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

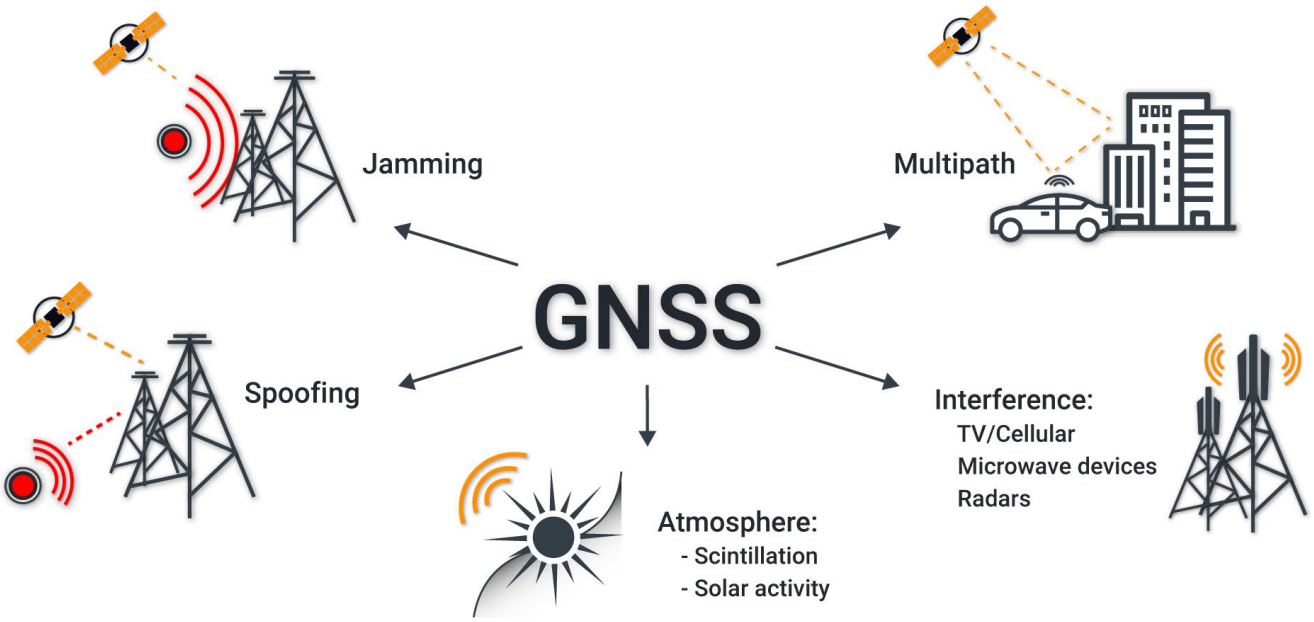
According to ICAO Annex 10 requirements, airports need to implement GNSS monitoring and recording systems to ensure a quick response to the degradation of accuracy and to conduct incident investigations.

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.

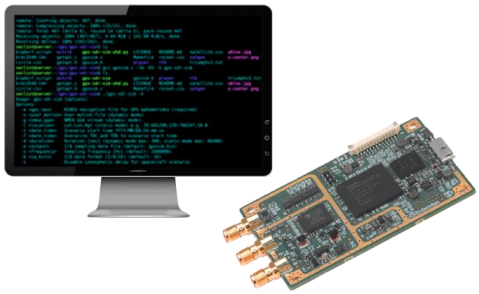
GNSS Spoofing

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.

