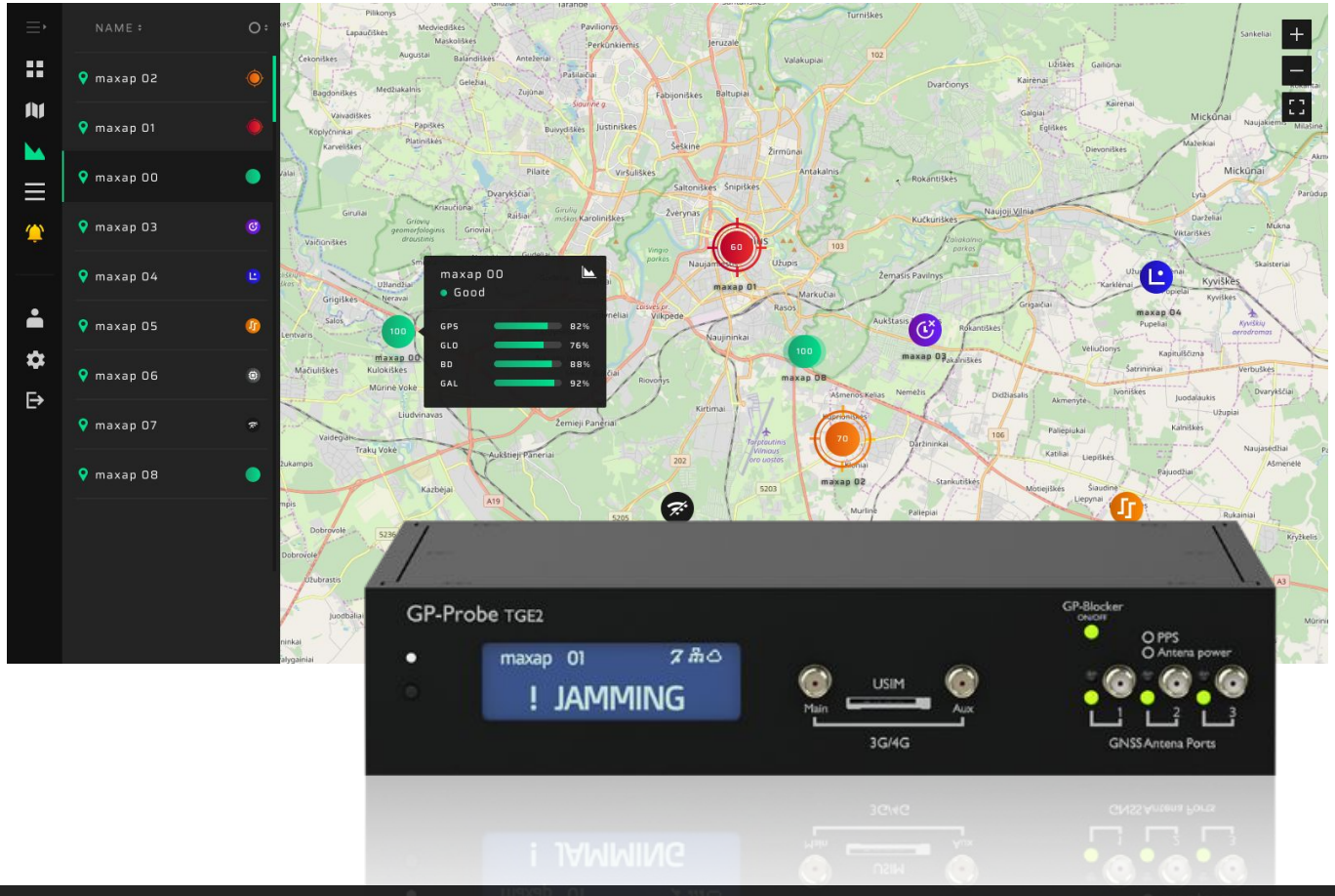
