



Anomaly Detection in Raw GNSS Data

Critical infrastructure protection against GNSS spoofing

Maksim Barodzka

CEO @ GPSPATRON

www.gpspatron.com

www.youtube.com/c/GPSPATRON

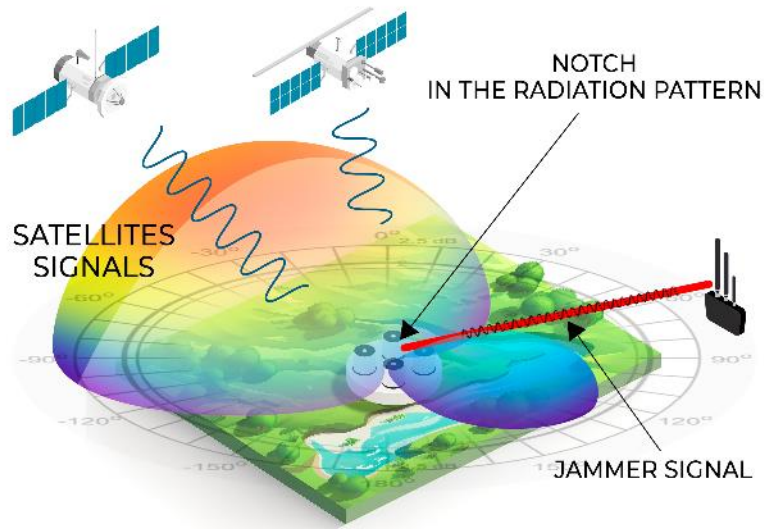
twitter.com/gpspatron

Techniques to protect a GNSS receiver from spoofing

Sophisticated Antenna Systems

Null Steering

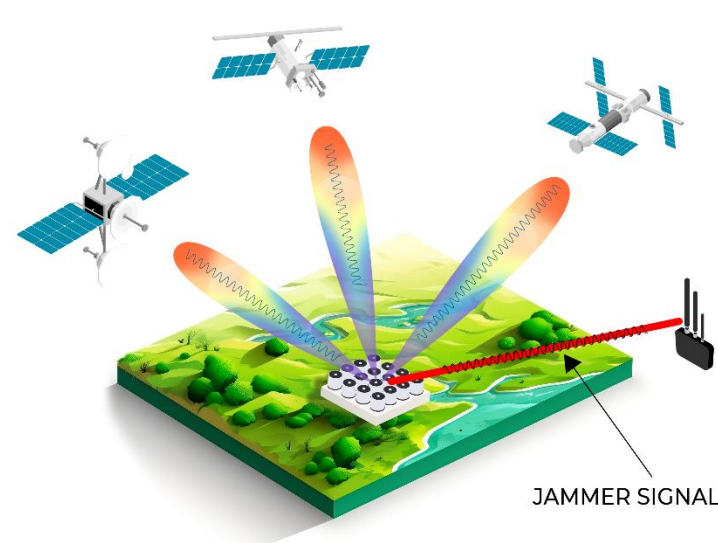
It creates "dead zones" to block fake signals.



- Real efficiency starts at 4 antenna elements.
- 40-60 dB interference suppression level.
- Effective against jamming and partially against spoofing

Beamforming

It strengthens authentic signals and weakens fake ones, making real signals clear.

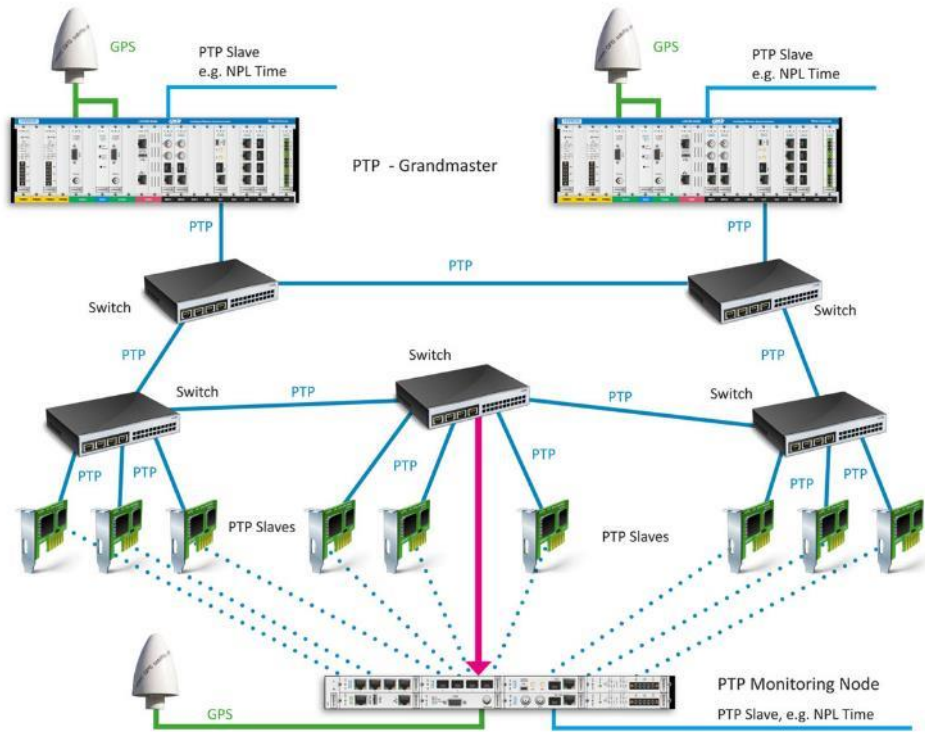


- Requires 8-16 antenna elements.
- High cost, large size and power consumption
- Acceptable technique to counteract low-power GNSS spoofing

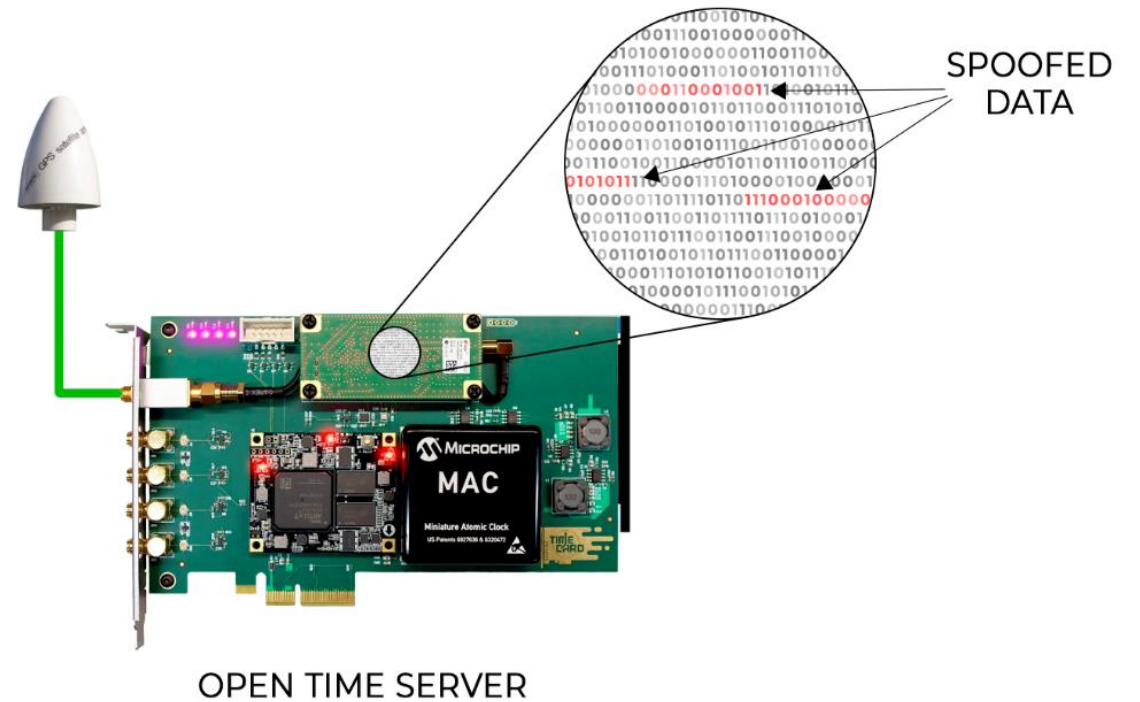
Techniques to protect a GNSS receiver from spoofing

Detect & Switch to Backup

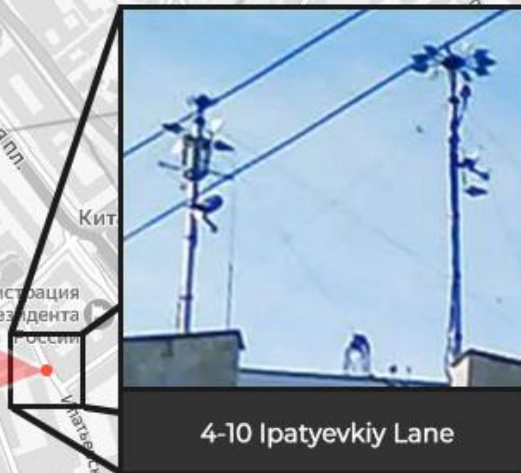
Synchronization systems with Grandmaster cross monitoring



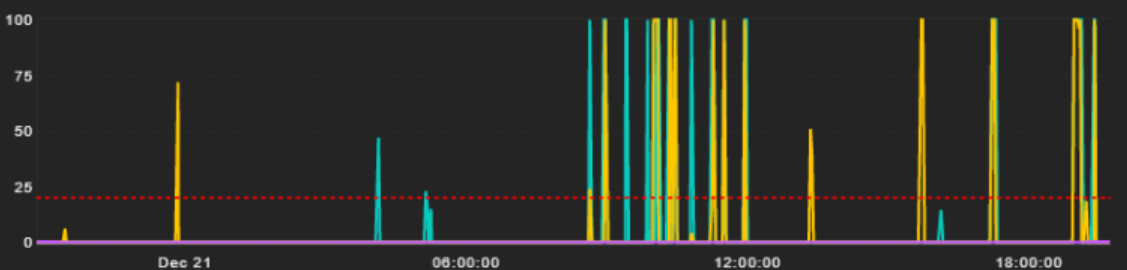
RAW GNSS data monitoring



GNSS spoofing in anti-drone systems



Spoofting vs GNSS (%)