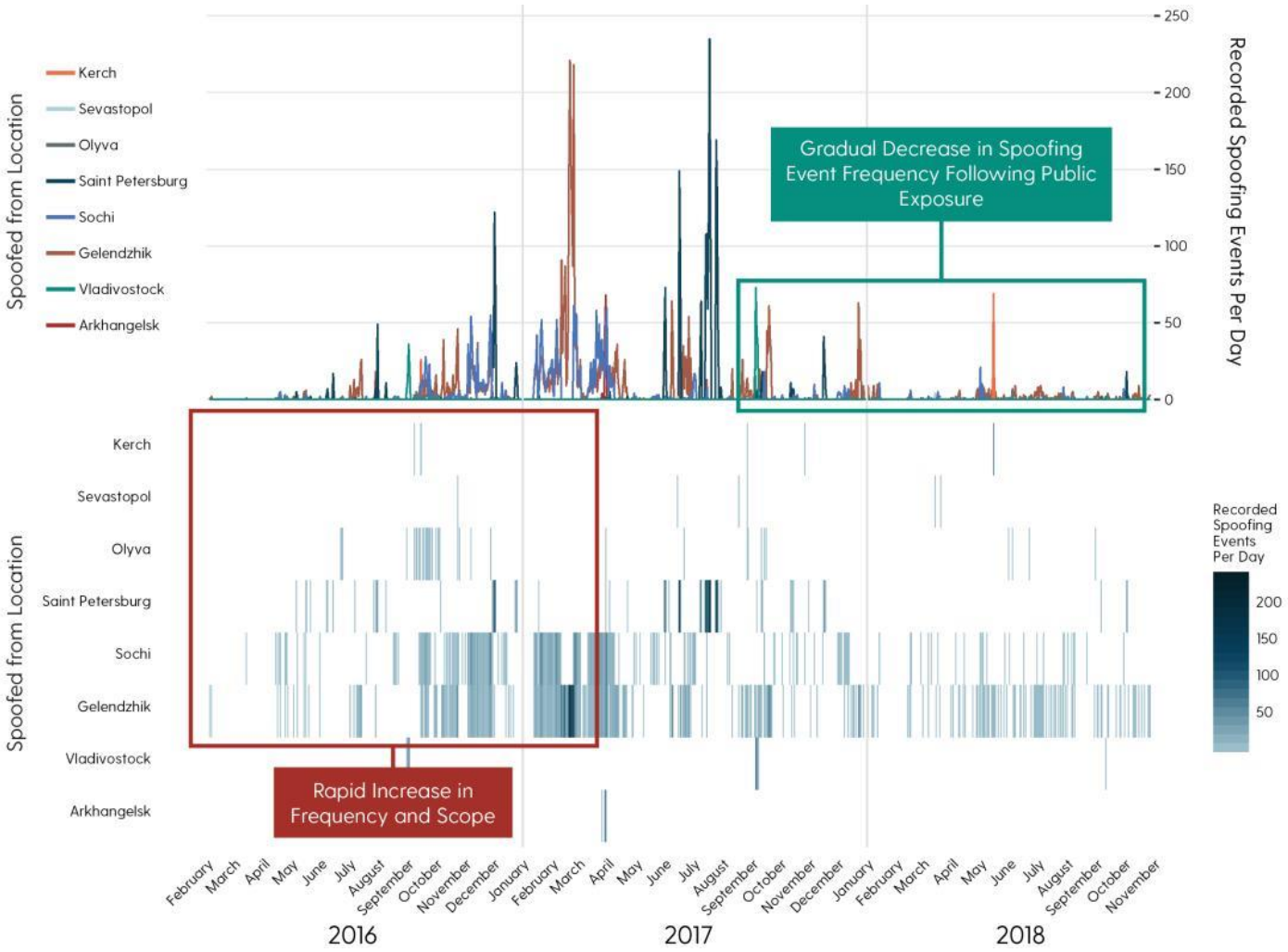
GPSPATRON



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 provides solutions to protect GNSS-dependent infrastructure against GNSS spoofing/jamming or other GNSS signals anomalies that cause time/position accuracy degradation.

Applications:

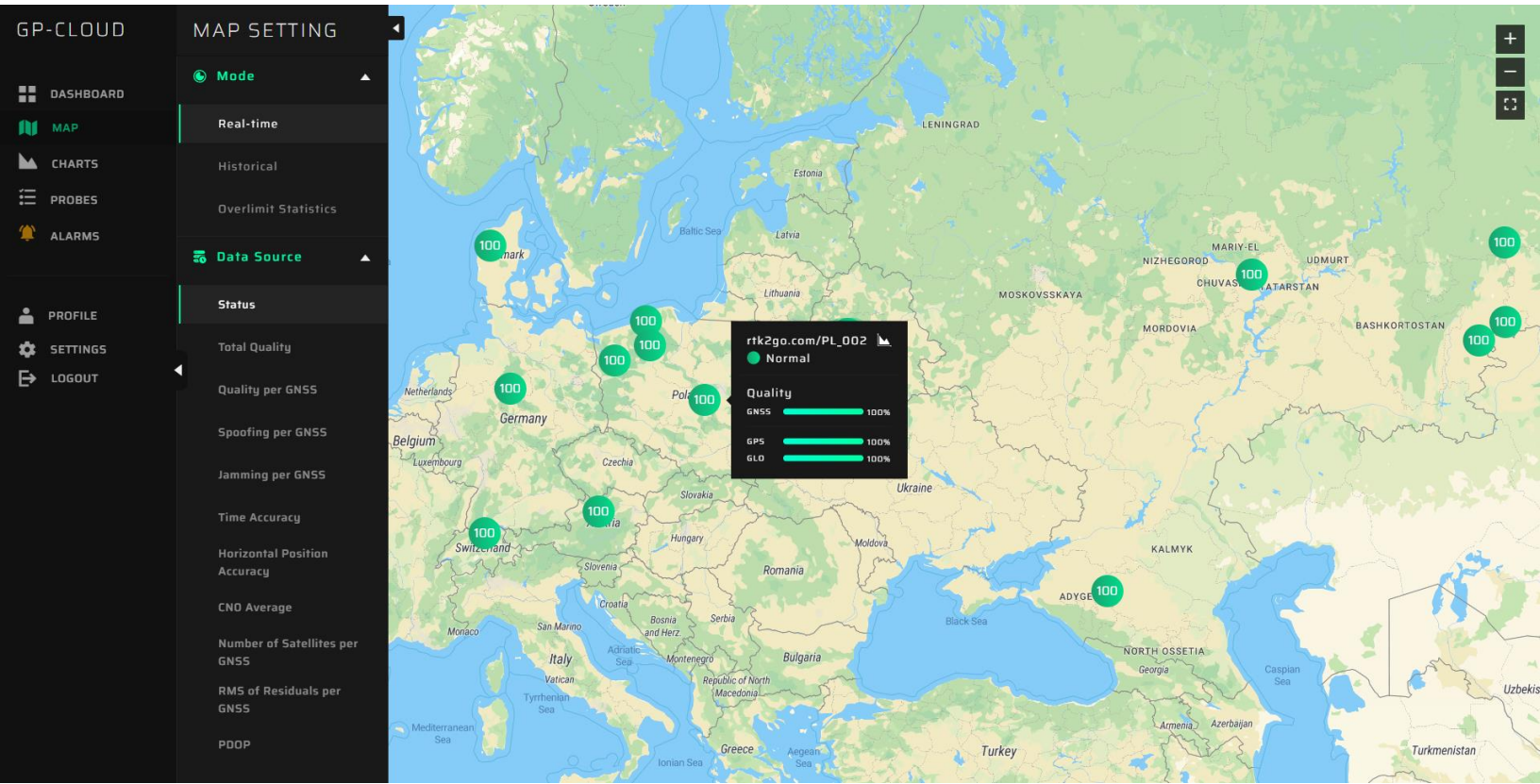
- time server protection against sophisticated GNSS spoofing attacks
- GNSS signal quality monitoring and logging
- GNSS interference detection, classification, and localization
- anomaly detection in raw data from RTK base station

The system consists of a three-channel GNSS probe (GP-Probe) and a cloud service (GP-Cloud). GP-Probe conducts GNSS signal measurements using three channels with spatial signal analysis and sends raw data to the GP-Cloud for real-time processing. GP-Cloud uses anomaly detection and classification algorithms.

