GPSPATRON's Strategy for GNSS Defense

In our increasingly interconnected world, the accuracy and integrity of GNSS signals is paramount. GNSS receivers, numbering in the billions globally, are integral to a myriad of sectors, yet remain vulnerable to RF interference like jamming and spoofing. This poses threats to critical national infrastructures:

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.

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.

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.

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.

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.

Power Grid System

Phasor Measurement Units (PMUs) are vital for keeping a nation's power grid stable by measuring electrical parameters. They rely on precise GNSS-provided time synchronization. Any errors in timing can trigger widespread blackouts.

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.

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.

Railway

Spoofing/jamming of GNSS signals can seriously disrupt Automatic Train Control Systems, which depend on GNSS for accurate speed and location data. Interference poses a serious safety risk and schedule disruption.

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.

GNSS Jamming & Spoofing

GNSS signals are extremely faint, comparable to viewing a car's headlights from thousands of miles away, and they have no inherent protection against interference. Industrial equipment can unintentionally disrupt these signals, in addition to deliberate interference like jamming and spoofing:

JAMMING

Definition:
Noise generation in GNSS operation bands. Prevents reception of signals and determination of coordinates and time.

Use Cases:
- Auto transport drivers to defraud vehicle tracking systems, road tolling systems.
- For personal privacy.
- Military conflicts/exercises to disable navigation in a region.

Infrastructure Threat:
- Aircraft landing in poor visibility conditions
- Operations with heavy industrial drones
- Autonomous delivery".

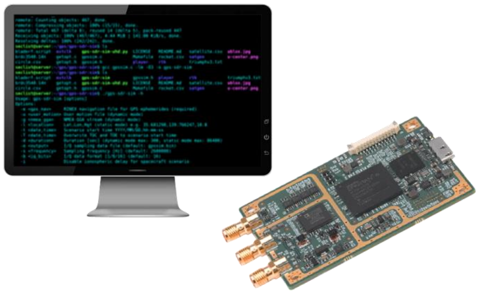
All applications requiring accurate real-time navigation.

SPOOFING

Definition:
Generation of fake GNSS signals with simulation of incorrect coordinates and time.

Use Cases:
- Anti-drone systems.
- Military Operations: to mislead missiles, drones.
- Hacker attacks on GNSS-dependent infrastructure.
- Deception of vehicle tracking systems.

Infrastructure Threat:
- Time-dependent applications: telecom, power grids, banking transaction processing centers, data centers.
- Navigation-dependent applications: marine vessels, autonomous vehicles, automated trains, etc.