GNSS interference in 2023

GPSJAM

Daily maps of GPS interference

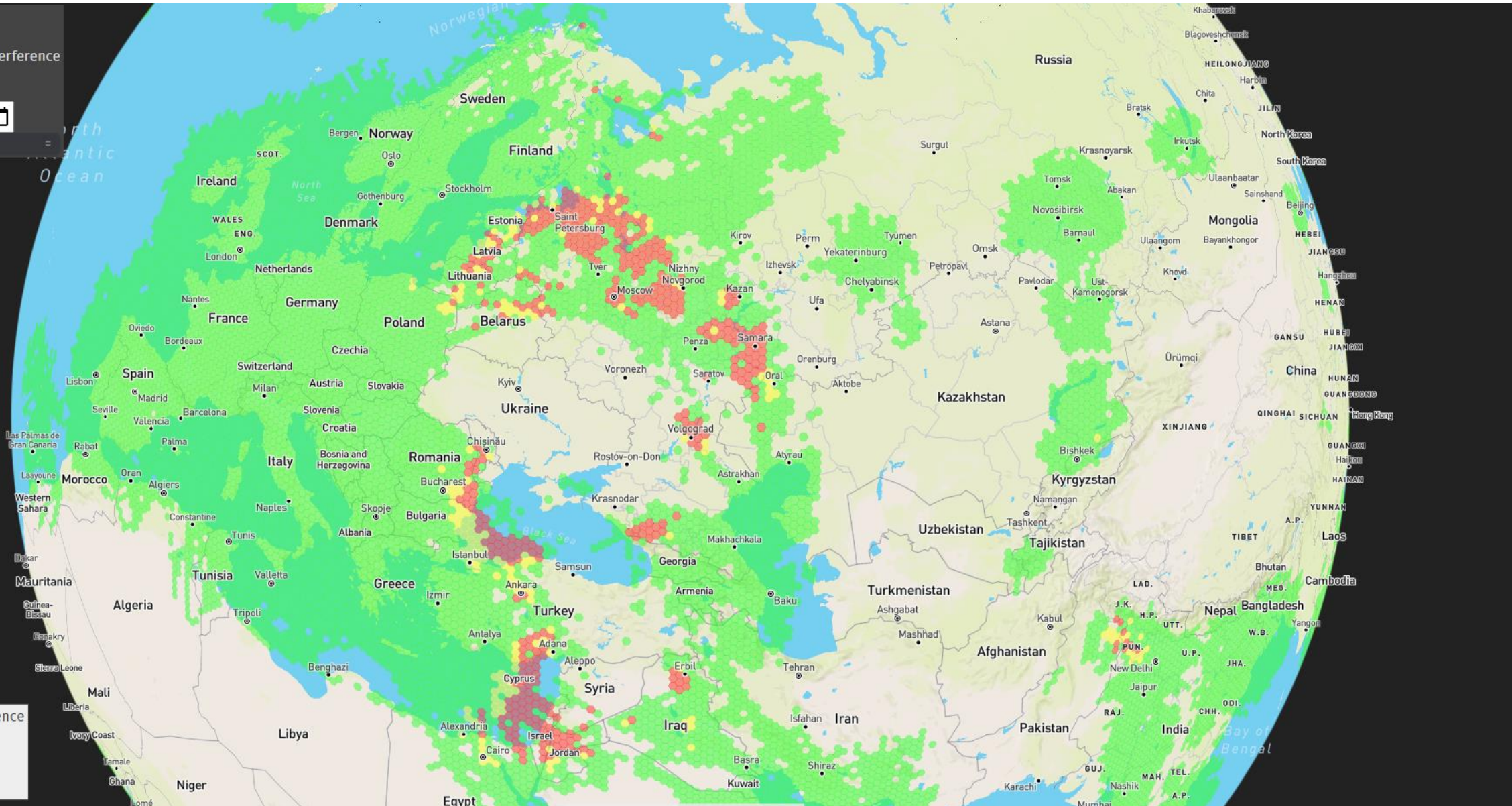
[About](#) | [FAQ](#)

10/22/2023

More

Level of GPS interference

- Low 0-2%
- Medium 2-10%
- High > 10%









Source: gpsjam.org

GNSS spoofing on vessels to avoid sanctions

nytimes.com/interactive/2023/05/30/world/asia/russia-oil-ships-sanctions.html

Tankers that The Times found spoofing since December

Satellite images revealed the true locations of spoofing ships, which shared similar traits like age, ownership and insurer.

<p>Alma - IMO: 9235892*</p> <p>Age: 20 years old Owned: Irish company Insured: American Club Cargo: Crude oil</p> <p>Spoofed location: Sea of Japan Found location: Kozmino oil terminal, Russia</p>		<p>Cathay Phoenix - IMO: 9249324</p> <p>Age: 22 years old Owned: Hong Kong company Insured: American Club Cargo: Crude oil</p> <p>Spoofed location: Near Niigata, Japan Found location: Kozmino oil terminal, Russia</p>	
<p>Eternal Peace - IMO: 9259745</p> <p>Age: 19 years old Owned: Hong Kong company Insured: American Club Cargo: Crude oil</p> <p>Spoofed location: Near Niigata, Japan Found location: Kozmino oil terminal, Russia</p>		<p>Ginza - IMO: 9220926</p> <p>Age: 22 years old Owned: Hong Kong company Insured: American Club Cargo: Unknown</p> <p>Spoofed location: Near Varna, Bulgaria Found location: Taman, Russia</p>	
<p>Lady Ella - IMO: 9252436</p> <p>Age: 20 years old Owned: Hong Kong company Insured: American Club Cargo: Unknown</p> <p>Spoofed location: Niigata Port, Japan Found location: Near Kozmino, Russia</p>		<p>Snow Lotus - IMO: 9259733</p> <p>Age: 19 years old Owned: Hong Kong company Insured: American Club Cargo: Unknown</p> <p>Spoofed location: Near Niigata, Japan Found location: Near Kozmino, Russia</p>	



GNSS jamming/spoofing on vessels



GNSS jamming/spoofing on vessels



Why is spoofing trending right now?

\$319.95



HackRF One Software Defined Radio (SDR) & ANT500 Antenna Bundle

★★★★★ ⌵ 29

\$319⁹⁵

\$198.50



ANALOG DEVICES ADALM-Pluto SDR Software Defined Radio Active Learning Module PlutoSDR

★★★★★ ⌵ 9

\$198⁵⁰

\$346.29



LimeSDR Flexible, Next-generation, Open Source Software Defined Radio USB 3.0 100 kHz - 3.8 GHz

★★★★★ ⌵ 523

\$346²⁹

\$480



bladeRF 2.0 micro xA4, 47MHz to 6GHz frequency range, 61.44MHz sampling rate, 2x2 MIMO channels USB 3.0 SuperSpeed Software Defined Radio.

★★★★★ ⌵ 17

\$480

680 Forks on GitHub for GPS Signal Simulation

[gym487/GPS-SDR-SIM-realtime](#)

Supports IQ data generation to the port for real-time playback via [GNU Radio](#)

[osqzss/bladeGPS](#)

Real-time signal generation with [bladeRF](#)

[osqzss/LimeGPS](#)

Real-time signal generation with [LimeSDR](#)

[Microtronics/PLUTO-GPS-SIM](#)

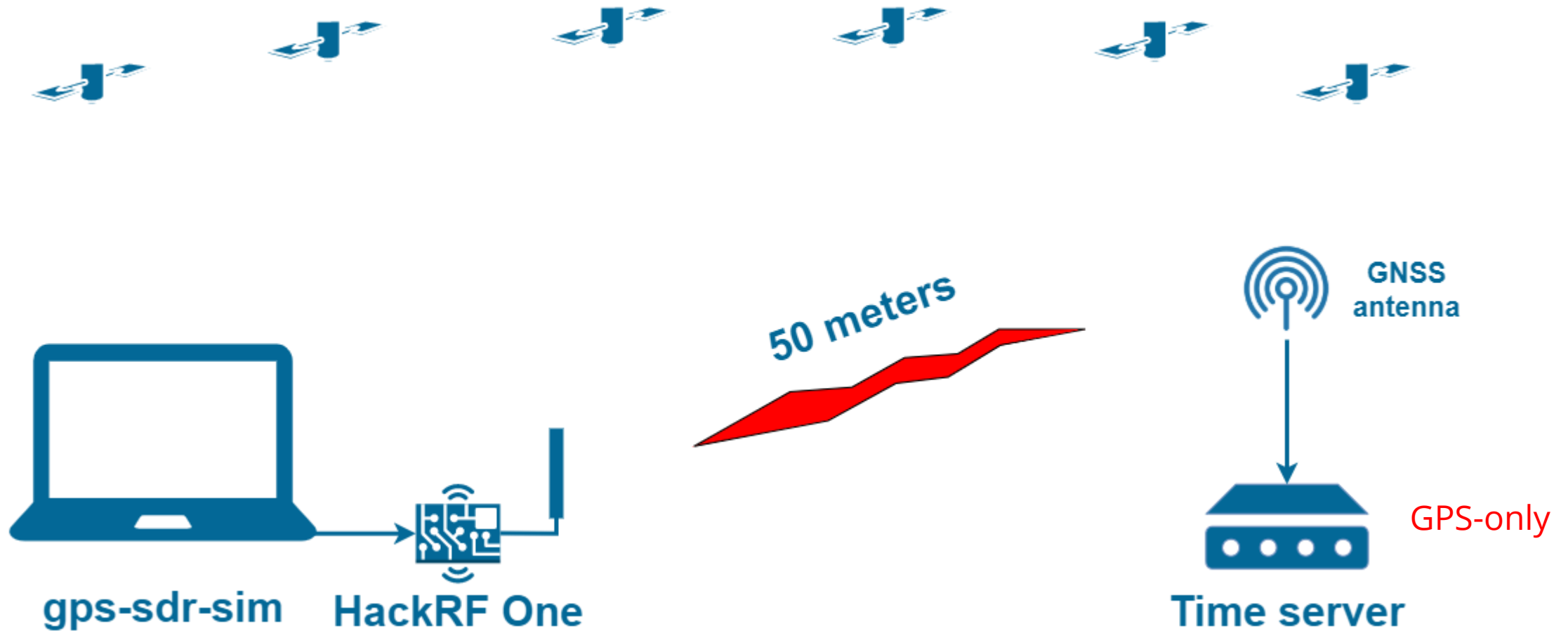
Real-time signal generation with [ADALM-Pluto](#)

[Microtronics/multi-SDR-GPS-SIM](#)

Real-time signal generation with [HackRF One](#) or [ADALM-PLUTO](#). Has settings for over-the-air operation: Target distance [m], bearing [°], and height [m]. Parameters can be changed on the fly.

