GNSS Spoofing Detektion

Sensoren

Produktinformationen

Die Sensoren GP-Probe DIN-L1 und TGE2 sind GNSS Interferenz Detektoren. Mit dem integrierten RF Signal Analyzer detektieren, klassifizieren und lokalisieren sie GNSS Spoofing und Jamming.

Die GP-Probe TGE2 kann mit ihren 3 HF Kanälen mittels spatial signal analysis auch fortschrittliche Spoofing Angriffe zuverlässig erkennen.

Die GP-Probe DIN-L1 ist die kostengünstige, leicht integrierbare Hutschienen-Version. Es ist auf das L1 Band begrenzt und enthält einen eingebautem RF Blocker und Jammer zum Unterbrechen des GNSS Signals im Falle erkannten Spoofings.

Anwendung

Die Sensoren benötigen minimal den Anschluss einer externen GPS-Antenne (im Lieferumfang) sowie der Spannungsversorgung. Die Konfiguration erfolgt einfach über das Webinterface – entweder lokal oder über die GP-Cloud.

Die empfangenen HF Parameter werden onboard verarbeitet, ausgewertet und ggf. ebenfalls via Netzwerk zur GP-Cloud übertragen. Die Alarmierung erfolgt in Echtzeit lokal und in der Cloud.

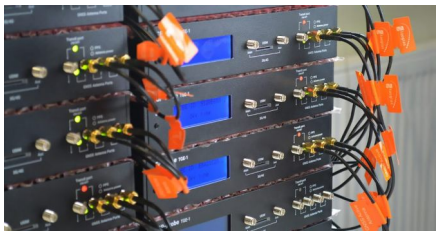
Features

- Spoofing Detektion, Jamming Detektion, Signalqualität
- Unterschiedliche Versionen – Für Desktop, halb 19“, Hutschiene, Rugged Case oder als Outdoor Headless Box
- Eingebauter RF Blocker – zum Schutz nachgeschalteter Empfänger bei erkanntem Spoofing
- Eingebaute Relais mit potentialfreien Kontakten
- Onboard Scripting – auf den Geräten selbst lassen sich via LUA Scripting eigene Abläufe programmieren
- Security by Design – non-Linux realtime OS for 24/7/365 Betrieb
- Leichte Installation, flexible Einsatzszenarien
- Unterstützte GNSS – GPS L1 C/A, QZSS L1 C/A L1S, GLONASS L1OF, BeiDou B1I/B1C, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN

Einsatzbereiche

Vielseitig im Einsatz: Qualitätskontrolle d. GNSS Signals, Früherkennung von Spoofing, Schutz von Schifffahrt, Zeitservern, Mobilfunkstationen, Kopfstationen, Industriestandorten, Rechenzentren, Kritischen Infrastrukturen, Regierungseinrichtungen, Flughäfen und anderen sensiblen Bereichen.

Weitere Informationen und Vertrieb: gnss@hensec.com https://www.hensec.com/ https://gpspatron.com/



hensec
Geschäftsführer: Kevin Heneka

Luisenstr. 56
76689 Karlsdorf-Neuthard

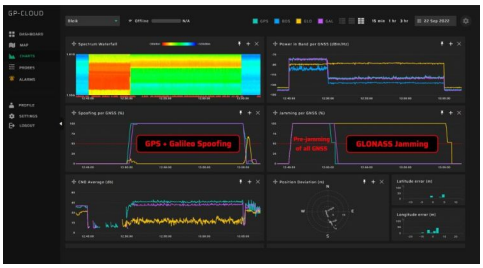
E-Mail: info@hensec.com
Web: www.hensec.com

Tel.: +49(0)7251-9238750
Fax: +49(0)7251-9238751

GNSS Spoofing Detektion

Software

Produktinformationen



Die GP-Cloud ist eine Webanwendung zur GPS / GNSS Signalanalyse, Interferenz Detektion und Klassifikation. Sie bietet eine fortschrittliche GNSS Spoofing und Jamming Detektion in Echtzeit, das Loggen von Ereignissen sowie das Lokalisieren der Störquellen.