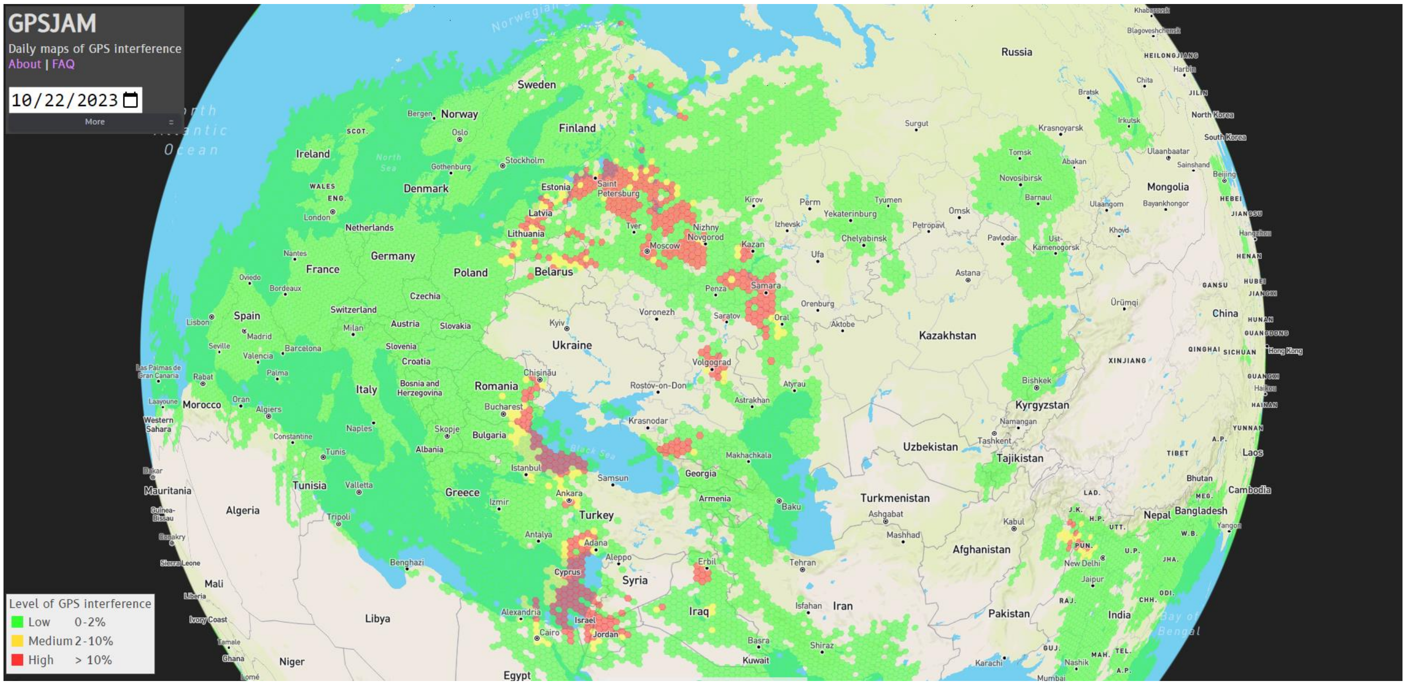


10 years ago, GPS spoofing used to require considerable technical skills and financial expenses. Now it can be done with low-cost commercial hardware (SDRs like HackRF) and software downloaded from the GitHub (e.g., osqzss/gps-sdr-sim).

So now, any student can organize a spoofing attack on a bank's processing center in 15 minutes.

GNSS Interference in 2023

The visual data depicted in the accompanying image, sourced from the GPSjam.org portal, illustrates a significant pattern of GNSS signal disruption as recorded by the ADS-B aircraft tracking system. The presence of red indicators demarcates areas where aircraft have reported substantial difficulties in receiving GNSS signals.



10/22/2023

The image displays only the most intense GNSS disruptions that have impacted aircraft at high altitudes. The situation on the ground is significantly worse.

Some recent news:

Dozens of planes sent off course with unprecedented navigation system attacks

'Spoofing almost caused us to enter Iranian airspace. Missiles were waiting.' - OpsGroup

Gaza & Israel GPS Jamming Increases with War

Suppressed GPS in Ukraine fuels development of US Army navigation tech - Defense News

GPS/GNSS interference everywhere - EuroControl at UN

Huge Increase in Middle-East Jamming

Lots of jammers near French airport

Hundreds of Drones Lost During Melbourne Show - DailyMail.com

GPSPATRON Solution

GPSPATRON provides the most robust solution on the market to safeguard vital infrastructure from GNSS spoofing, jamming, and signal anomalies that impact time and position accuracy.

The system includes a GNSS interference detector, the GP-Probe, which measures GNSS signals parameters and transmits the raw data to our web application, GP-Cloud, for immediate analysis. GP-Cloud employs advanced algorithms for detecting and classifying anomalies to identify complex spoofing or jamming attacks.

Besides the GP-Probe, GP-Cloud is compatible with multiple protocols including NMEA, RTCM, and SBF. This allows for seamless integration with any existing GNSS receiver, enabling extensive monitoring of GNSS-dependent infrastructure and providing instant notifications of any detected anomalies.

Key applications include:

- Safeguarding GNSS-dependent critical infrastructure from deliberate and non-deliberate attacks.
- GNSS interference detection, classification, and localization as part of radio spectrum monitoring.
- Protecting time-critical infrastructure against sophisticated GNSS spoofing.
- Monitoring and securing RTK base stations.
- Tracking and logging GNSS signal quality.

Notable features:

- The combination of GP-Cloud and GP-Probe ensures the detection of high-precision GNSS spoofing attacks.
- Accurate interference classification is crucial for identifying attack scenarios and formulating countermeasures.
- Genuine real-time operation with interference detection latency under three seconds.
- Limitless horizontal scaling of GP-Cloud for nationwide data processing.
- Compatibility with GPS, GLONASS, Galileo, and BeiDou systems.

The system has been validated through comprehensive testing at JammerTest2022 and JammerTest2023, affirming its robustness, low interference detection latency, and superior classification capabilities. For detailed test protocols, please refer to the following links:

https://gpspatron.com/jammertest2023-test-report/

https://gpspatron.com/jammertest2022-norway/

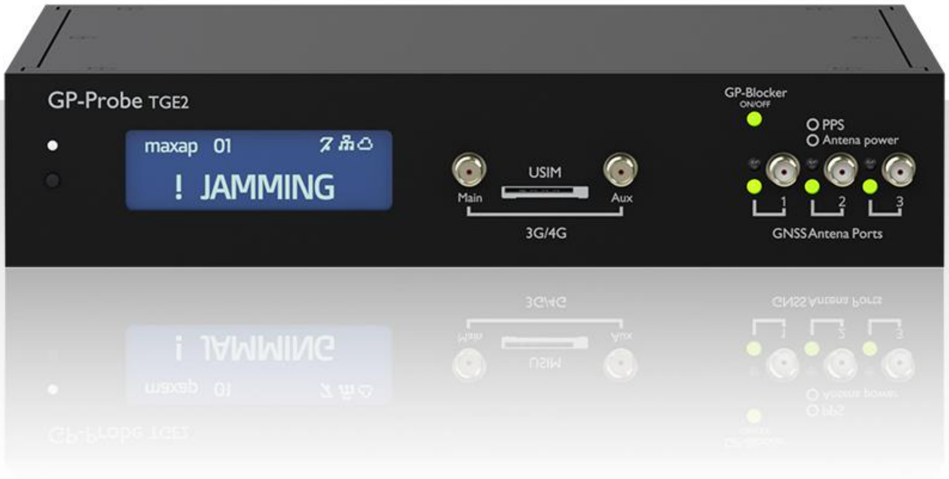
JAMMERTEST2022
NORWAY
September 19th - 23rd
Statens vegvesen
Nasjonal kommunikasjons-myndighet
FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