We can assume that the application is designed to perform real attacks.

Attack scenarios. GPS spoofing with HackRF One



Attack cost - 320 USD

Attack time - from 15 seconds to 5 minutes

Protection - use multi-GNSS receivers

Detection at the system level is easy

RF Amplifier + directional antenna



RF Microwave Power
r 10W

US \$291.19

US \$3.32 Вам купон

Quantity:

1 999 piec

Free Shipping
to Belarus via AliExpr
Estimated Delivery o

Buy Now

75-Day Buyer Pro
Money back guar



HyperLOG® 7025

€199.95*

Addable options

Qty

1

Add to Cart

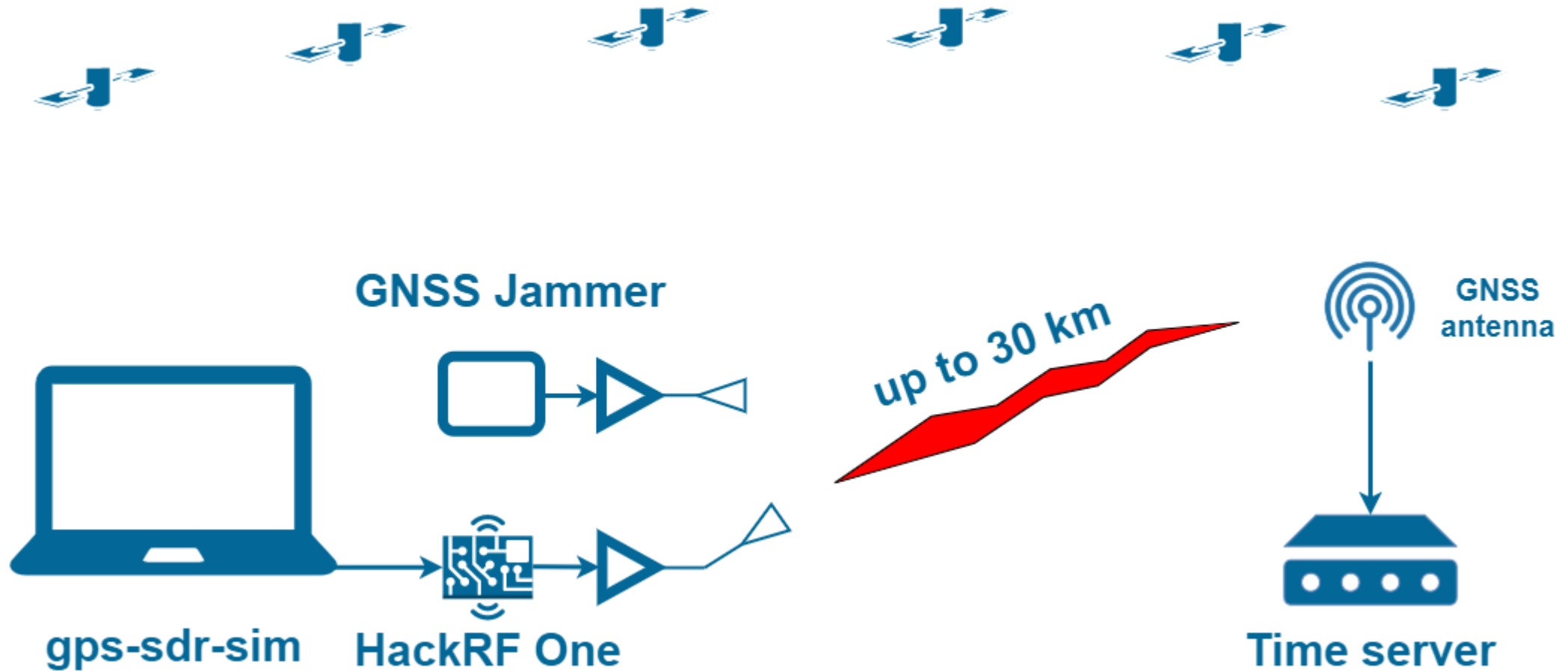
ADD TO COMPARE

- Only a single broadband antenna for the complete frequency range 700MHz up to 2,5GHz
- Optimal for usage with spectrum analysers for EMC measurements
- Incl. high-tech radom with modern, appealing design
- Freely alignable polarisation
- Calibration data can be saved to an IC on the antenna
- Excellent forward/backward ratio
- Excellent symmetry of radiation patterns
- Integrated 1/4" tripod socket
- Suitable for mobile use
- Suitable for outdoor installation
- Directional
- Robust design

Output power 10W

4 dB antenna gain

Attack Scenarios. GNSS spoofing with HackRF One, jammer and amplifier



Attack cost – 1.5k USD

Attack time - from 15 seconds to 5 minutes

System-level detection is not possible if all time servers are being covered

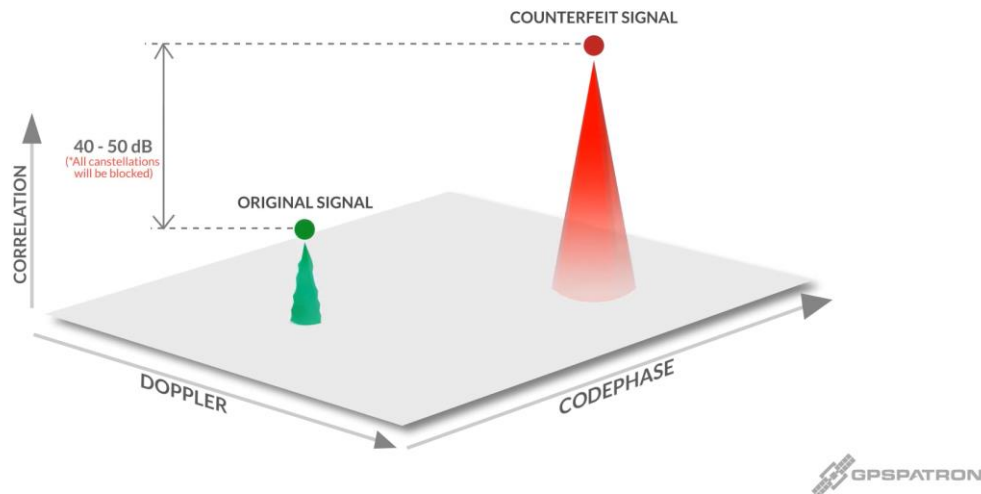
Types of GNSS Spoofing

Non-coherent

Generation of a fake GNSS signal not synchronized with the real one.

Incorrect coordinates, time, pseudo-distance, Doppler, etc.

The first step of the attack requires suppressing the real signals so that the receiver under attack goes into tracking mode and switches to the fake signals.



Coherent

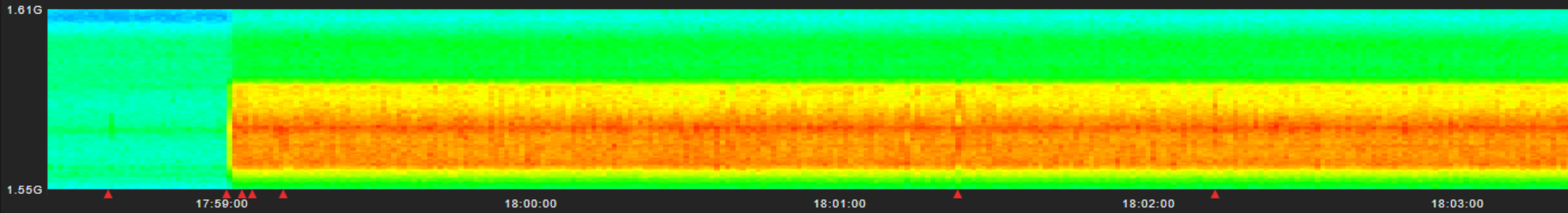
Generation of a fake GNS signal that is **completely identical** to the real one.

