GPSPATRON – GNSS Quality Monitoring System

With a world that is heavily dependent on Global Navigational Satellite Systems (GNSS), it is important that the integrity of the signals, especially location and time accuracy, remain uncompromised. There are 4 billion of GNSS receivers in various applications around the world that are highly susceptible to GNSS signals quality degradation. This includes:

Financial Services

Based on regulations MiFID II and SEC 613, financial service firms in Europe and the US must comply with the 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

PMU, as the central part of WAMS, requires exactitude of synchronization to ensure flawless Network Monitoring and Automatic Protection. Time synchronization distortion of a PMUs can lead to cascading faults and large-scale power blackouts.

Autonomous Machines

The success of autonomous machines requires uncompromised accuracy and reliability of the GNSS. Coordinate or speed manipulations can lead to undesired damages, and even human loses.

5G

Meeting the 5G time synchronization accuracy requirements is the most challenging for the industry. GPSPATRON helps to obtain the mandatory precision from GNSS in difficult jamming conditions, an inferior GNSS antenna placement, and even under spoofing.

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 Centers

Data centers require sub-millisecond precision timestamping 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/jamming attack, high RF interference level.

Airport

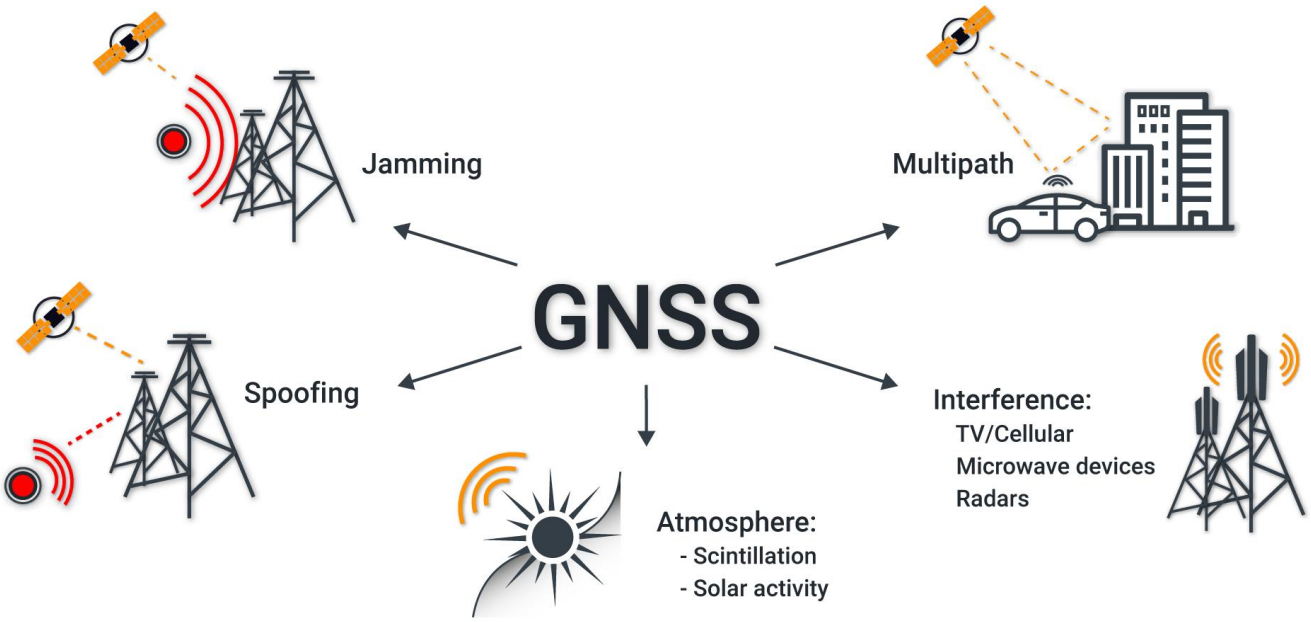
According to ICAO Annex 10 requirements, airports need to implement GNSS monitoring and recording systems to ensure a quick response to the degradation of accuracy and to conduct incident investigations.