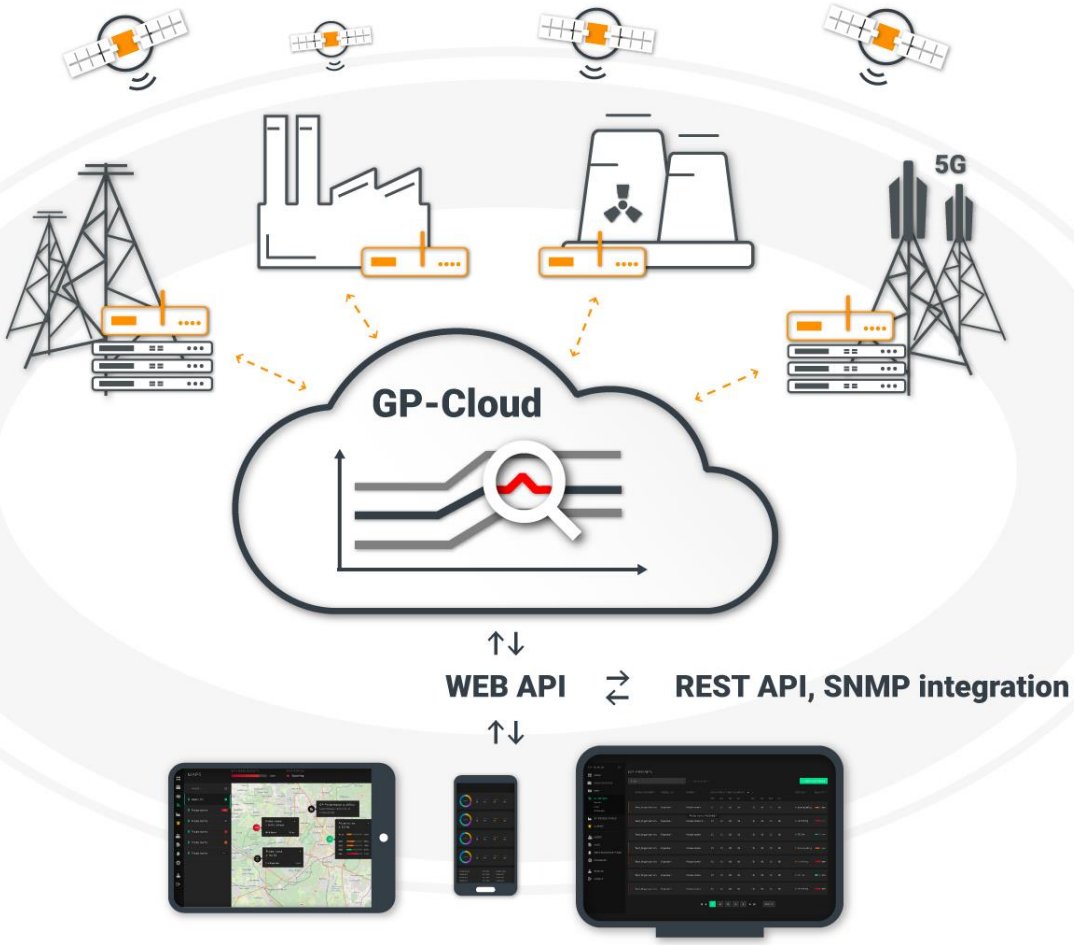
Key features:

- three-channel probe and spatial signal analysis ensure detection of deliberate precision GNSS spoofing attacks.
- Embedded FPGA-powered RF signal analyzer provides spectrum monitoring, RF interference detection\classification, TDOA implementation for source localization.
- true real-time. Spoofing detection latency is less than three seconds.
- GP-Cloud can process NMEA, RTCM, SBF data streams.
- GP-Cloud limitless horizontal scaling.
- supports GPS, GLONASS, Galileo, BeiDou.

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



The central part of the system is the web application called GP-Cloud.
Tech stacks: .net core, Angular, Python, PostgreSQL with time scale plugin, RabbitMQ, Dapper, Swagger.



The architecture of the software allows unlimited scalability of the application. We can process raw GNSS data nationwide in real-time. GP-Cloud can process data from GP-Probe or other sources of GNSS data like RTK base station.

In combination with three-channel GP-Probe, the solution detects all spoofing attacks scenario: asynchronous, synchronous, synchronous with multiple-TX, meaconing.

GP-Cloud estimates signal quality for each GNSS individually and supports the detection of the following events: spoofing, jamming, low position\time accuracy, PPS offset (applicable for GP-Probe only)

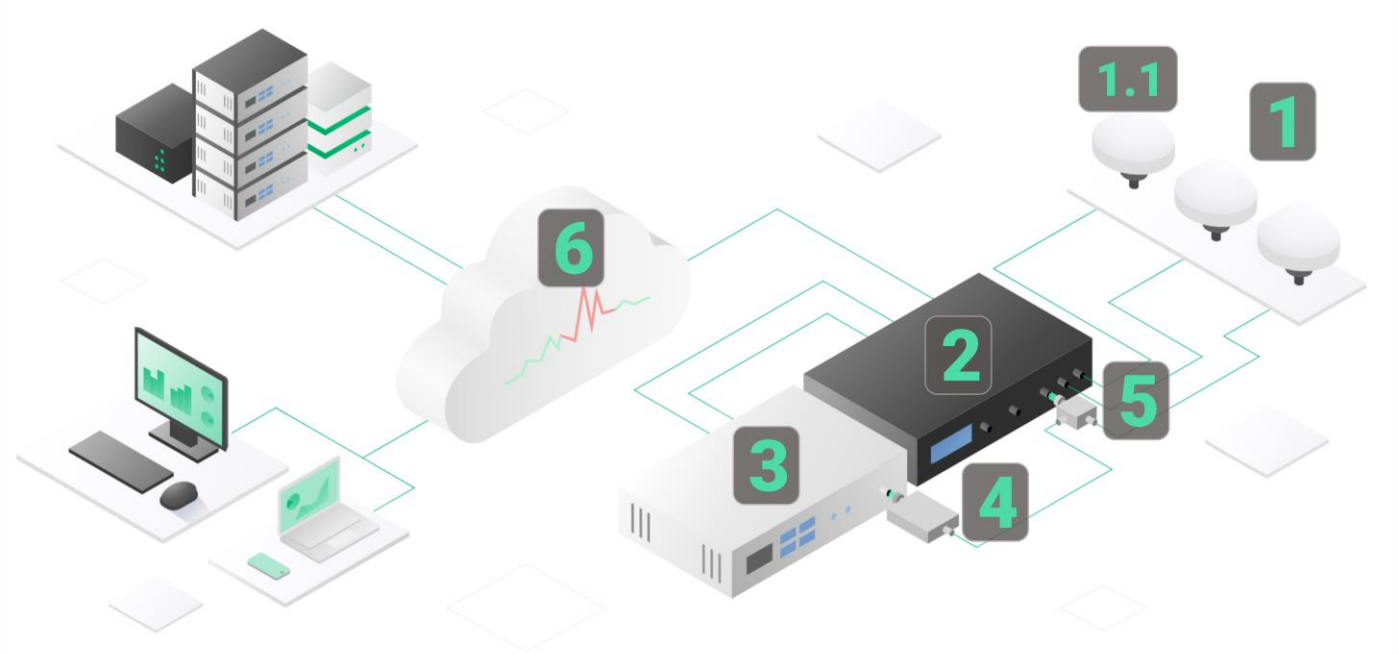
We utilize mathematical models and a neuron network for anomaly detection/classification in raw GNSS data. The detection algorithms are tuned for low possible spoofing detection latency:

- spoofing false-positive rate is 0.1% for the real live urban environment (without unintentional interference).
- latency – one or two 1-Hz data samples for spoofing detection. (Really depends on attack scenario)

How to protect a time server against GNSS spoofing

The GP-Probe measures GNSS signal parameters of all visible satellites and transmits raw data to the GP-Cloud for real-time processing. If GP-Cloud detects spoofing/jamming or signal quality degradation, it sends a notification to GP-Probe. The GP-Probe sends a command to GP-Blocker via RS485 interface (not shown in diagram) to block the GNSS antenna port of the time server. The time server loses satellites and switches to Hold Over mode.

Spoofing detection latency < 3 sec



1. Antenna system. To guarantee uncompromised detection of an advanced spoofing attack, the GP-Probe uses three-spaced antennas for spatial integrity analysis of GNSS signals.

1.1. The GNSS antenna will be shared between two receivers: the first channel of the GP-Probe and the GNSS receiver of a time server.

2. GP-Probe. The first channel is connected to a shared antenna through GP-Divider. For additional time server health monitoring, you can connect the server's PPS output to the probe PPS input. The GP-Probe measures the difference between internal and external PPS. The protected time server 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.

3. Protected time server. The server's GNSS receiver is connected to the shared antenna through GP-Blocker and GP-Divider.

4. GP-Blocker. An RF switch with 110 dB of RF isolation level and embedded L-band GNSS jammer.

5. GP-Divider. 2-way GNSS splitter to share one GNSS antenna between two receivers

6. GP-Cloud.

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. 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.

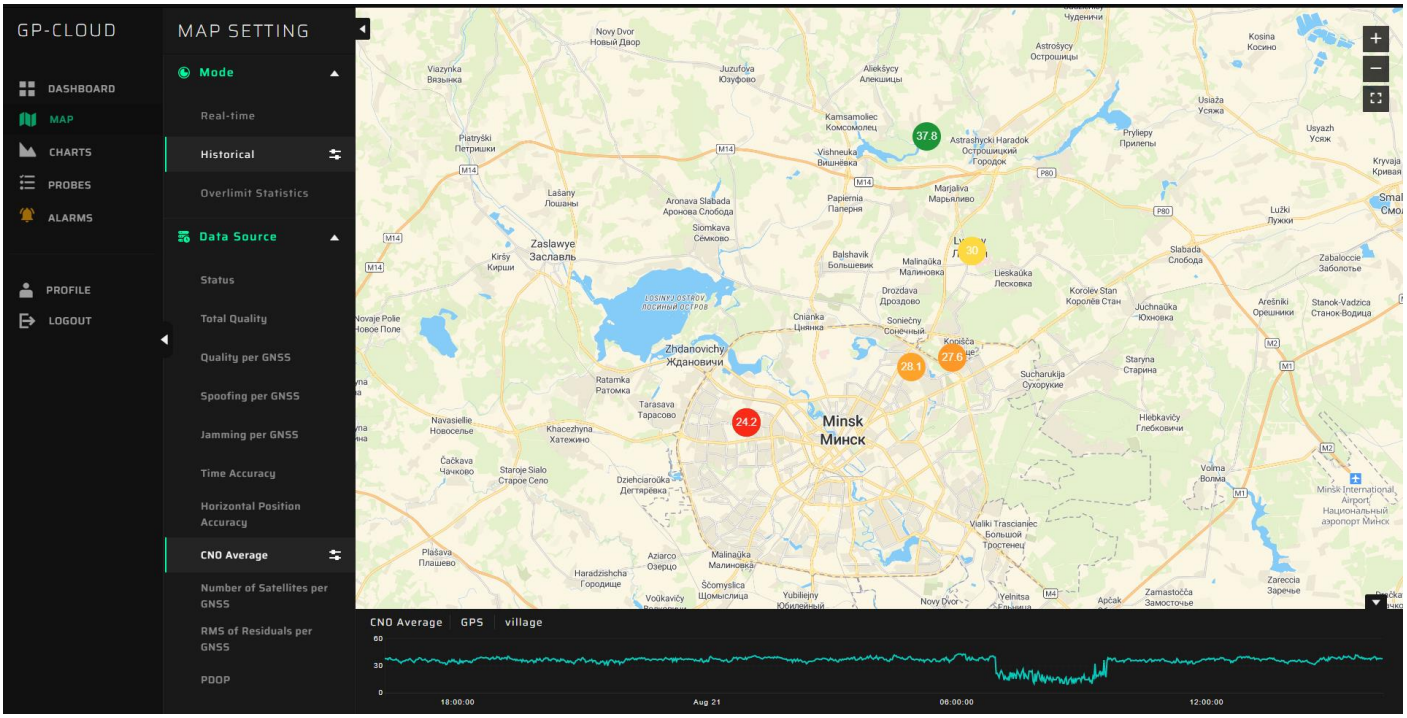
Key Features

- Three RF channels enable spatial signal analysis for intentional coherent spoofing detection.
- GNSS signal quality measurements: pseudorange errors, carrier phase, SNR, etc.
- PPS input for checking time server health and monitoring the entire synchronization system. 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 application for true real-time GNSS signal quality monitoring, logging, and post-analysis