Instant switching to a fake signal → imperceptible, smooth drift of LLA or PPS phase

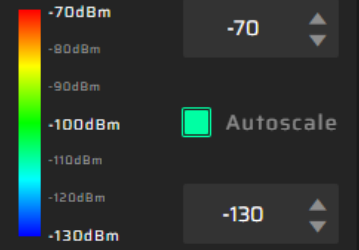


Non-Coherent Attack Example

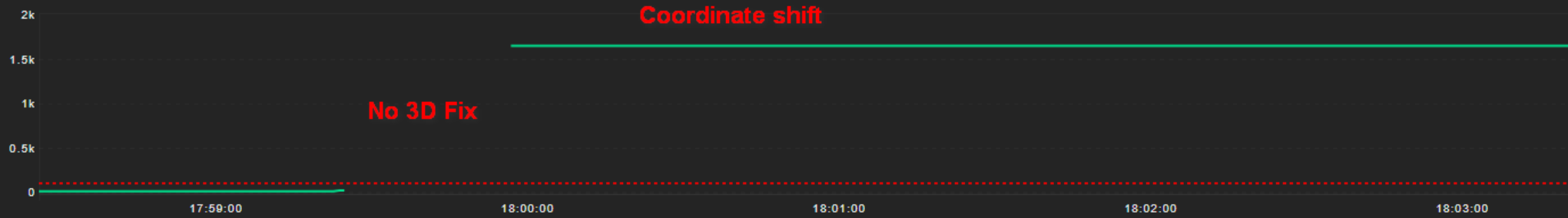
Spectrum Waterfall



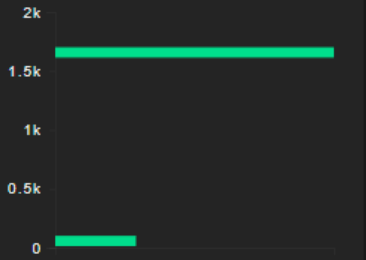
Power Scale



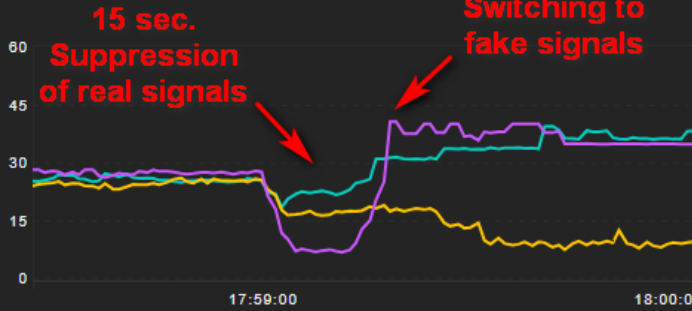
Horizontal Position Accuracy (m)



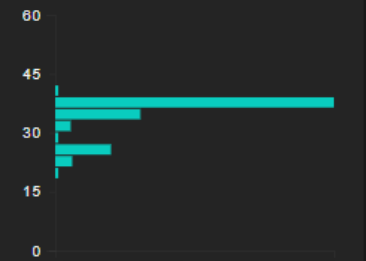
Histogram



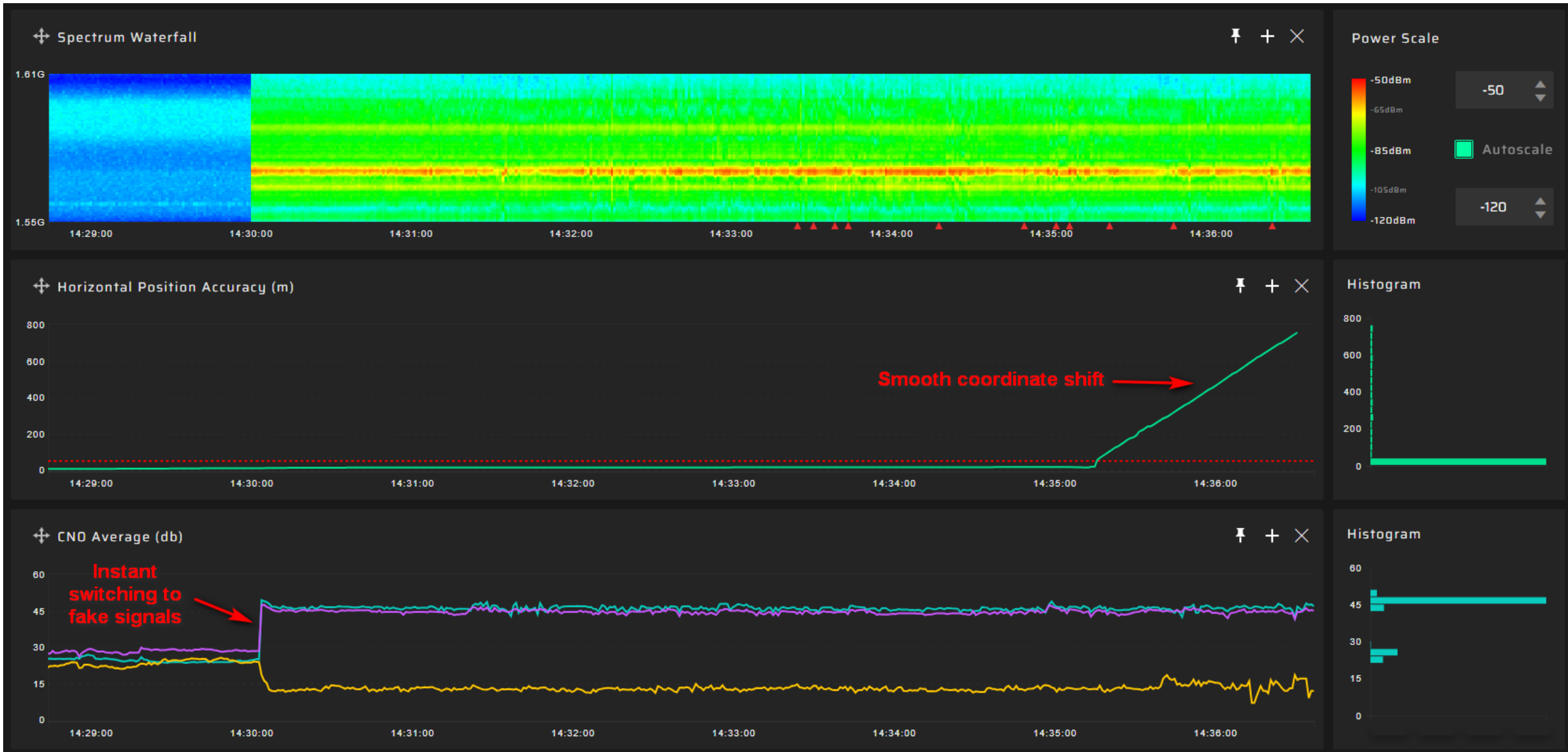
CNO Average (db)



Histogram



Coherent attack example with gradual coordinate shift



Data Formats for Analysis

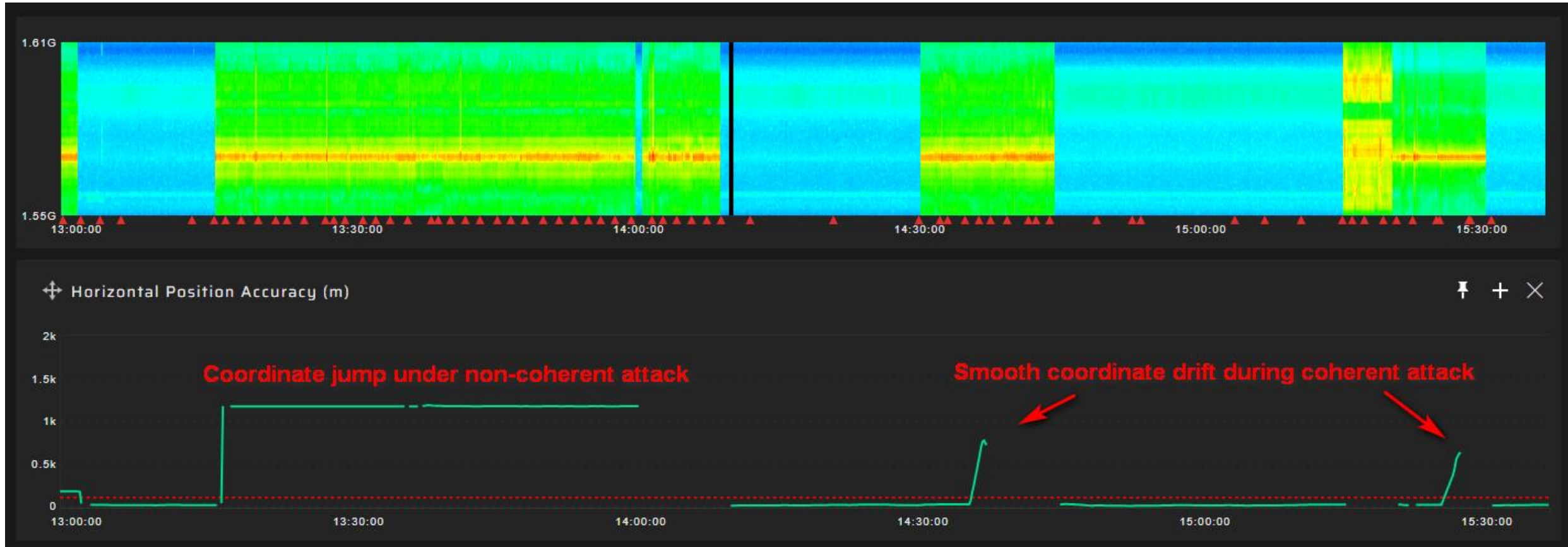
NMEA

- Timestamp
- Coordinates
- Velocity
- Signal to noise ratio
- Number of visible sats

Proprietary binary data format (UBX)

- Gain
- RF Spectrum
- Residuals
- Pseudorange
- Doppler
- Carrier Phase & Lock Time

Coordinate Monitoring



Advantages: the most simple algorithm

Disadvantages:

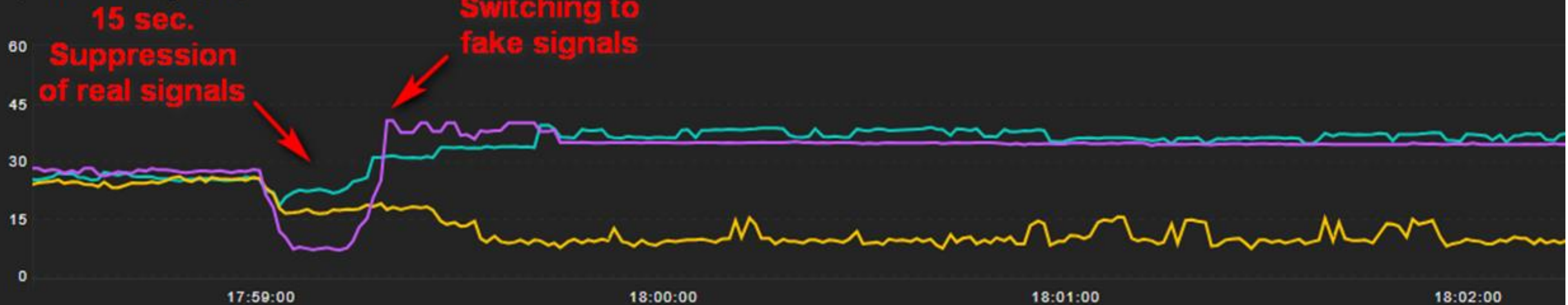
- late detection - you will only detect spoofing after your receiver has successfully spoofed.
- GNSS generator can simulate your coordinates

Coordinate Monitoring Weakness - Late Detection

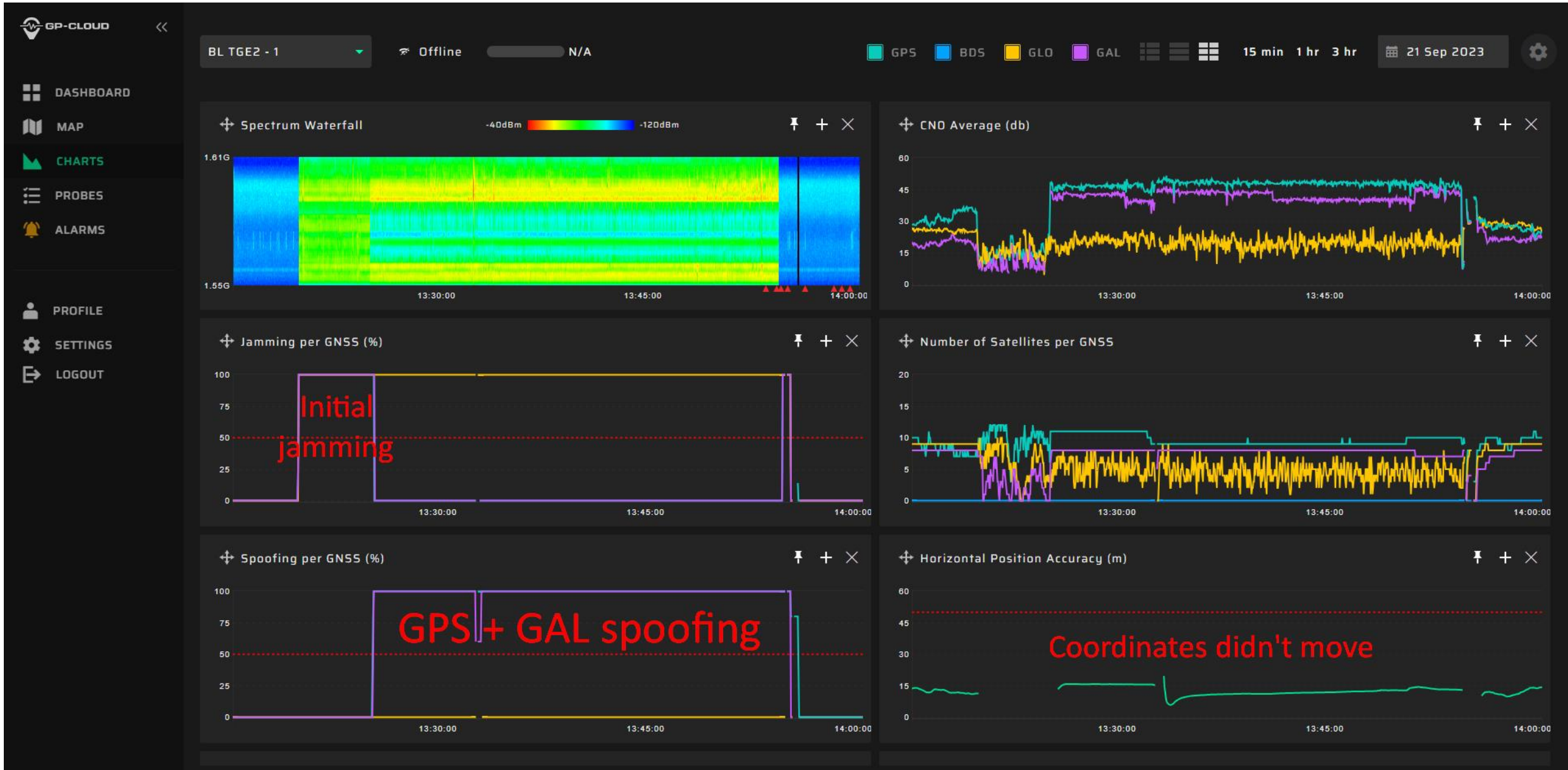
Horizontal Position Accuracy (m)



CNO Average (db)



Coordinate Monitoring Weakness - A time-only attack



Stop Scenario Generation DUT input power, dBm -80,00

Time Manipulation Coordinates Manipulation DUT ECEF impairment Satellites impairment In-Band Noise

PPS Phase Shift, s: -2u
GPS Time of Week Shift, s*: +0
Sats Clock Corr Offset, ns**: +0n

* ToW manipulation will lead to loss satellites tracking ** Rough value estimation

```

Message 14:41:02 --> USRP config CF: 1,57542G; IQ rate: 2M; DUT Input Power: -80; USRP Gain: -8
=====
Message 14:41:05 --> USRP GPSDO successfully locked at 14:41:06
Please wait until 14:41:42
=====
Message 14:41:42 --> GENERATION STARTED
=====
Message 14:42:29 --> PPS shifted by -500ns. Total PPS shift -500n
=====
Message 14:42:38 --> PPS shifted by -500ns. Total PPS shift -1u
=====
Message 14:43:23 --> PPS shifted by -500ns. Total PPS shift -1,5u
=====
Message 14:43:35 --> PPS shifted by -500ns. Total PPS shift -2u
=====

```

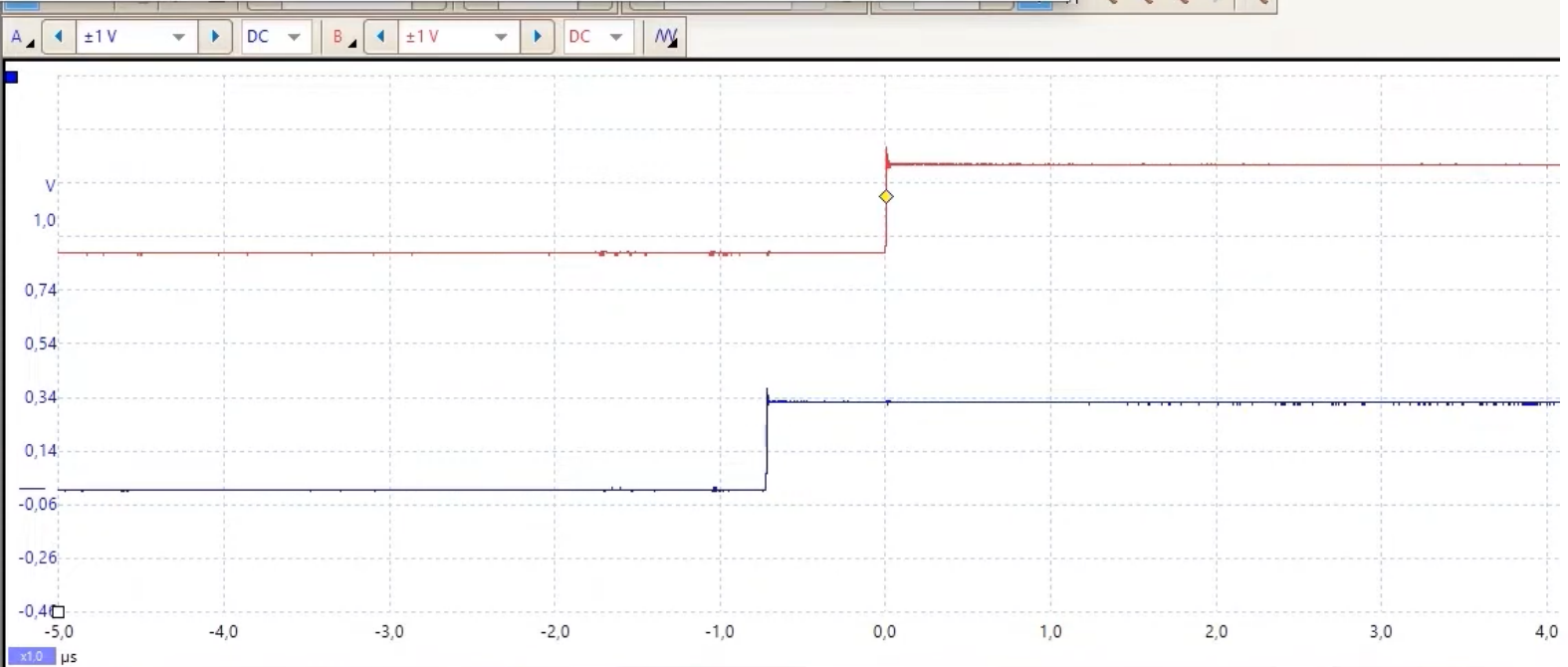
Messages - UBX - NAV (Navigation) - TIMEUTC (UTC Time)