Network RTK

GNSS RTK network 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:



The power of GNSS signals is as low as minus 155 dBW. Therefore, the receivers are ultra-sensitive to even out-of-band RF interferences generated by assorted electronic devices.

Since GNSS can play a key role in assuring numerous systems' operability, it is essential to provide analysis and storage of navigation signal parameters for quick response to emergency events and the investigation. For example, if your network of GNSS RTK sites fails every so often, or you have many random errors during self-driven car tests, a tool should monitor the status of the navigation field.

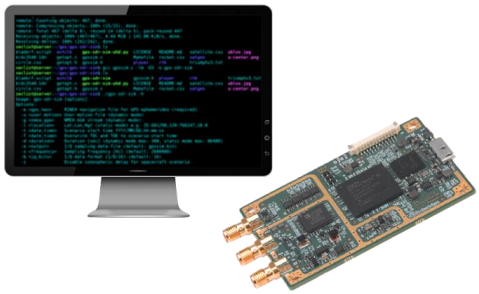
GNSS Spoofing

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 experiencing problems with time synchronization of time servers with GNSS receiver. An unintended spoofing attack leads to time and coordinates shift and cause unpredictable heavy damages to businesses.

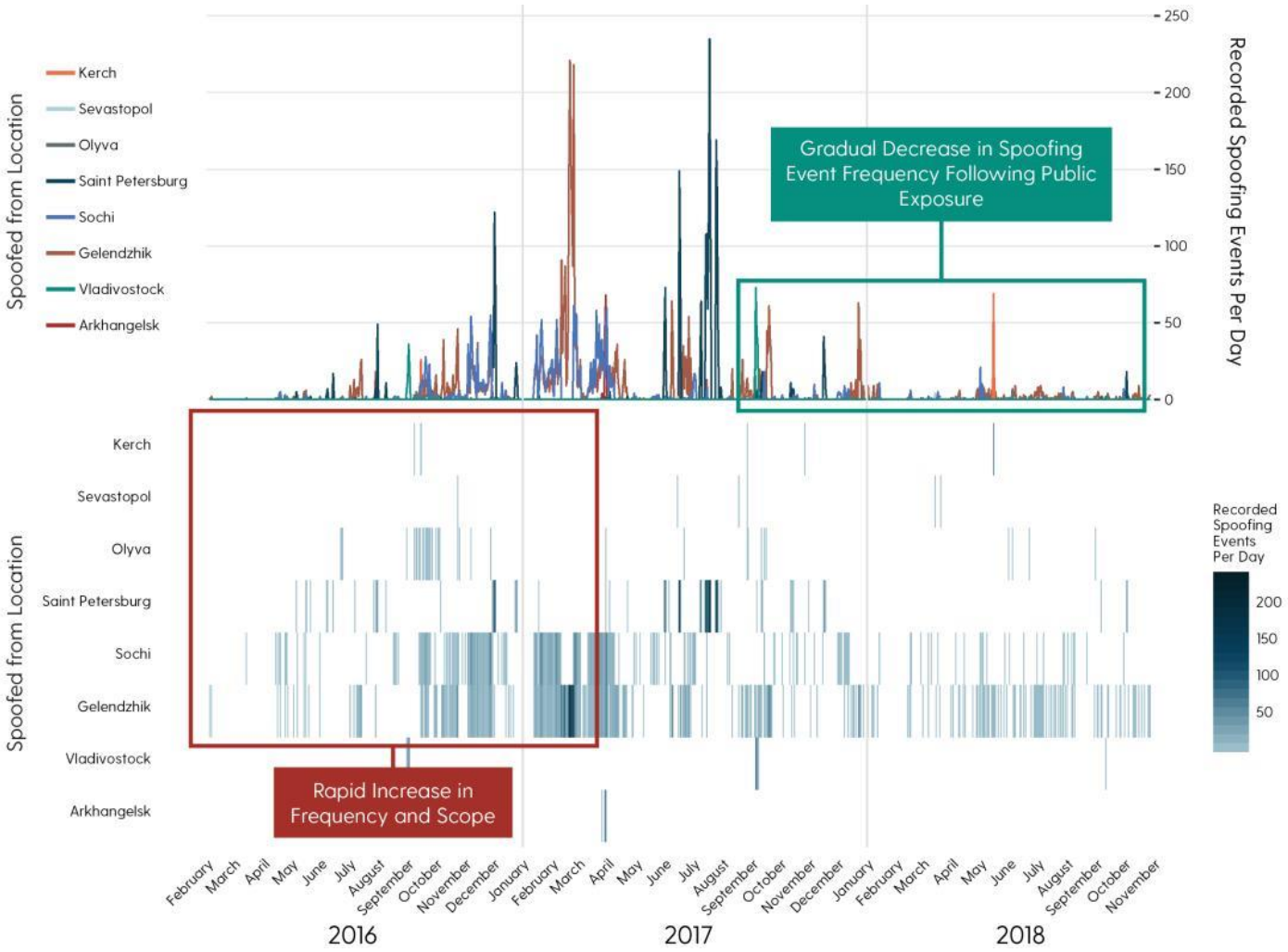
GPSPATRON



7 years ago, GPS spoofing used to require considerable technical skills and financial expenses. Now it can be done with low-cost commercial hardware (SDRs like HackRF) and software downloaded from the GitHub (e.e., 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 — ABOVE US ONLY STARS. There were 9883 emergency events registered over the two years of research.



GPSPATRON Solution

GPSPATRON - GNSS Quality Monitoring System is a neural network based distributed system for monitoring and protecting time/coordinates critical infrastructure. It supports: GPS, GLONASS, BeiDou, Galileo.

GNSS Signal Monitoring

Measurement and storage of GNSS signal parameters. Signal quality estimation

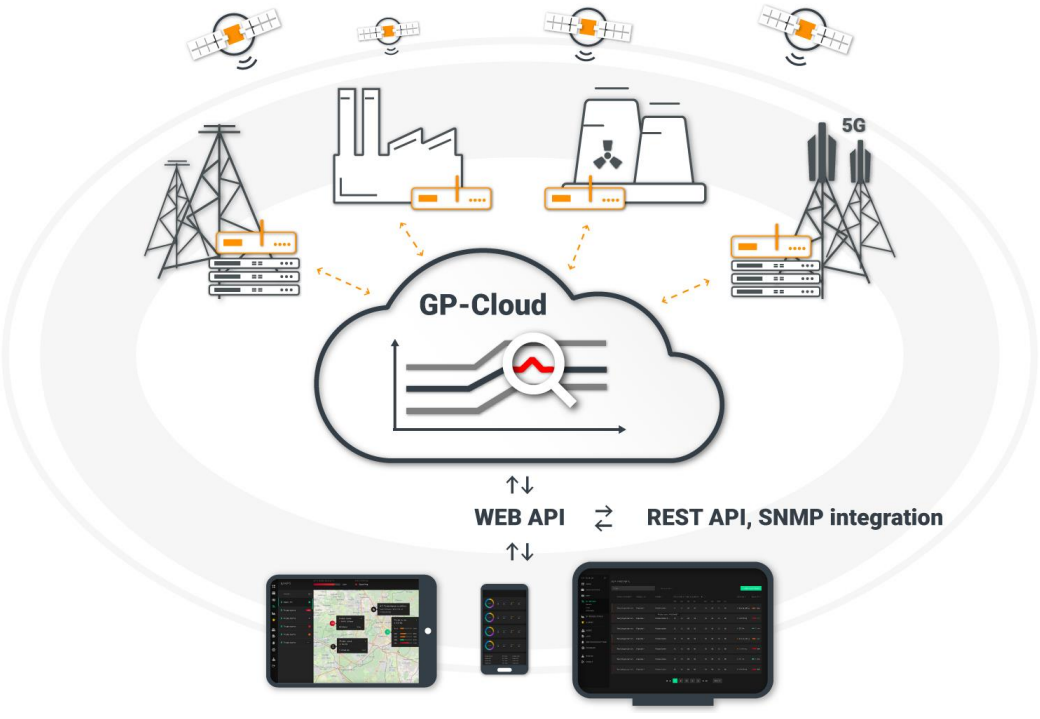
GNSS Threat Detection

Detection of military-scale, multi-constellation GNSS spoofing and jamming and other threats