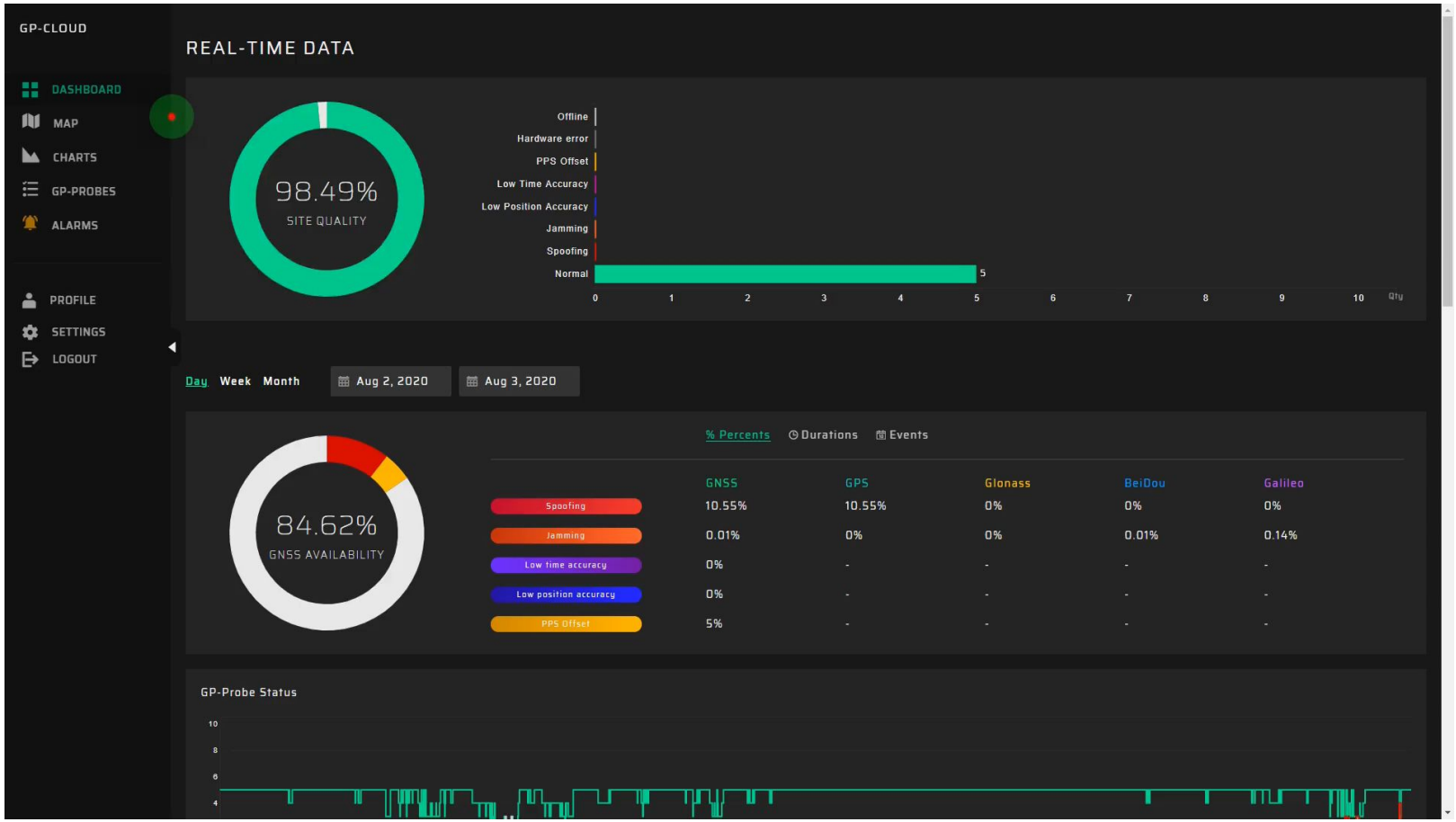