- ... POSECEF (Position ECEF)
- ... POSLLH (Geodetic Position)
- ... PVT (Navigation PVT Solution)
- ... RELPOSNED (Relative Position NED)
- ... RESETODO (Reset Odometer)
- ... SAT (Satellite Information)
- ... SBAS (SBAS Status)
- ... SIG (Signal Information)
- ... SLAS (QZSS SLAS Status)
- ... SOL (Navigation Solution)
- ... STATUS (Navigation Status)
- ... SVIN (Survey-in)
- ... SVINFO (SV Information)
- ... TIMEBDS (BDS Time)

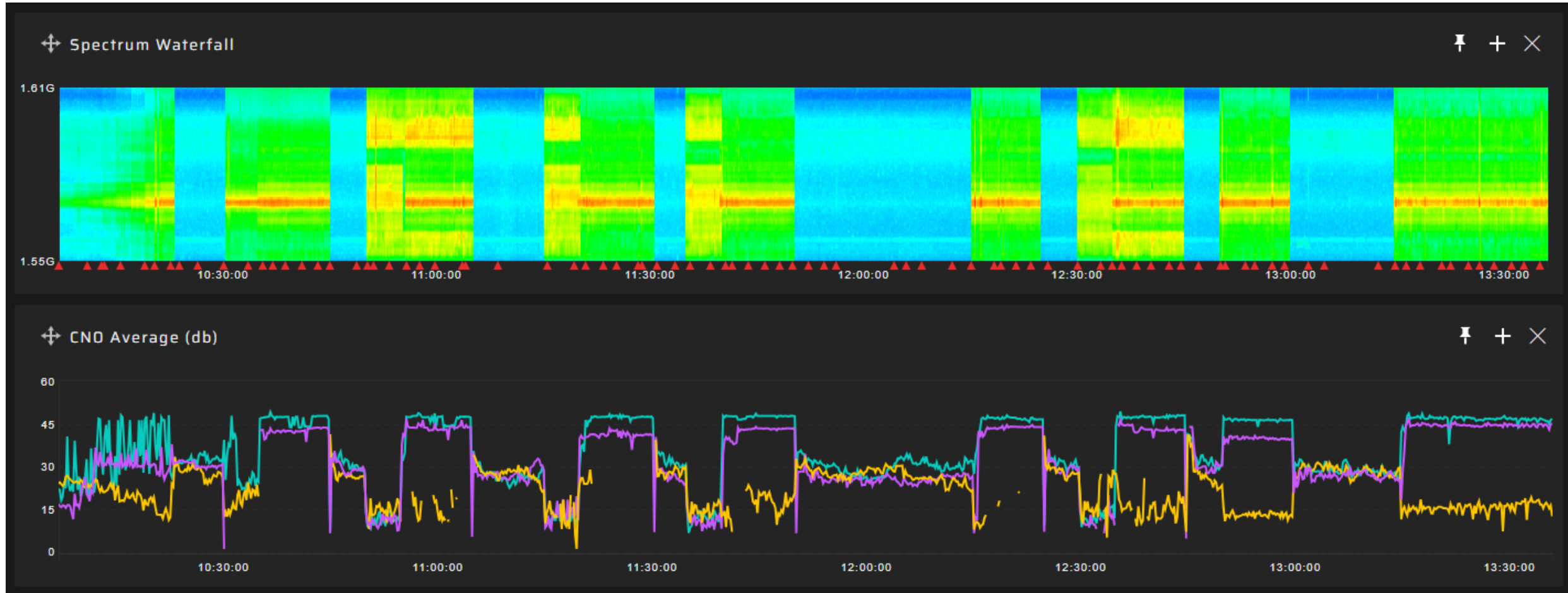
UBX - NAV (Navigation) - TIMEUTC (UTC Time)

Time of week: 225848.000 [s]
Date: 19. 4. 2022 [D/M/Y]
Time: 14:43:50 [H/M/S]
Standard: USNO
Fract. Seconds: 0000 [ns]

Longitude	27.67581300
Latitude	54.01172867
Altitude	236.690 m
Altitude (msl)	212.000 m
TTFB	
Fix Mode	3D
3D Acc. (m)	50
2D Acc. (m)	16.0
PDOP	1.1
HDOP	1.06
Satellites	



CNO Average Monitoring



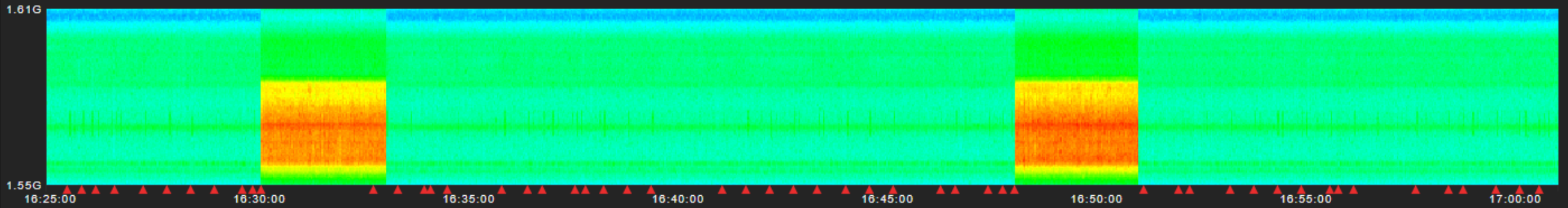
Advantages: Spoofing early detection. It is easy to set limits for powerful spoofing detection

Disadvantages:

- GNSS generator can simulate any value of signal-to-noise ratio.
- It is difficult to set thresholds to detect low-power spoofing combined in combination with an acceptable false alarm rate.

CNO Average Monitoring Weakness - Minor CNO shift

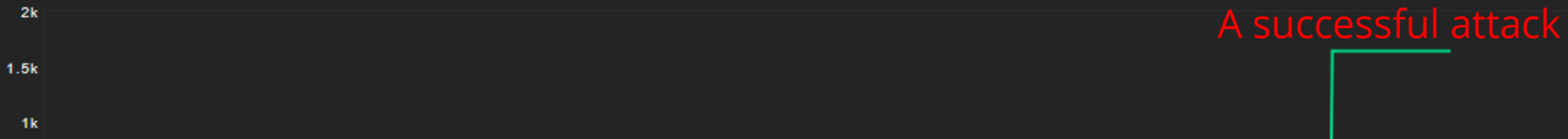
Spectrum Waterfall



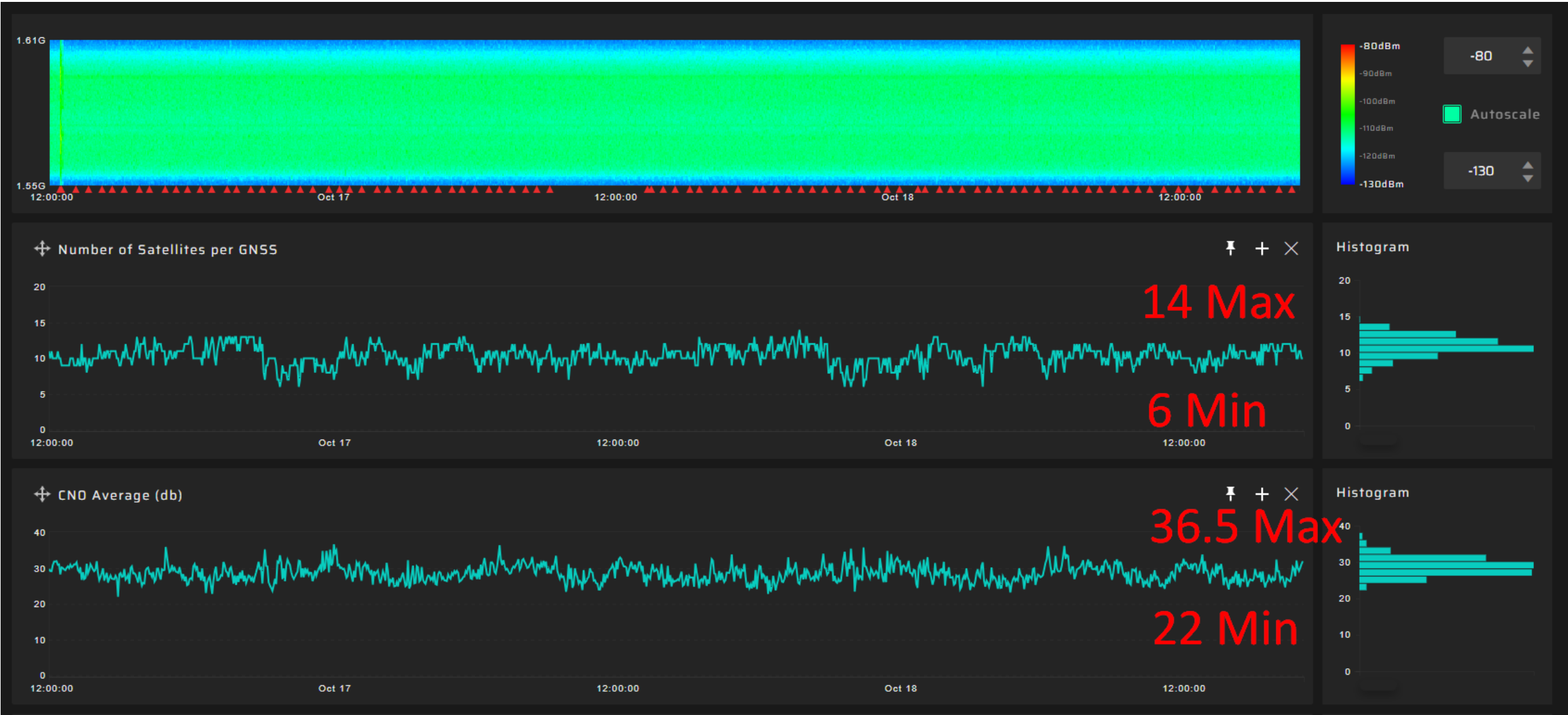
CNO Average (db)



Horizontal Position Accuracy (m)