Synchronization Monitoring

Precise real-time PPS phase accuracy monitoring for time-critical applications

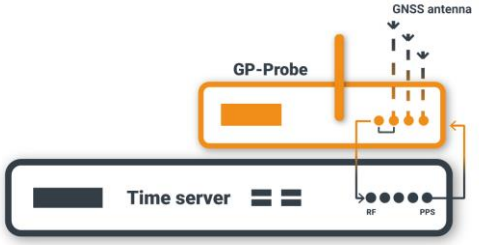
The system consists of affordable three-channel GNSS probes (GP-Probe) and a powerful cloud service (GP-Cloud). GP-Probe conducts GNSS signal measurements using 3 channels with angle-of-arrival estimation and transmits raw data to the GP-Cloud for real-time processing. GP-Cloud uses advanced anomaly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

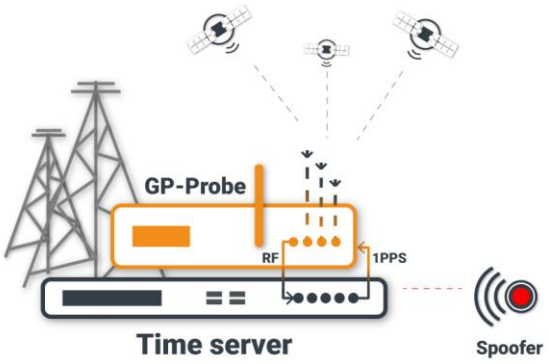


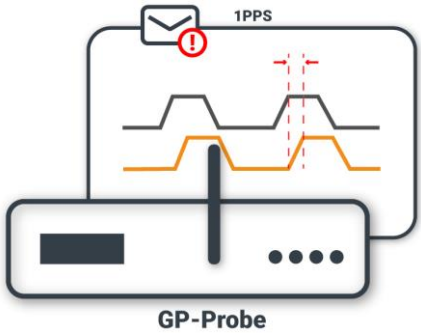
1. Install GP-Probe on your time/coordinates-critical infrastructure, for example, near your time server. The GP-Probe has a transit RF port for transmitting GNSS signals to the protected receiver.

In case of spoofing or low signal quality, GP-Probe disables transit 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.



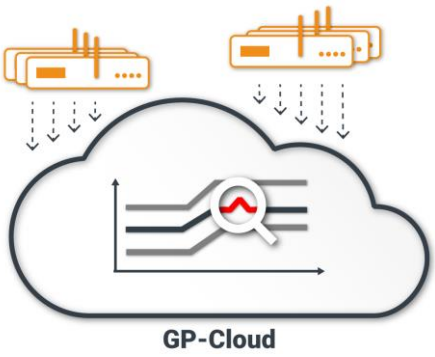


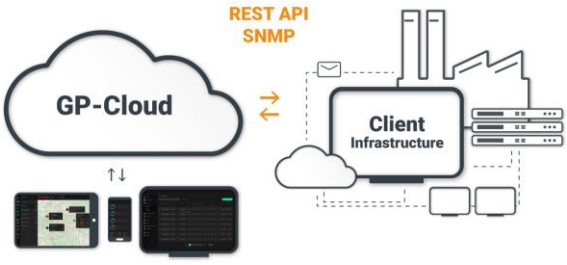
3. For advanced time server protection, the GP-Probe can measure the difference between internal and external PPS. In the case of any major mismatch, GP-Probe instantly sends the corresponding alarm to the GP-Cloud.

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.

GP-Probe TGE2
Time Guard Edition 2

Three-channel probe for GNSS signal quality measurements and GNSS threat detection

The GP-Probe TGE2 is designed to protect time servers (PNT) against a GNSS threat such as cutting-edge intentional spoofing, jamming, ionospheric scintillation, system errors, for example. An embedded PPS phase error measurement function enables the reliable monitoring of the time server's health. The GP-Probe, in conjunction with the GP-Cloud, allows developing a robust and resilient clock synchronization system for critical infrastructure.