GP-Probe TGE2

High performance sensor for interference detection/classification/localisation

Three RF channels enable spatial signal analysis, ensuring identification of sophisticated GNSS spoofing.

The GP-Probe TGE2, operating in tandem with GP-Cloud, is a sophisticated instrument designed to safeguard critical infrastructures from GNSS disruptions. It not only detects interferences but also precisely classifies them into spoofing or jamming. The data it collects is crucial for in-depth analysis of GNSS attack techniques, enabling engineers to develop tailored mitigation solutions and enhance the robustness of essential national services.



Key Features

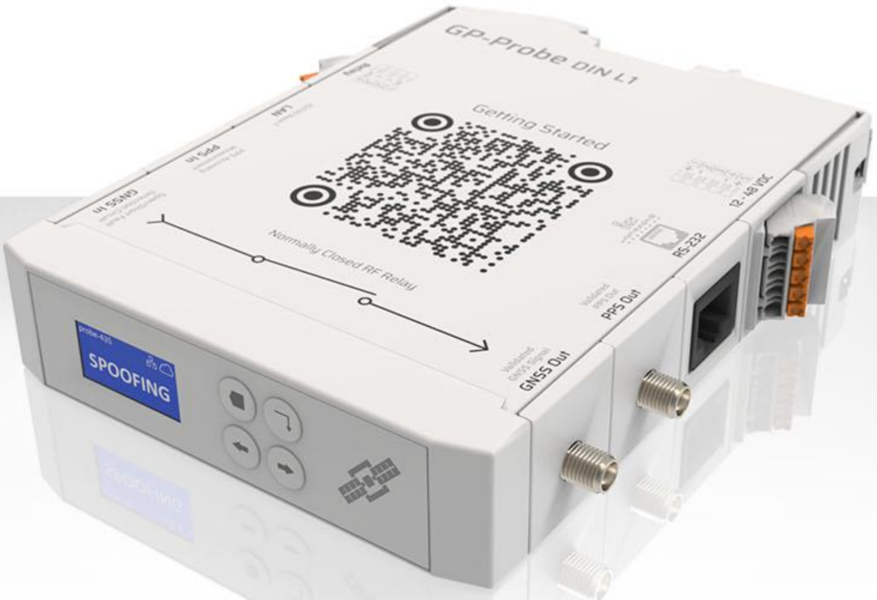
- Three RF channels enable spatial signal analysis for intentional coherent spoofing detection.
- 60 MHz real-time RF signal analyzer for spectrum monitoring, interference classification and localization with TDOA.
- PPS input for checking time server health and monitoring the entire synchronization 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 GNSS jammer suppresses the most powerful spoofing signals.
- PPS output for synchronization of external equipment.
- 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.
- Embedded Lua Scripting: Develop custom scenarios for external equipment remote control via RS232/Telnet/SNMP with the embedded LUA scripting engine.

GP-Probe DIN L1

Cost effective GNSS interference detector with PPS accuracy tracking

Designed for telecom to monitor GNSS interference and synchronization quality.

GP-Probe DIN L1 covers three primary applications: GNSS interference detection and classification, PPS accuracy monitoring, GNSS signal quality analysis, and logging. The device is easily installed between a GNSS antenna and a receiver or time server. When an event is detected, the GNSS and PPS outputs are immediately disabled, preventing any counterfeit signals from reaching your systems.



Key Features

- The combination of three functions: interference detection, PPS accuracy and signal quality monitoring makes the device perfect for ensuring reliable synchronization of 5G infrastructure.
- Onboard RF Blocker: In the event of spoofing detection or signal quality degradation, the integrated RF switch and GNSS jammer will block your GNSS receiver, ensuring high synchronization accuracy in any GNSS interference scenario.
- Embedded Lua Scripting: Develop custom scenarios for external equipment remote control via RS232/Telnet/SNMP with the embedded LUA scripting engine.
- PPS Accuracy Monitoring: GP-Probe DIN1 measures the time offset between internal and external PPS and streams the data to GP-Cloud for real-time monitoring, statistical analysis, and user notifications.
- Easy-to-Install: The device is installed and configured in minutes thanks to the DIN-compliant mounting and the integrated Web Configuration Panel