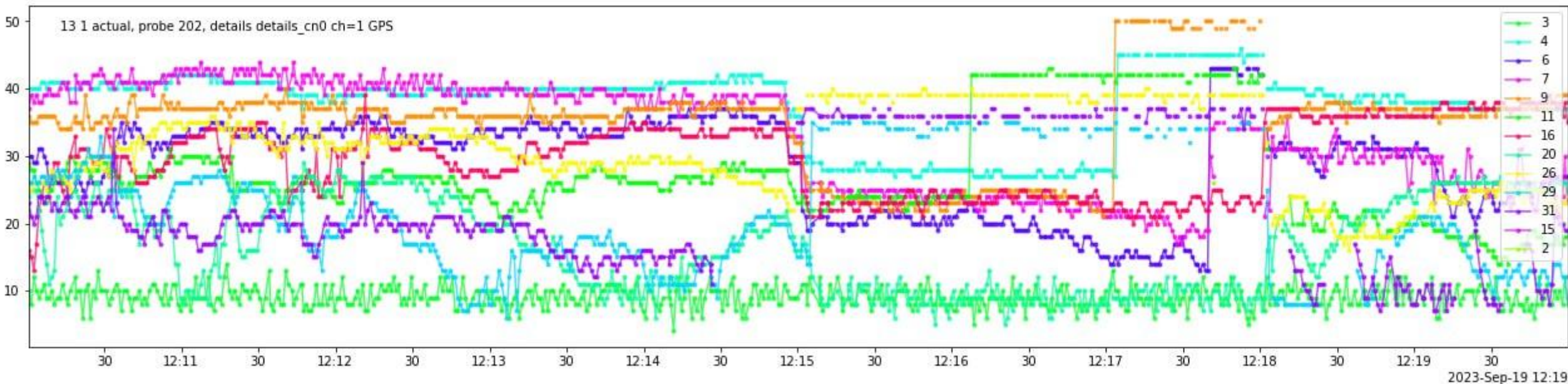
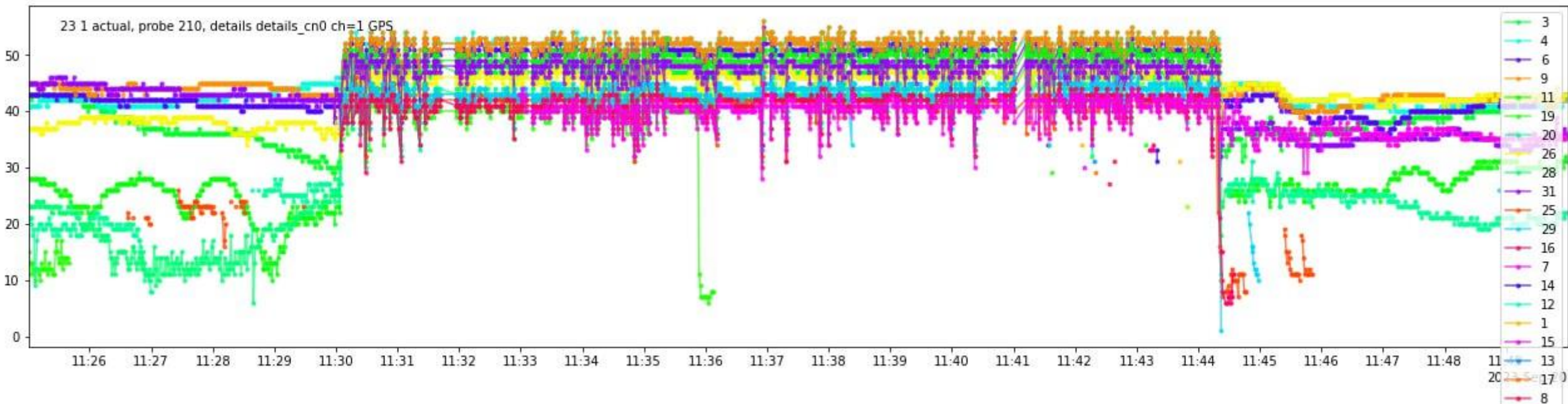
CNO Average Monitoring Weakness - Large CNO deviation under normal conditions



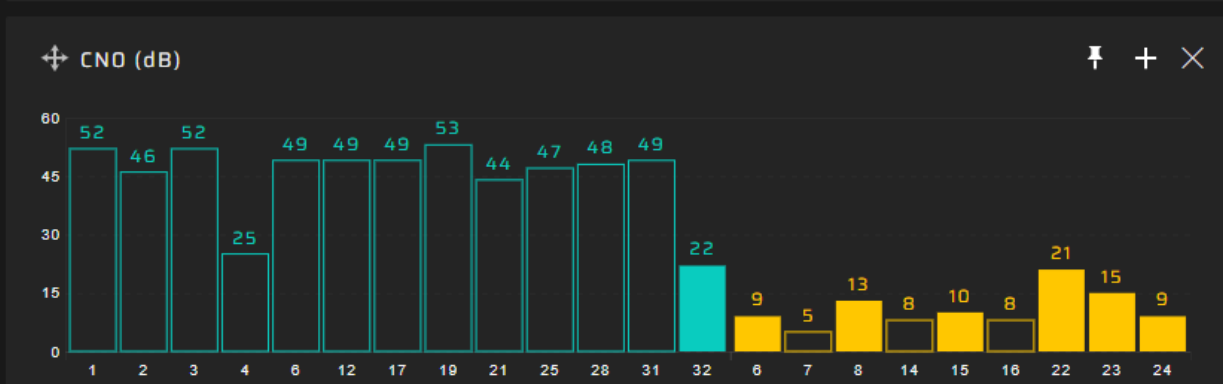
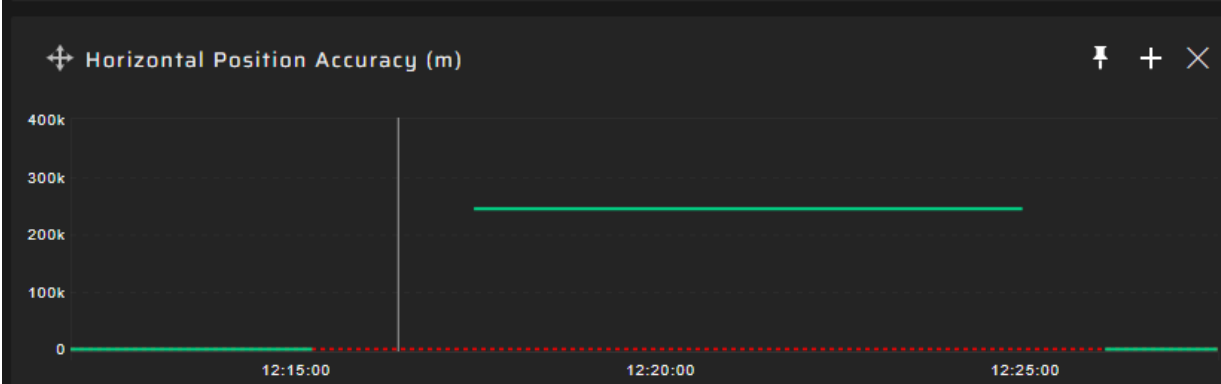
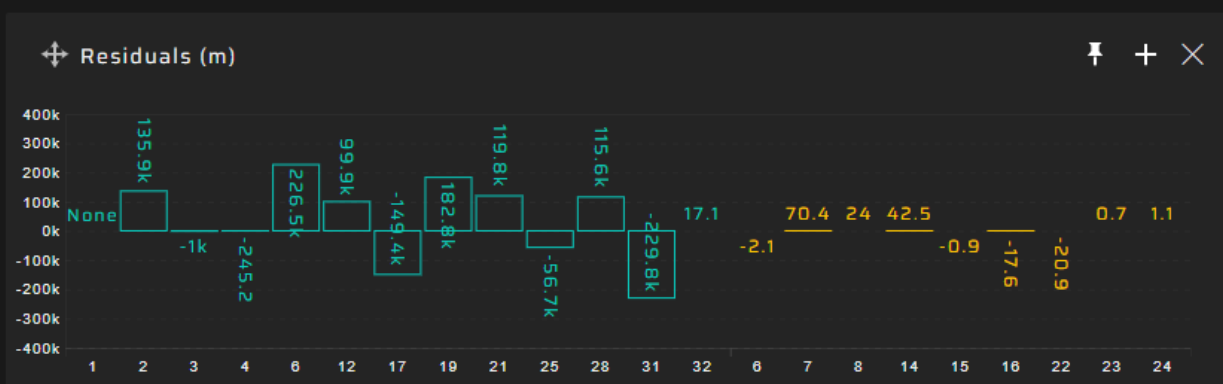
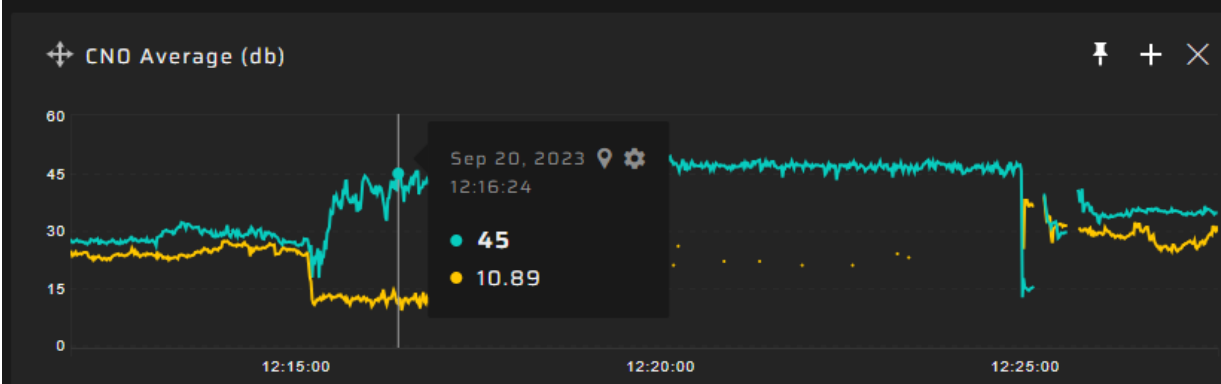
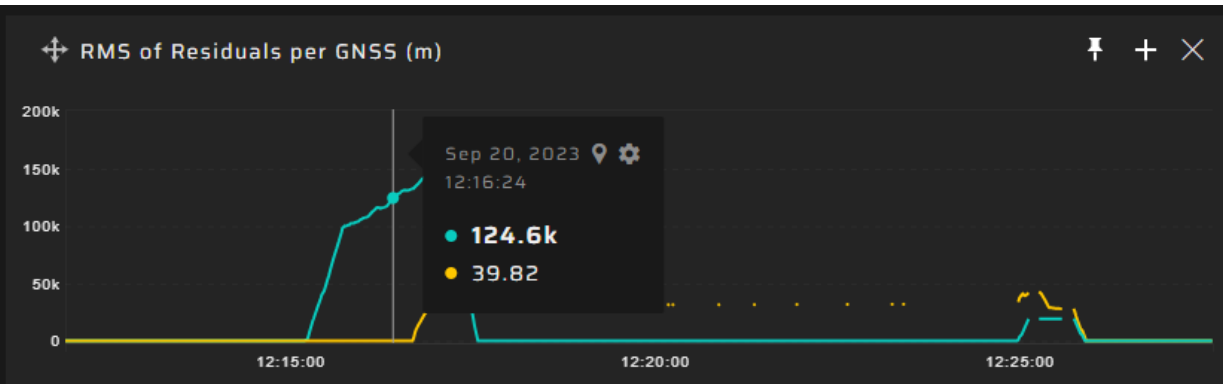
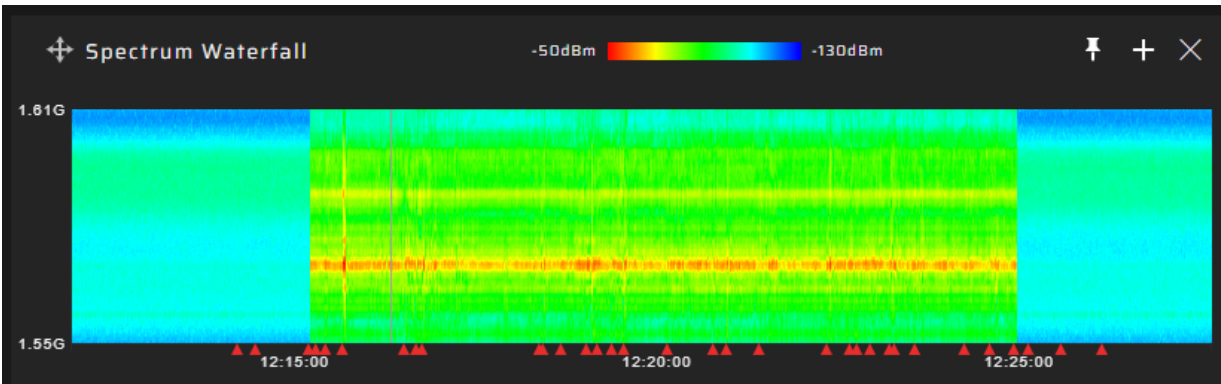
Monitoring of CNO distribution between satellites