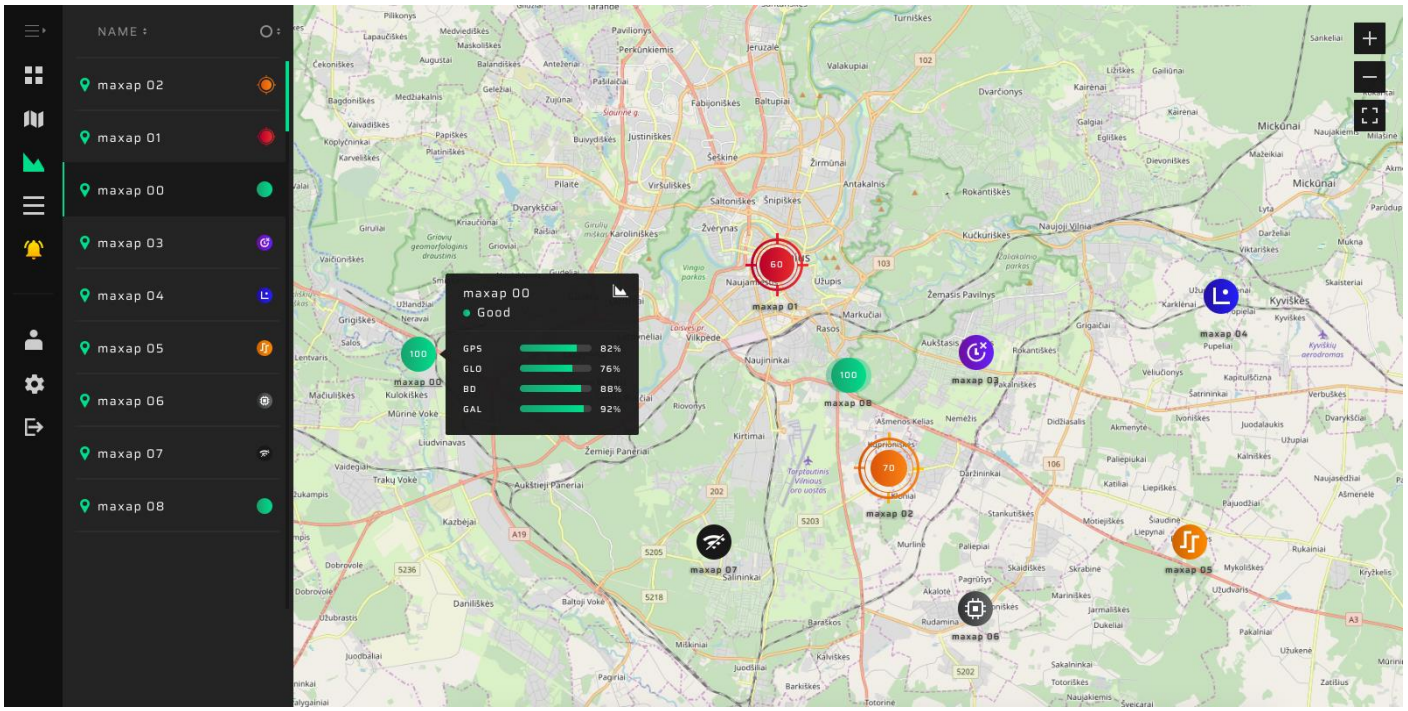
Key Features

- Three RF channels for intentional, synchronous, multiple-TX GNSS spoofing detection.
- GNSS signal quality measurements: pseudorange errors, carrier phase, SNR, etc.
- PPS input for the external time server health checking. The GP-Probe measures the time offset between internal and external PPS. PPS input supports low-current signals.
- Optional GP-Blocker with an embedded noise generator suppresses the most powerful counterfeit RF signals.
- PPS output for synchronization of external equipment.
- Optional RF power divider - GP-Divider enables to utilize one GNSS antenna for two receivers. The GP-Divider supports the GNSS antenna preamplifier current simulation.
- Form factor: 19-inch rack, half-size.
- Double power module: 110 – 220 AC, 18 – 75 DC.
- Active/passive GNSS antenna support.
- 4G modem and 100BASE-TX Ethernet for data transferring to the GP-Cloud.
- Web interface for configuration (HTTP or HTTPS).
- External devices can be controlled via remote interfaces: RS232/Telnet/SNMP with embedded Lua scripting language. GP-Probe can send commands to the connected time server for switching to holdover, etc. This facilitates integration with existing client infrastructure.