Advanced GNSS spoofing/jamming/ interference detection and classification

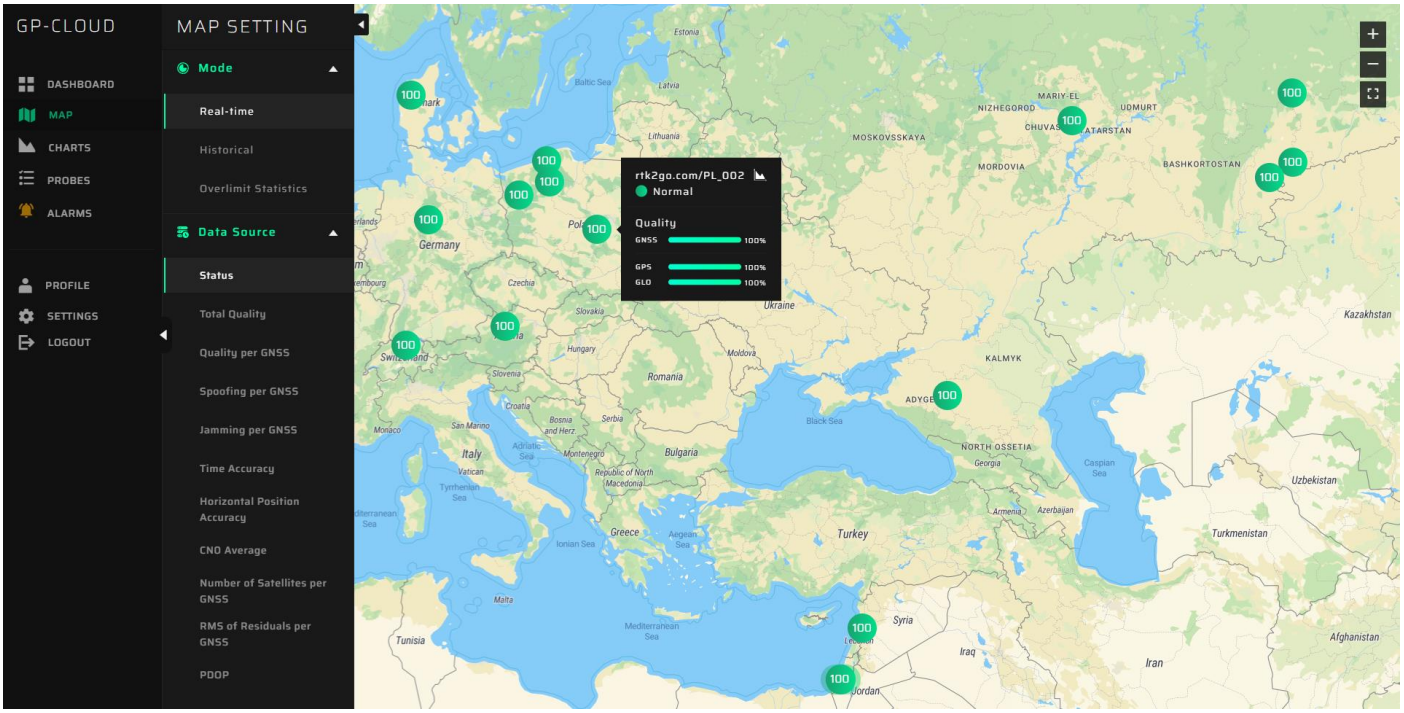


Key Features

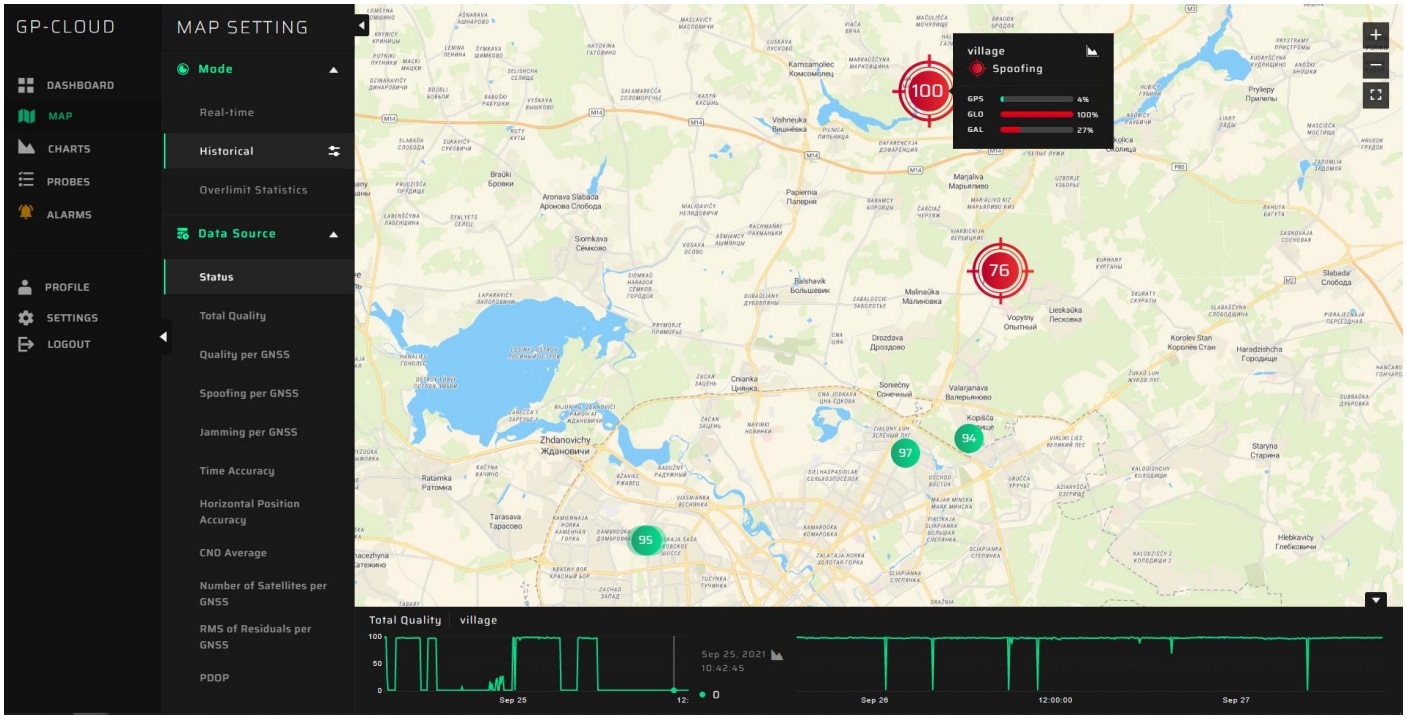
- The application processes in real-time the data from the connected GP-Probes or GNSS receivers, calculates the quality of the signal and its accuracy, detects spoofing, and stores all results in the database.
- The application is distributed over two types of licenses: cloud-based and self-hosted
- Coherent GNSS spoofing detection algorithm based on neural network.
- Detection of signal anomalies that result in the degradation of coordinates/time accuracy.
- GNSS signal quality/accuracy estimation.
- The GP-Cloud supports 1-Hz GNSS data from RTK base stations or other GNSS probes\receivers using the RTCM, NMEA, Septentrio SBF protocols over NTRIP
- Dashboard, events log, map, and advanced charts for in-depth data investigation and analysis in real-time.
- Enterprise-grade application with limitless scalability
- Powerful API with documentation in Swagger allows you to integrate the solution in an existing infrastructure.