GPSPATRON

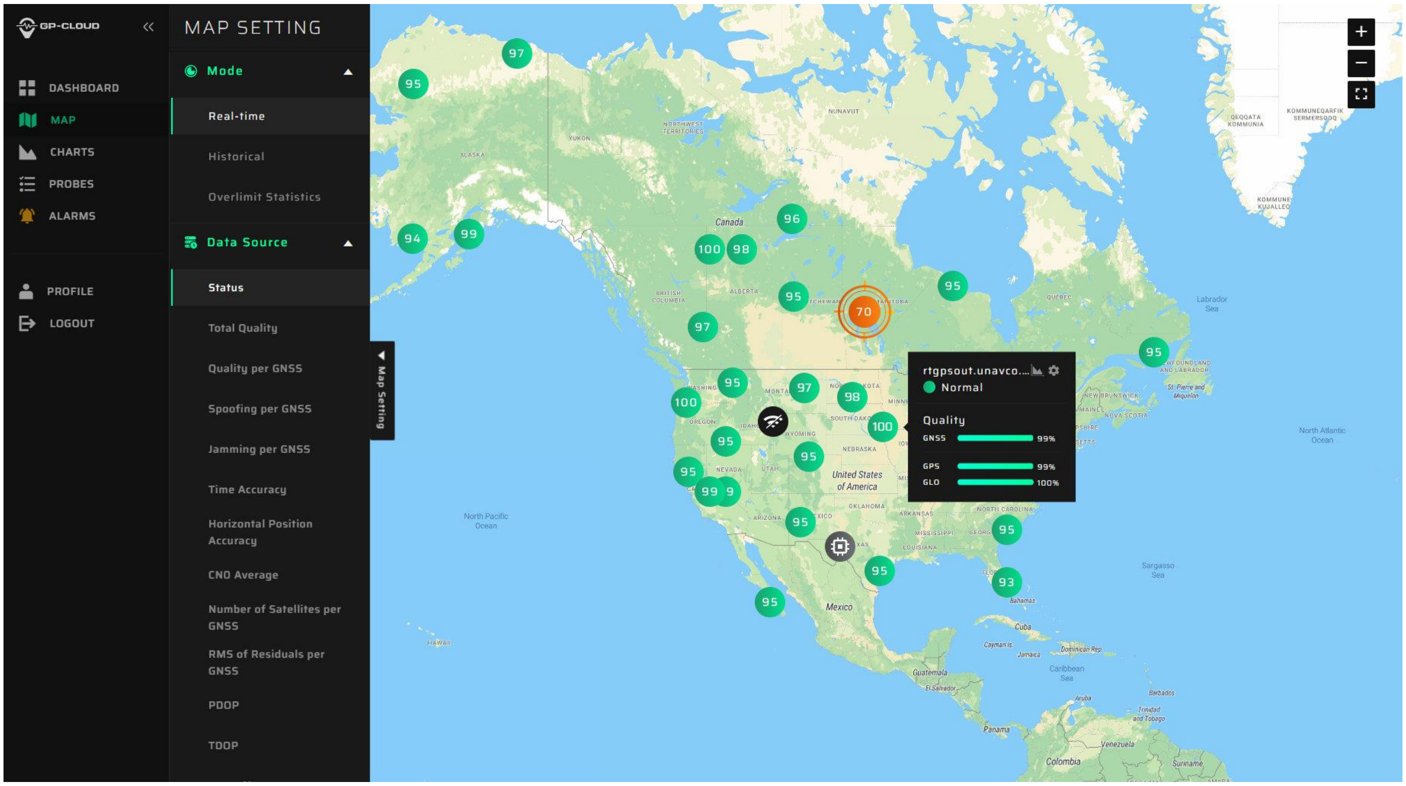
hensec
secure solutions

GP-Cloud

Web app for real-time GNSS signal quality analysis, interference detection and classification

Advanced GNSS spoofing/jamming detection, localization and logging

GP-Cloud is a comprehensive platform designed to streamline the monitoring of your GNSS infrastructure. By connecting RTK Base Stations through RTCM@NTRIP, or other GNSS receivers via NMEA@NTRIP, GP-Cloud offers real-time alerts on signal anomalies. It facilitates detailed post-event analysis to craft robust defense strategies against GNSS spoofing and jamming. With the integration of our GP-Probe, users gain a granular analysis of GNSS interference, enhancing both immediate response and long-term protective measures.



rtgpsout.unavco....