GPSPATRON

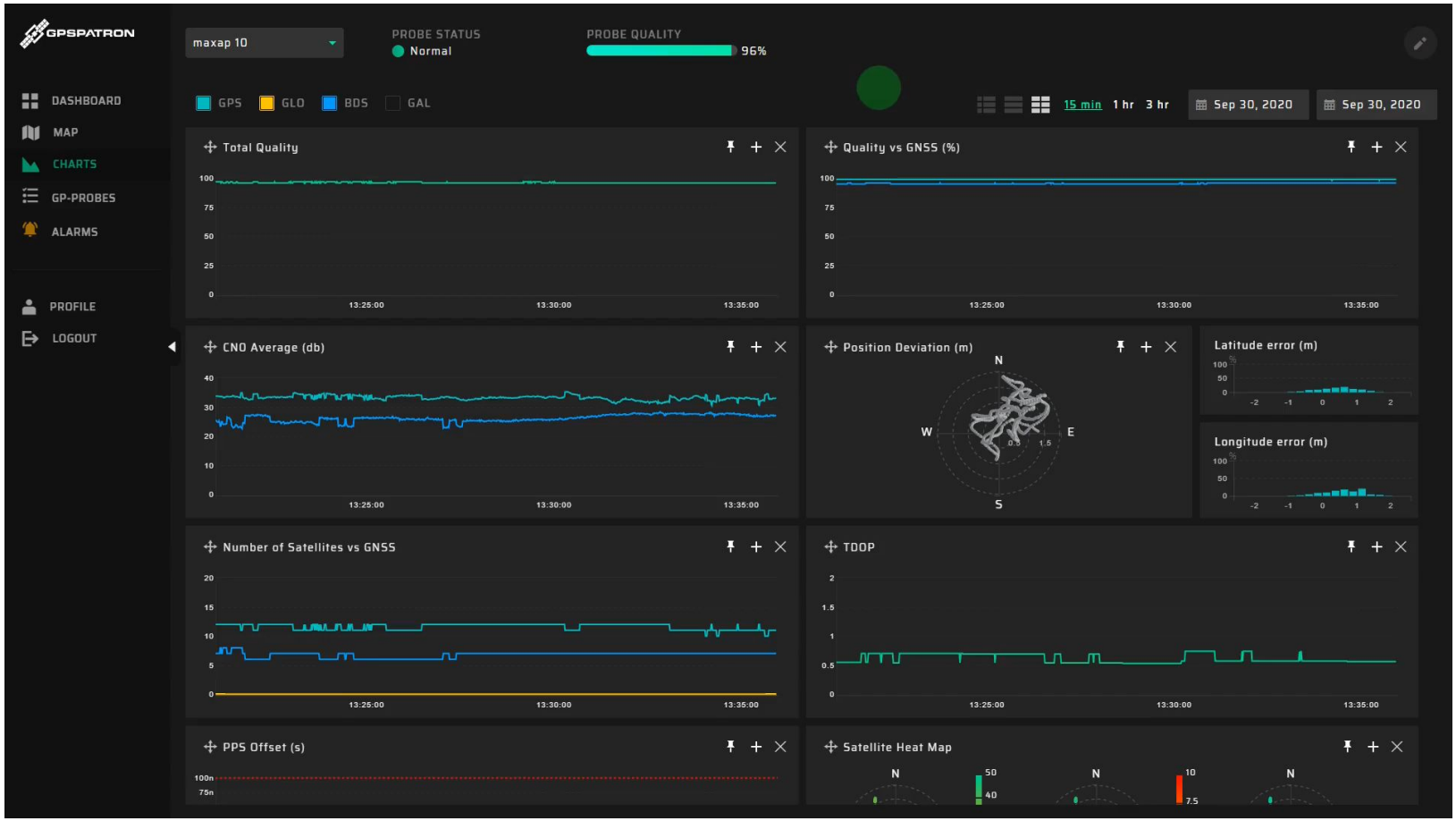
Top Advantages

Detection of all GNSS spoofing patterns



With three-channel GP-Probe TGE2 and cloud-based anomaly detection algorithms, the system estimates the spatial characteristics of GNSS signals. This ensures reliable detection of all types of deliberate spoofing attacks: asynchronous, synchronous, synchronous with multiple TX, meaconing. Users can utilize any GNSS antennas installed in any geometric configuration