GP-Cloud

Web applications for monitoring the quality of the GNSS signal and detecting Spoofing attacks

Control all your GNSS-dependent critical infrastructure in a single UI



Key Features

- The application processes in real-time the data from the connected GP-Probes, calculates the quality of the signal and its accuracy, detects spoofing and stores all results in the database.
- The application is distributed over two types of licenses: cloud-based and self-hosted
- Synchronous GNSS spoofing detection algorithm based on neural network.
- Detection of signal anomalies that result in the degradation of coordinates/time accuracy.
- GNSS signal quality estimation.
- Interactive dashboard and detailed alarm logs tracking.
- Cloud or self-hosted, annual or perpetual license options.
- Interactive map with real-time GNSS health status.
- 15 informative charts for in-depth data investigation and analysis.
- Time and position accuracy calculation.
- GP-Probe's measurements history.
- Available as an enterprise-grade solution.
- Powerful REST API with documentation in Swagger.

GPSPATRON Services

Evaluate the Vulnerability of Your GNSS Equipment to Spoofing

Do you have GNSS-dependent critical infrastructure and you wish to evaluate its vulnerability to a new and more common threat of GNSS spoofing attacks?

GPSPATRON provides laboratory testing services of your GNSS equipment for identifying vulnerabilities to spoofing attacks. Since we are developing a dedicated system of protection against spoofing and experimenting in the field, we hold all the necessary empirical knowledge about different types of attacks, their features, as well as their methods of execution. To simulate a spoofing attack, we use our unique solution — the GP-Simulator. For your exact requirements, we will modify test methods and protocol templates. Typical test objects are the RTK Base Stations and Time Servers.

We would also like to draw your attention to our Test Patron team — test and measurement automation provider. Our Test Patron team can custom-build automated test stands for performing the corresponding types of tests.

On-Site Testing of Your Infrastructure's Resistance to GNSS Spoofing

Would you like to evaluate the vulnerability of your entire GNSS-dependent infrastructure to spoofing?

The GPSPATRON team can conduct all the indispensable tests on your site following a pre-approved test schedule. You can appraise how your existing infrastructure responds to a timestamp shift, PPS shift, and GNSS signal quality degradation.

GNSS Signal Quality Monitoring as a Service

Is it essential to select the appropriate site for GNSS equipment like RTK Base Station, Time Server, etc.? Or do you want to confirm that the quality of GNSS signals on your current site meets strict requirements?

GPSPATRON offers its solutions as a service so you can monitor and protect your time coordinate-critical infrastructure without investing in new hardware and software. We can lease the GP-Probe, install it on your site, and conduct the corresponding measurements.

The GP-Probe registers more than 900 parameters for all visible GPS, GLONASS, BeiDou. Galileo satellites every second. The massive volume of data is collected and stored in the GP-Cloud for further analysis. We submit all the compulsory methods and tools required to scrutinize that data for calculating GNSS quality indicators. We prepare test reports with further recommendations. This service is expedient for EGNOS and WARS providers and operators for the factual site selection and RFI monitoring.

System Installation Services

The GPSPATRON team provides the GNSS quality monitoring system as a turnkey solution. Our professional team can install the GP-Probe on your infrastructure, arrange it, and implement its integration.

System Integration Services

We can integrate our solutions into your existing infrastructure without hindrance. The GP-Cloud provides a powerful API for third-party service integration, which can be implemented on your own or contracted from us as a service.

GP-Probe Customization

The GP-Probe can be personalized to adapt to any circumstances. The customizations include but are not limited to: IP – 67, Vibration protection, built-in GNSS antennas, built-in battery, power supply, and custom radio links.