● Normal

Quality

GNSS 99%

GPS 99%

GLO 100%

Key Features

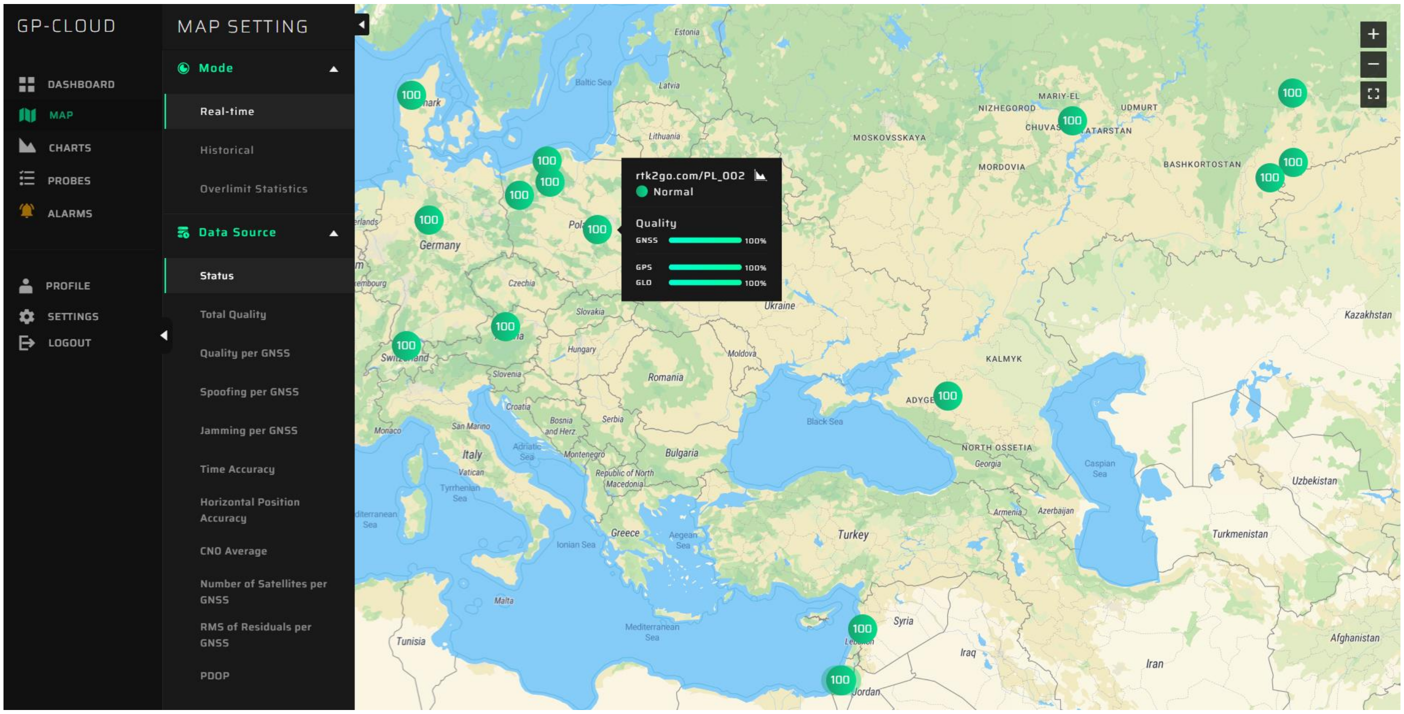
- Real-time anomaly detection in GNSS observation. Supports: RTCM, NMEA, and Septentrio SBF protocols.
- High-precision detection and classification of sophisticated spoofing attacks.
- Enterprise-Grade Application: real-time, high-load operation, scalable to nation-wide data processing.
- GNSS Quality Monitoring
- Data Logging
- Open API for seamless integration into existing infrastructure.