GPSPATRON

Map for real-time GNSS-dependent infrastructure monitoring



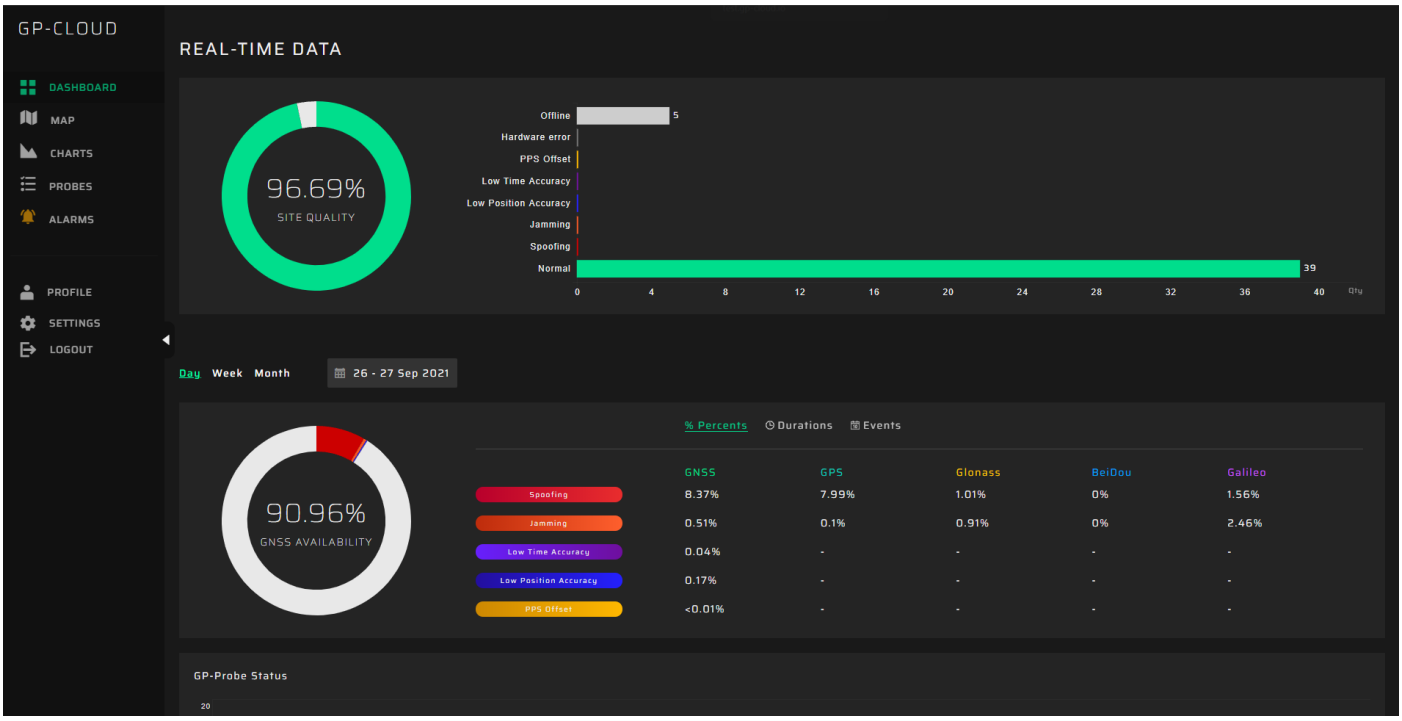
Map for historical data analysis and statistic review



GPSPATRON

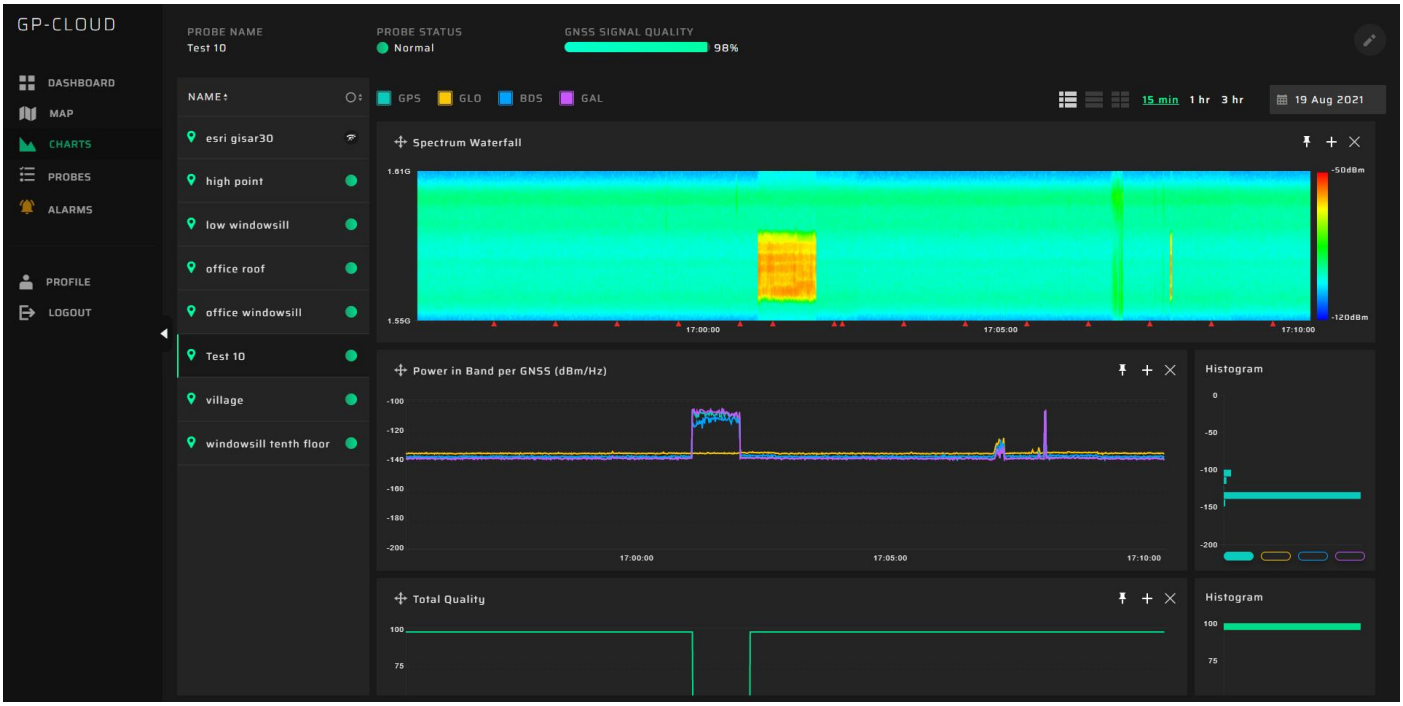
Cool graphs for analyzing raw data in real time and for investigating recorded data