GNSS Signal Quality Monitoring & Logging with Advanced UI



Every second, the GP-Probe measures many parameters of radio signals of all visible satellites: PR, CP, LockTime, Doppler, PR residual, CN0, etc. The GP-Cloud processes in real-time the data and estimates the quality/accuracy, and stores all results in the database.

There are 19 charts for a detailed analysis of GNSS signals parameters. Zoom and synchronous cursor enable the user to estimate the signals' parameters in real-time and investigate what happened in the past.

GNSS Interference Analysis

The GP-Probe TGE2 has an embedded RF signal analyzer with 60MHz real-time bandwidth and low noise figure < 3 dB. Every second, the signal analyzer acquires RF data and calculates power in band, power spectrum, and spectrogram for the most powerful events.

All data is stored in a database for further analysis and classification of interference.

Com!nt the system integrator

Feature #1. Low Latency Spoofing Detection Algorithms

1. In the case of a time server, you have **only 15 seconds** to respond to non-coherent spoofing. You can disconnect GNSS antenna port and the time server will switch to holdover. Or you can send a command to embedded GNSS receiver to switch to a clear constellation.

2. GP-Cloud analyzes RAW GNSS data from a three-channel GP-Probe in real-time. In the case of spoofing detection, the cloud sends an instant notification to the probe. The probe can disable the GNSS antenna port with a GP-Blocker or send a custom command to the time server.

3. The total delay from the start of an attack to the cut-off of the GNSS antenna port does not exceed

3 seconds

4. If you are analyzing GNSS receiver derived data such as coordinates, PPS phase, timestamp, etc. you can only detect spoofing after it has already reduced your time server's accuracy

Com!nt the system integrator

Feature #2. GP-Cloud – Enterprise-Grade Web App

1. The application is available with two types of licenses: **cloud-based and self-hosted**. This means that the customer can use the software as a service in our cloud or deploy it on his own servers.
2. The application is developed on the .NET core. Therefore, it can be hosted on both Windows and Linux.

"Enterprise-grade" means that the software is able to work reliably under high loads in the 24\365 mode. For this purpose, we use the following methodologies and technologies:

- Active-active application clustering.

We can provide unlimited application licenses for the required instances. The clustering of multiple active application servers maximizes resilience and uptime as the number of connected GP-Probes increases.

- Database clustering enables load sharing between unlimited database nodes.
- The Web API specification is available in Swagger.
- RabbitMQ can be used to set up instant notifications.

And finally, our UI is the best on the market :-)

ComInt the system integrator

Feature #3. GPSPATRON is Commercial read and Validated

The solution has been tested in both laboratory and live-sky environments under military-scale, multi-constellation GNSS spoofing and jamming:

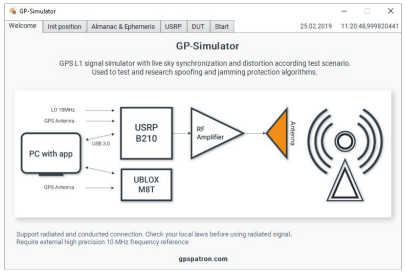
1. The system has been tested during JammerTest2022\2023 and showed excellent results in detection performance and classification accuracy.
   https://gpspatron.com/jammertest2023-test-report/