Info and Sales: gps@hensec.com   www.hensec.com

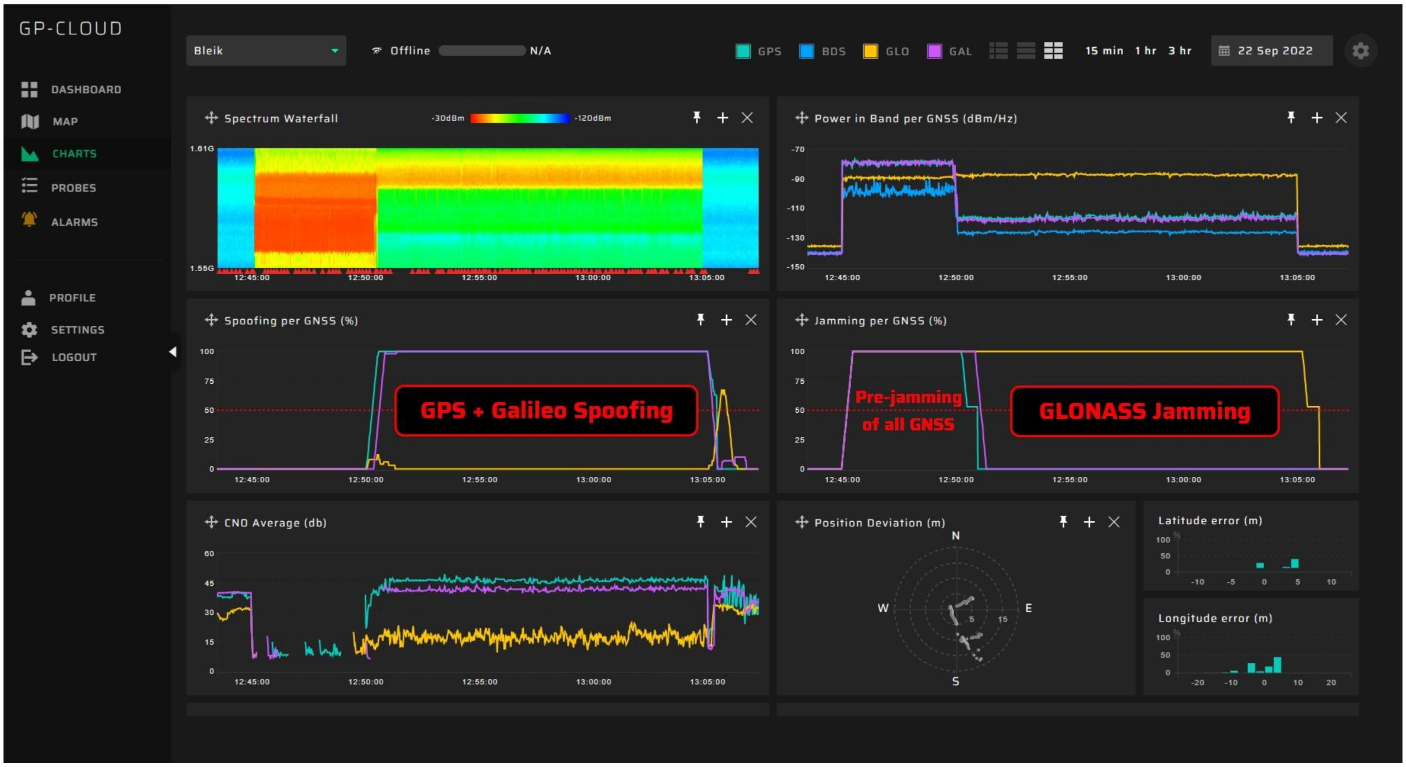
GPSPATRON

hensec
secure solutions

GP-Cloud UI: Map for Real-Time Monitoring of GNSS-Dependent Infrastructure



GP-Cloud UI: Detailed Graphs for Event Investigation

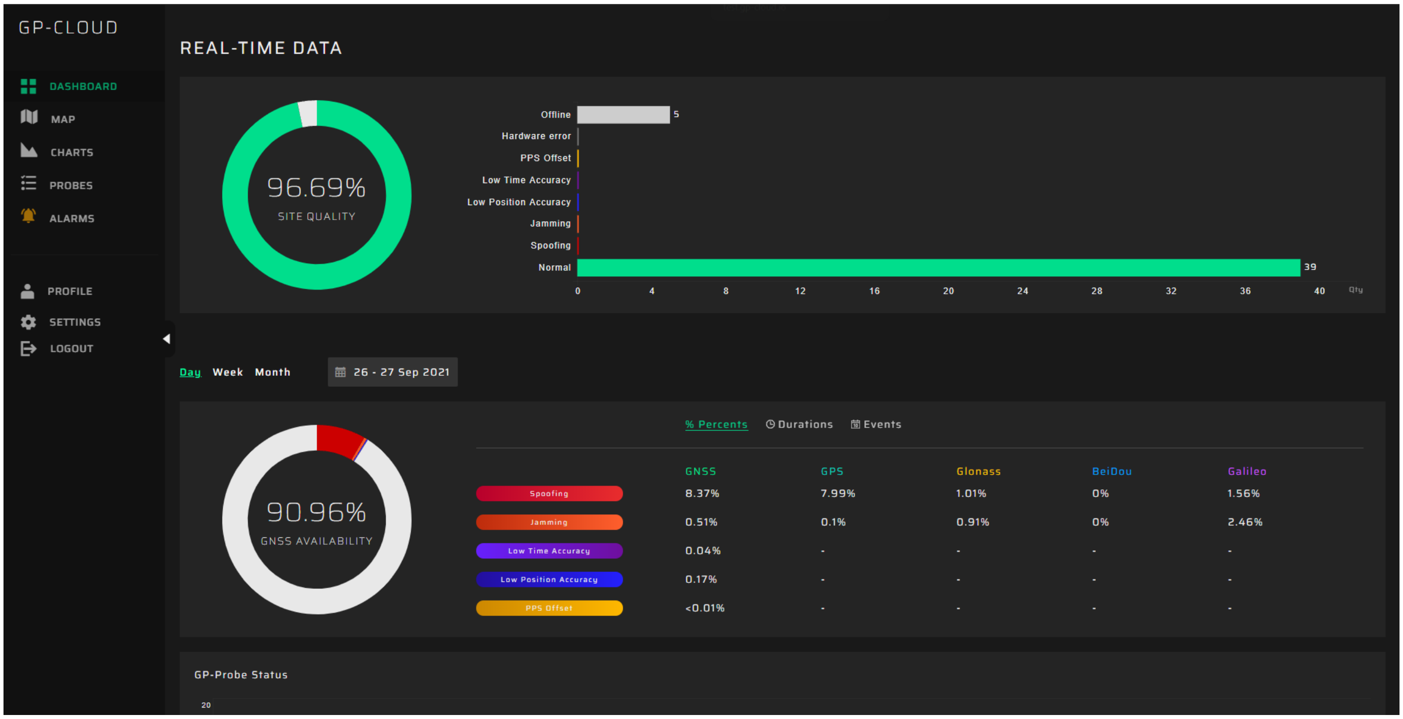


Info and Sales: gps@hensec.com   www.hensec.com