Dashboard for statistical analysis and current situation monitoring

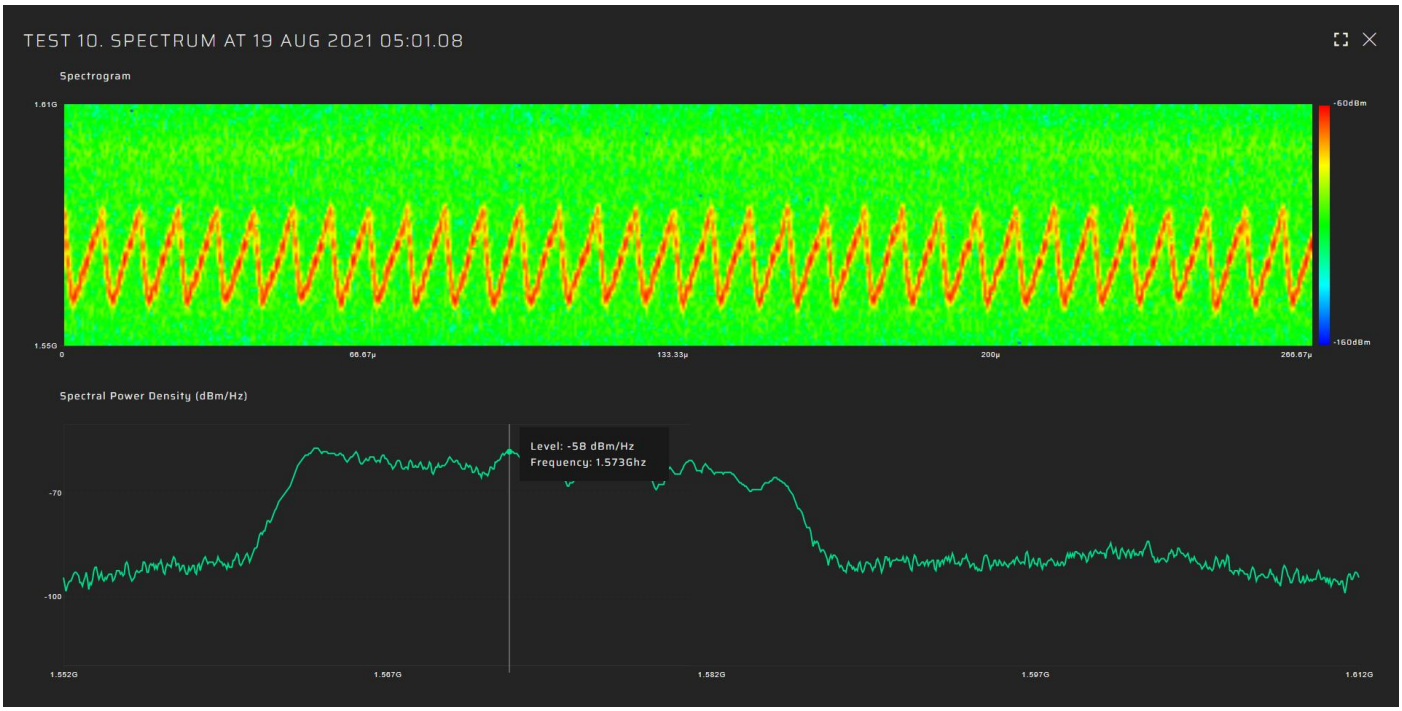


GPSPATRON

Spectrum waterfall and power in band

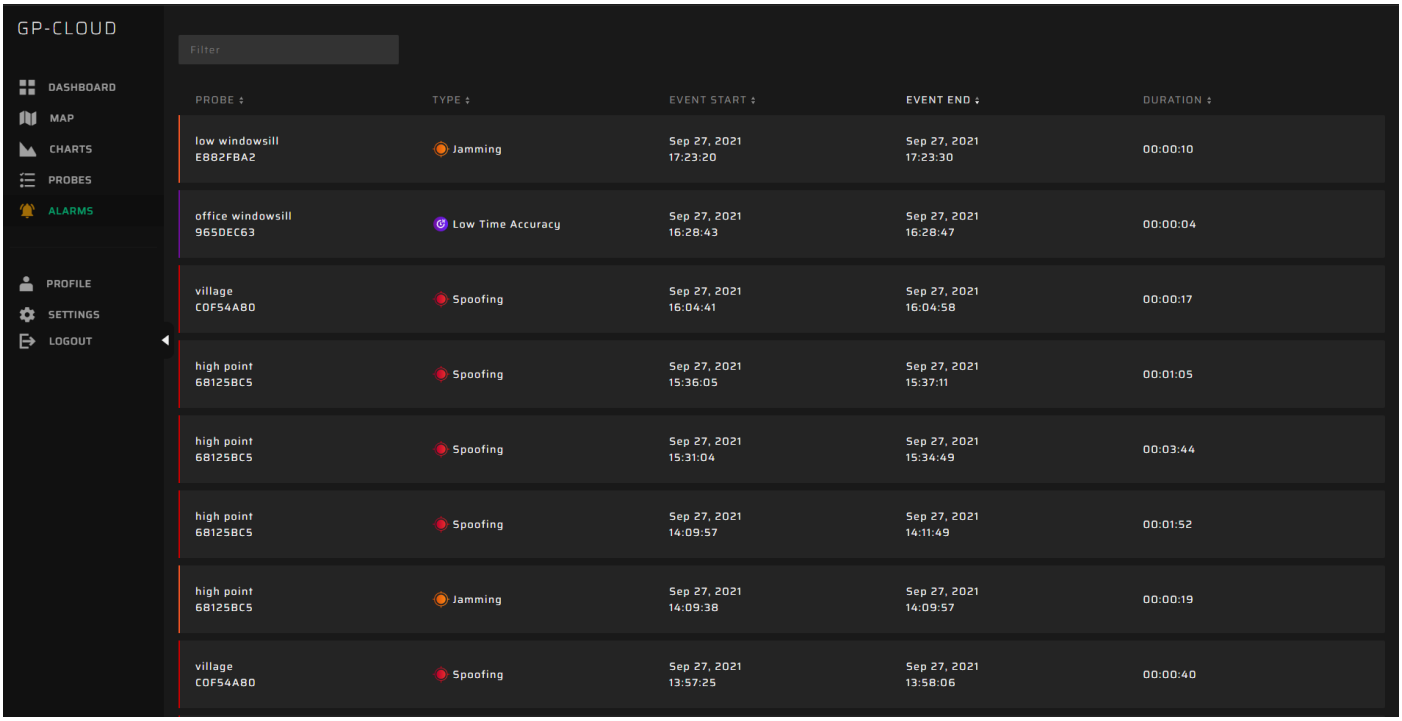


Spectrogram and power spectrum for interference analysis

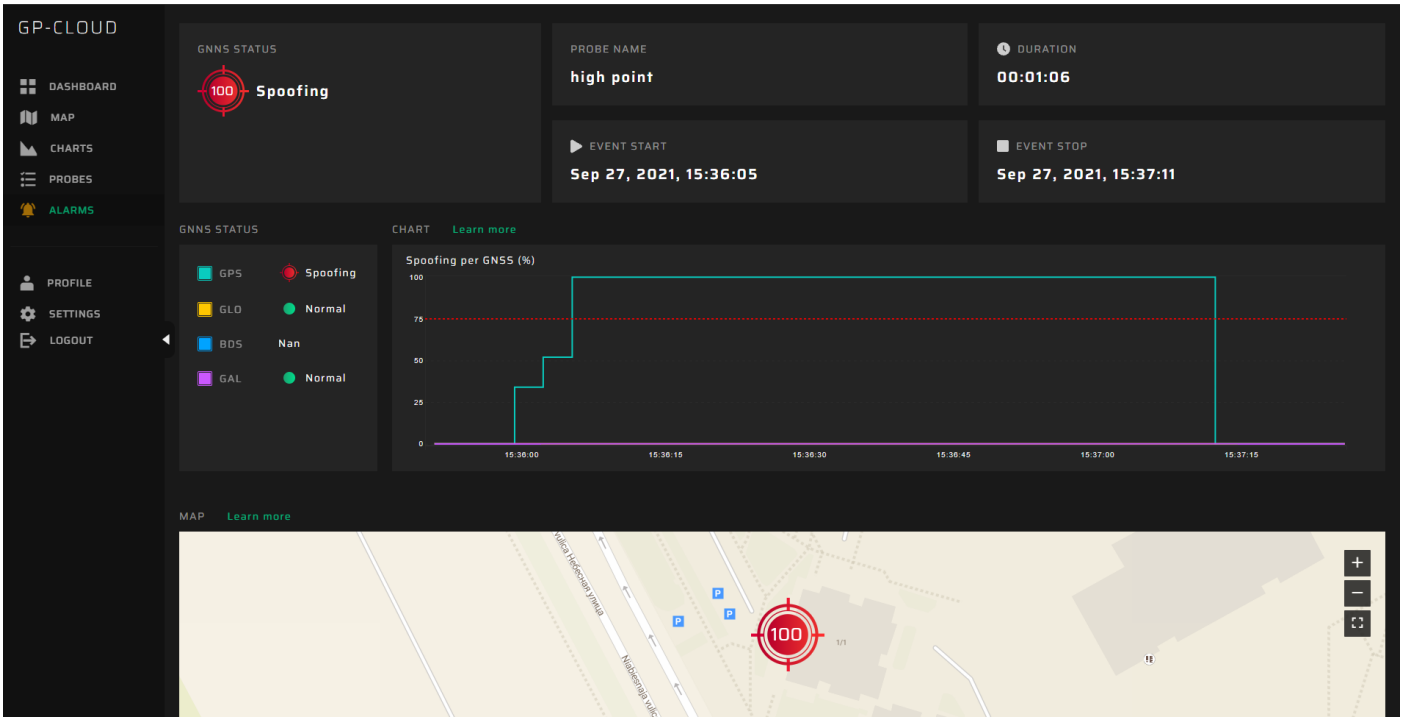


GPSPATRON

List of registered events



Event status with detailed information and comments



GPSPATRON

Useful Resources

1

Sign up for Resource Center updates

You will find there time servers spoofing vulnerability reports, GNSS receiver testing report, scientific articles, datasheets, presentations

https://gpspatron.com/resource-center/

2

Subscribe to our YouTube channel

Interesting experiments with GNSS spoofing, receiver testing, the solution description

https://www.youtube.com/c/GPSPATRON/videos

3

Stay up-to-date with our company news

https://www.linkedin.com/company/gpspatron

https://twitter.com/gpspatron

Nice video presentation of the GNSS spoofing problem and how we solve it:
https://youtu.be/qLcHe18rtvI

An article describing the critical importance of low spoofing response times:
https://gpspatron.com/the-significance-of-low-gnss-spoofing-detection-latency/

Videos showing how to simply spoof a GNSS receiver:
https://youtu.be/g-bdK7tRpBI
https://youtu.be/Ya_B7tqA-X8

Video explaining why GP-Blocker is needed:
https://youtu.be/sVDZRcFbHFo

To protect against spoofing you should know what types of attacks exist. Learn more:
https://gpspatron.com/gnss-spoofing-scenarios-with-sdrs/
https://gpspatron.com/types-of-gnss-spoofing/
https://gpspatron.com/types-of-gnss-spoofing-explainer-video/

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.