm is based on the cutting edge Machine Learning Techniques for anomalies detection and classification.




**5.** Monitor your entire time/coordinates critical infrastructure in a single user-friendly web-interface. If the system detects any type of spoofing or jamming, as well as GNSS parameters degradation, you will receive instant notification.

A powerful REST API allows you to integrate your existing infrastructure to our solution.

For More information contact Step Global

P +61 3 9551 7334
E sales@stepglobal.com W stepglobal.com
Unit 7, 444 Warrigal Road, Heatherton, Victoria Australia 3202