GPSPATRON

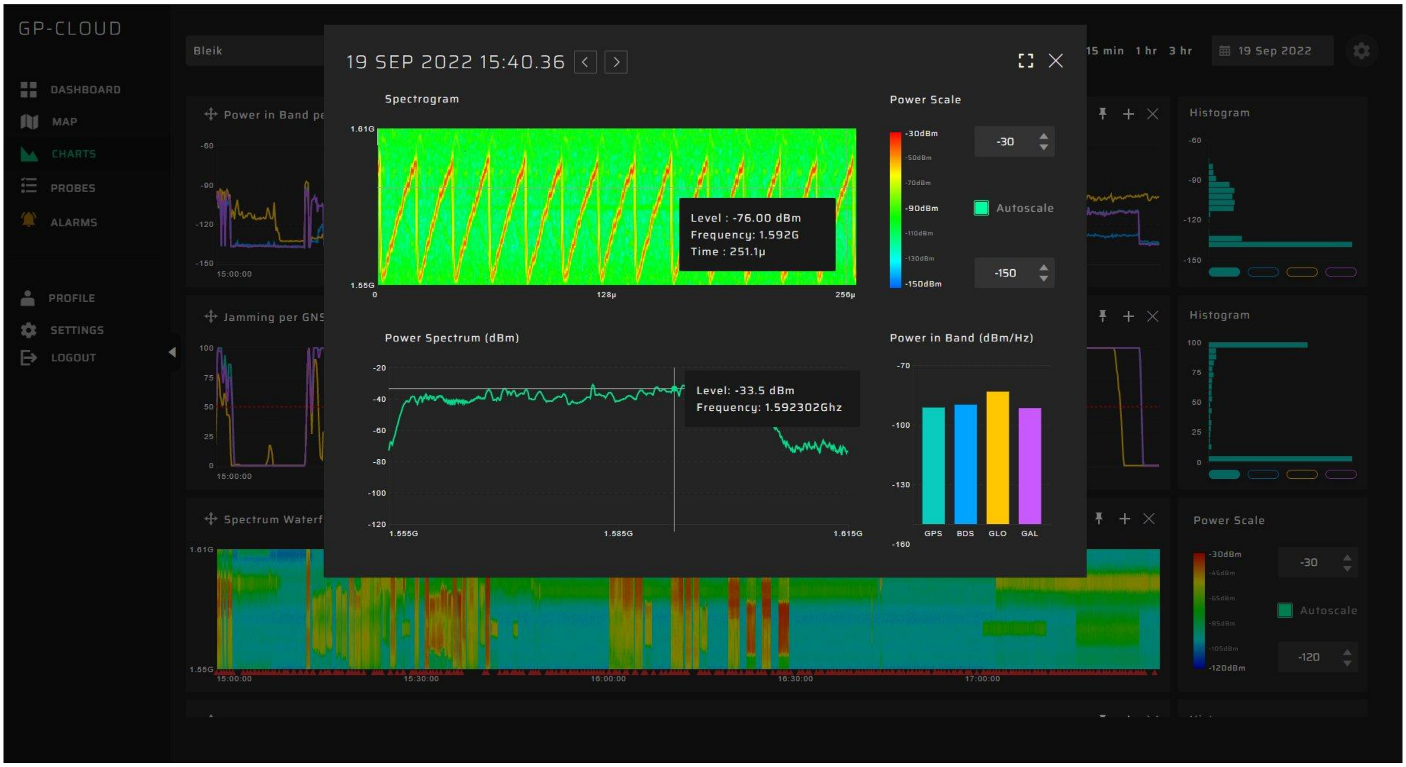
hensec
secure solutions

GP-Cloud UI: Dashboard for Real-Time Status Monitoring and Statistical Analysis



	GNSS	GPS	Glonass	BeiDou	Galileo
Spoofing	8.37%	7.99%	1.01%	0%	1.56%
Jamming	0.51%	0.1%	0.91%	0%	2.46%
Low Time Accuracy	0.04%	-	-	-	-
Low Position Accuracy	0.17%	-	-	-	-
PPS Offset	<0.01%	-	-	-	-