Jamming, Spoofing und Fehler werden in Echtzeit erkannt, ausgewertet und entsprechende Alarme oder Benachrichtigungen ausgegeben. Ebenso ist eine nachträgliche Auswertung der gespeicherten Ereignisse möglich.
Unsere GP-Cloud Server befinden sich in der EU. Die Installation ist ebenso On-Prem möglich.

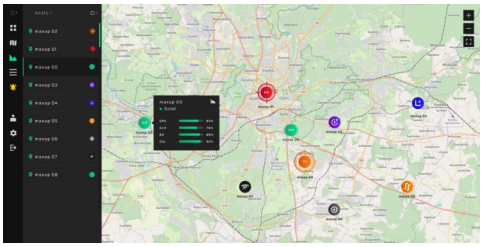
Anwendung

Unsere GNSS-Spoofing Sensoren werden einfach über einen API Key in das System eingebunden. Auch können vorhandene RTK BS (via RTCM@NTRIP) oder andere GNSS Empfänger (via NMEA@NTRIP) mit der GP-Cloud verbunden werden. Die Einbindung von weiteren Datenquellen (z.B. ADSB) ist ebenso möglich.

Die Webanwendung sammelt alle Daten und bereitet sie in übersichtliche Informationen auf. Hier lassen sich Benutzer in entsprechenden Berechtigungen anlegen, Alarme und Grenzwerte konfigurieren und die eigenen Sensoren verwalten.

Fragen Sie uns nach einem Demo-Zugang: gnss@hensec.com

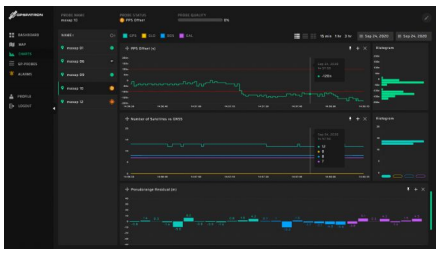
Features

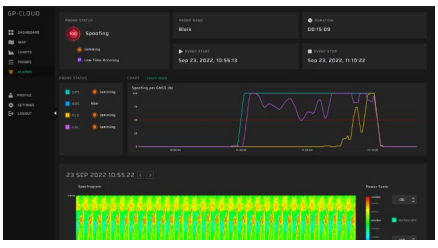


- GNSS Anomalie Detection – Spoofing, Jamming, Interference, …
- GNSS Interference Classification
- GNSS Qualitätskontrolle
- Data Logging – viele Parameter wie doppler, position, accuracy, ...
- API – mächtige API ermöglicht Einbindung in eigene Anwendungen
- Unterstytzte Systeme – GPS, GLONASS, Galileo, BeiDou
- Erkanntes Spoofing – Aynchrones, Synchrones, Multi-TX, Jamming
- Ansichten – Dashboard, Sensorkarte, Diagramme, Histogramme, Sensorliste, User

Einsatzbereiche

Vielseitig im Einsatz: Qualitätskontrolle d. GNSS Signals, Früherkennung von Spoofing, Schutz von Schifffahrt, Mobilfunkstationen, Kopfstationen, Industriestandorten, Rechenzentren, Kritischen Infrastrukturen, Regierungseinrichtungen, Flughäfen und anderen sensiblen Bereichen.





Weitere Informationen und Vertrieb: gnss@hensec.com
https://www.hensec.com/ https://gpspatron.com/gp-cloud/

hensec
Geschäftsführer: Kevin Heneka
Luisenstr. 56
76689 Karlsdorf-Neuthard
E-Mail: info@hensec.com
Web: www.hensec.com
Tel.: +49(0)7251-9238750
Fax: +49(0)7251-9238751