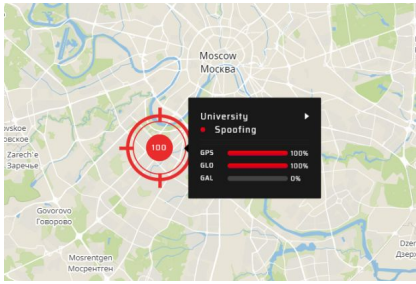
2. We have tested the solution with all available open-source GNSS simulation projects from GitHub

3. We tested our solution using commercially available gnss simulators

4. We have developed our GPS spoofer and tested the solution under various attack scenarios, both on cable and over the air

5. We have deployed three test zones in regions with the highest density of electronic weapons. Our system detects significant spoofing incidents every day!





Feature #4. Extensive Integration Capabilities

Three system integration methods to support the client's multivendor infrastructure:

1. WEB API

Web API is the best way to integrate GPSPATRON into the customer's existing synchronization management system. You can request information about the current state of GP-Probes, as well as historical data

2. GP-Probe LUA Automation Scripts

With the Lua scripting engine built into GP-Probe, users can create a custom script to respond to events. When the probe receives a notification from the cloud, it launches a user's LUA script. Lua scripting engine supports RS232, RS485, Ethernet, Telnet, and SNMP

3. GP-Blocker

All time servers are equipped with a high-stable local oscillator to provide an accurate clock if PTP or GNSS signals are unavailable. Therefore, the simplest way to protect against GNSS spoofing is to disable the GNSS antenna port and switch the time server to HoldOver mode.

GP-Blocker RF signal isolation level reaches 110dB. In combination with a built-in noise source, GP-Blocker suppresses the most powerful military-scale spoofing signals

We cover all needs: with advanced GP-Probe TGE2 and low-cost GP-Probe DIN L1

- Three RF channels enable spatial signal analysis to ensure detection of all sophisticated GNSS spoofing attack scenarios.
- Operates **only** in combination with GP-Cloud
- PPS input for the external time server health checking.
- High-end 60 MHz real-time RF signal analyzer for spectrum monitoring, interference classification and localization with TDOA.
- Form factor: 19-inch rack, half-size.
- Double power module: 110 – 220 AC, 18 – 75 DC.
- 4G modem and 100BASE-TX LAN Port

- One RF channel. Can detect anomalies in GNSS data caused by spoofing or jamming.
- Can operate in combination with GP-Cloud or completely independently with OSP
- Embedded RF blocker and GNSS output
- PPS input for the external time server health checking.
- Basic 60 MHz real-time RF signal analyzer for spectrum monitoring.
- Form factor: DIN rail mounted.
- Power module: 12-48 VDC.

IP67 Rated Protective Case and Enclosure for Outdoor use
of GP-Probe TGE2

We offer two products for using the GP-Probe TGE2 in harsh environments:

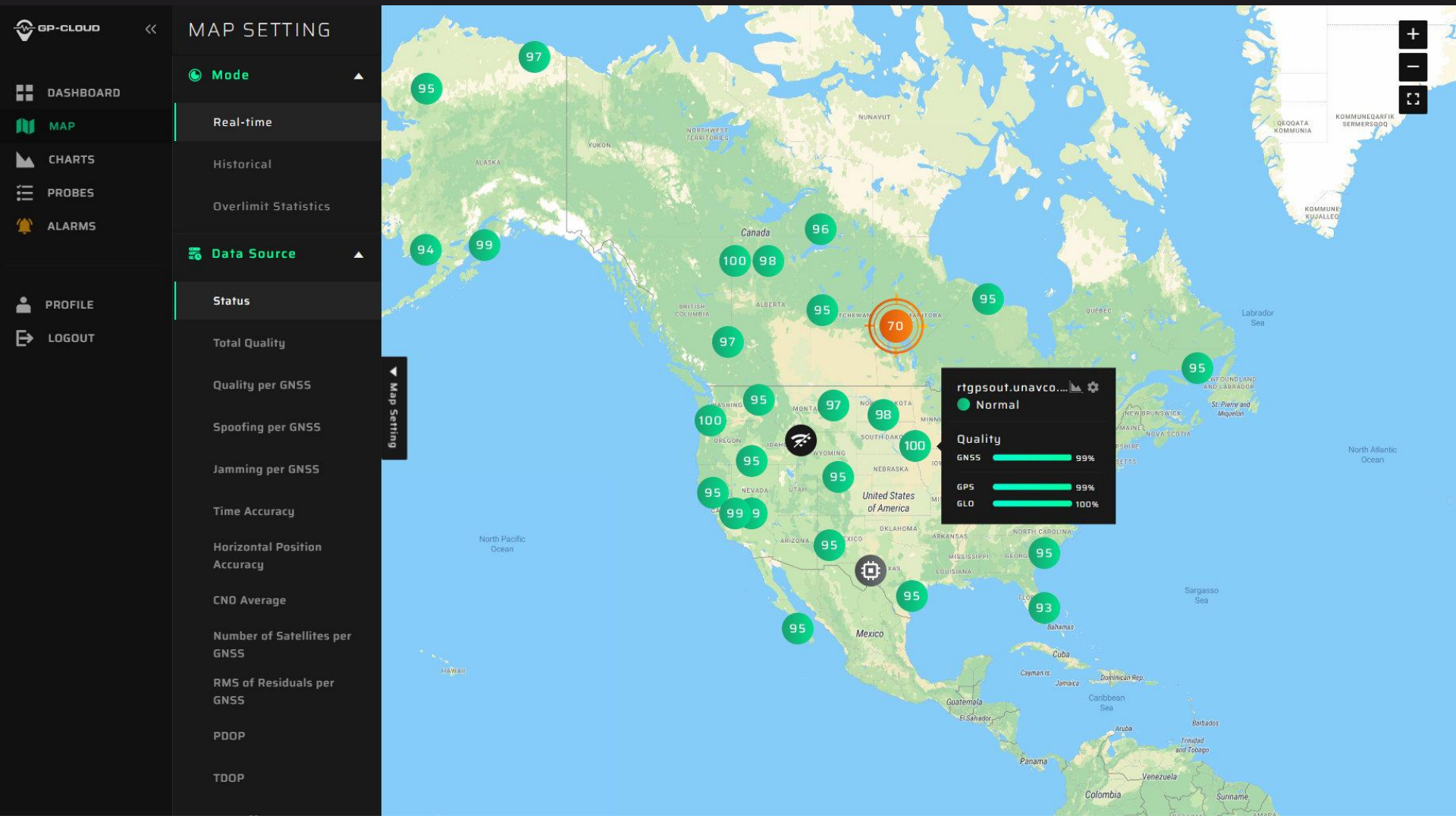
GP-Probe Case for TGE2

An IP67-rated protective case designed for outdoor use of the GP-Probe TGE2. It features a built-in LiPo battery, providing water and dust resistance, true shock protection, and a wide operational temperature range, ensuring reliable performance in challenging conditions.

GP-Probe BOX for TGE2

An IP66-rated protective enclosure guarantees reliable operation in extreme conditions with its high-quality stainless steel body and built-in automated heating module. It is easy to mount on walls or poles, making it a versatile solution for various outdoor installations.

GP-Cloud: Versatile Support for Any GNSS Receivers



GP-Cloud is designed to work seamlessly not only with our devices but also with any GNSS receivers or reference stations. It supports a wide range of protocols, ensuring compatibility and flexibility for diverse applications. Whether you're using our equipment or integrating third-party solutions, GP-Cloud provides a reliable and adaptable platform for your GNSS needs.

Feature #5. GPSPATRON Supports All Constellations

The cloud estimates the probability of spoofing and jamming for each system individually. Therefore, when spoofing the GPS, your equipment can be switched to clear constellation using a custom command.

ComInt the system integrator