GP-Cloud UI: Spectrogram for In-Depth Interference Analysis



Info and Sales: gps@hensec.com www.hensec.com

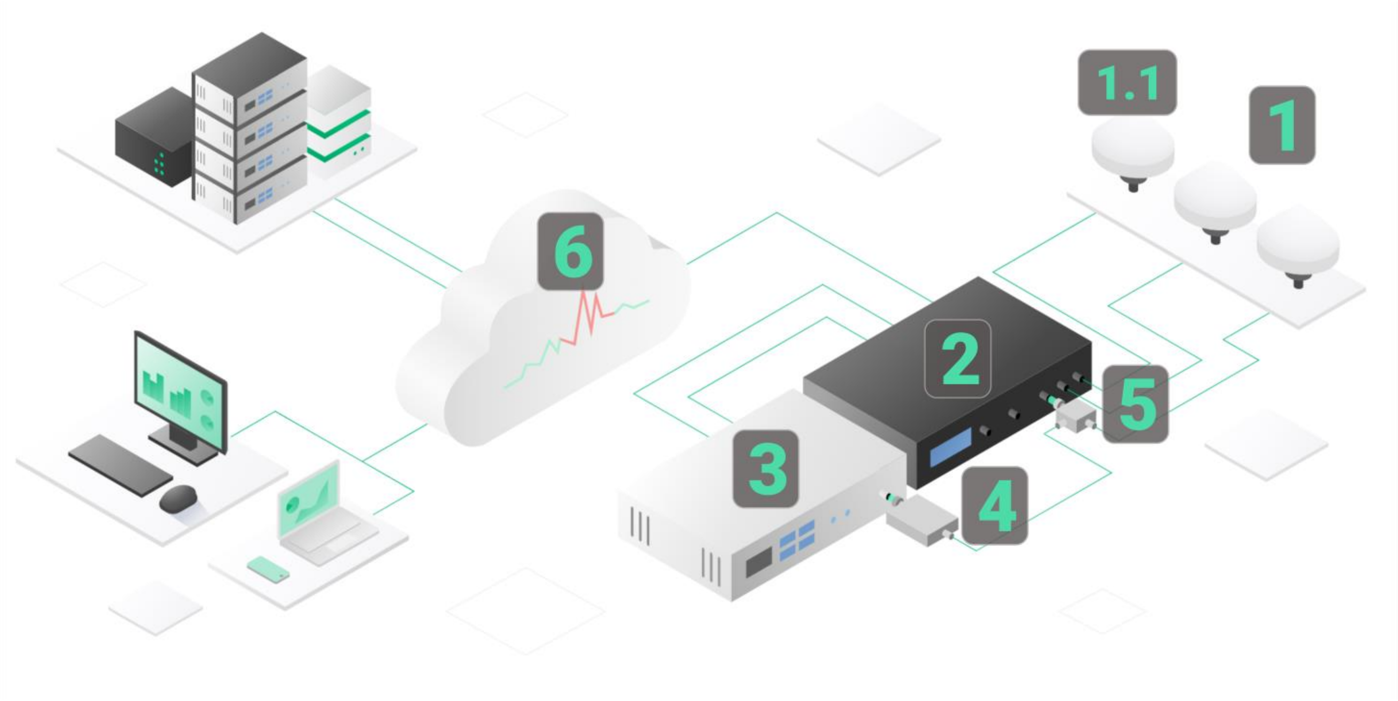
GPSPATRON

hensec secure solutions

Case Study: Defending Time Servers

In sectors where precision timing is non-negotiable, uninterrupted system functionality depends on unerring time signals. At GPSPATRON, we've tailored a product integration framework specifically for such high-stakes environments. The GP-Probe TGE2, coupled with GP-Cloud, forms the market's most reliable defense mechanism against GNSS spoofing, having been rigorously tested during JammerTest2022 and 2023. The addition of GP-Blocker provides a robust countermeasure capable of suppressing even the most potent spoofing signals, including those from military sources, safeguarding the precision and security of time servers.

Interference/anomaly detection latency < 3 sec



1. **Three-Channel Antenna System**: Ensures advanced coherent spoofing attack detection through spatial signal analysis.
2. **GP-Probe TGE2**: Measures GNSS signal parameters, assesses the PPS signal phase accuracy of the time server, and sends raw data to GP-Cloud.
3. **Protected Time Server**: Connects to the antenna via GP-Blocker and GP-Divider. If GP-Cloud detects spoofing/anomaly/interference/signal degradation, GP-Blocker disconnects the GNSS antenna, triggering the time server to switch to holdover mode, maintaining precise time.
4. **GP-Blocker**: An RF switch with 110 dB of isolation. It includes an L-band GNSS jammer for additional suppression of fake signals when isolation alone is insufficient.
5. **GP-Divider**: A 2-way GNSS splitter that allows one GNSS antenna to be shared between two receivers.
6. **GP-Cloud**: Monitors GNSS-dependent infrastructure, detecting and classifying anomalies in GNSS observations.

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/