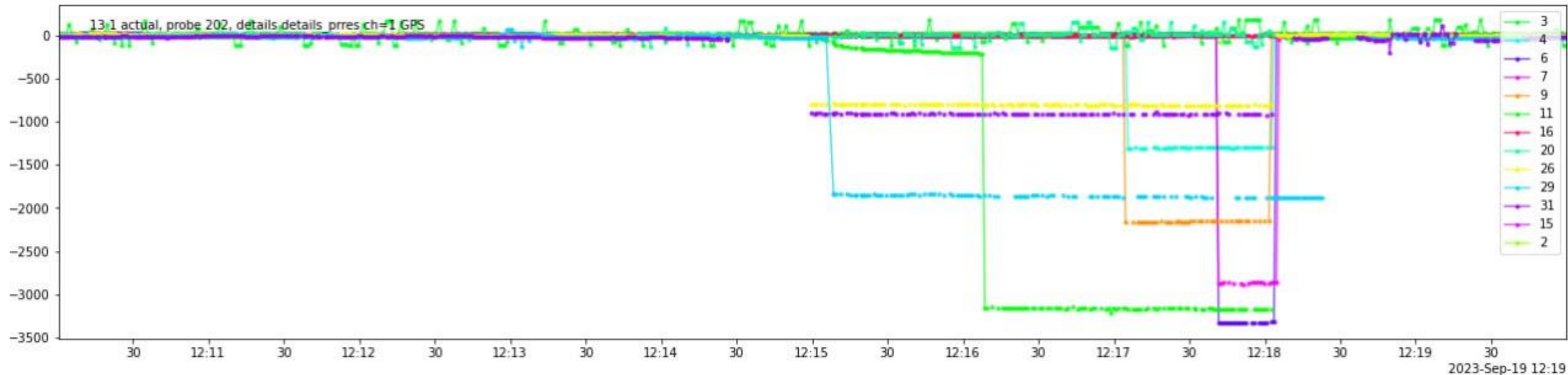
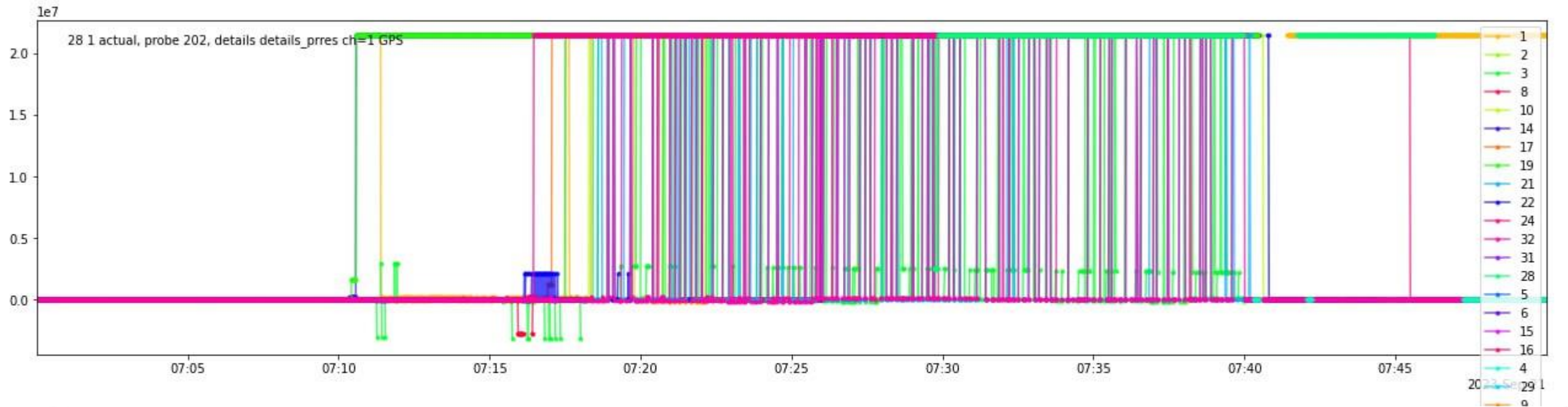
CNO monitoring for each satellite



Pseudorange residuals monitoring for non-coherent spoofing detection

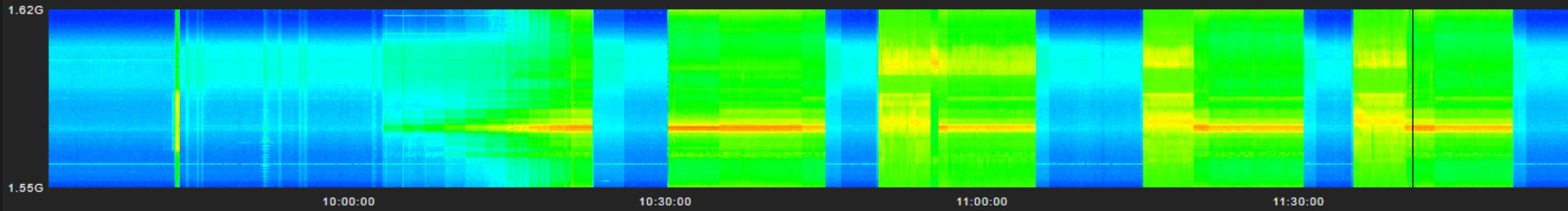


Pseudorange residuals monitoring for non-coherent spoofing detection



Spectrum, power & gain monitoring

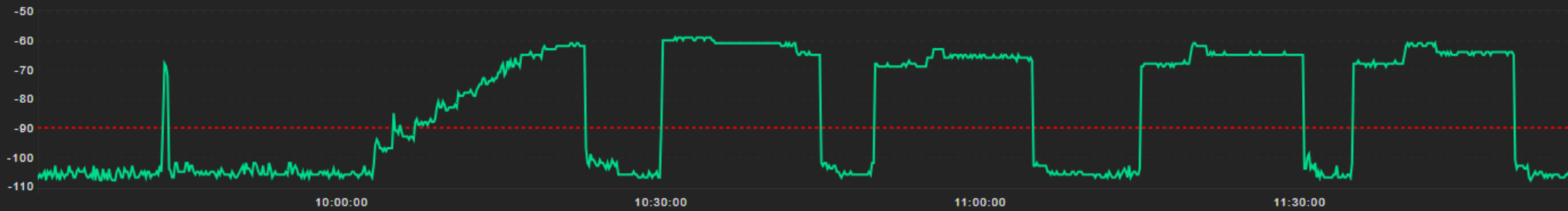
Spectrum Waterfall



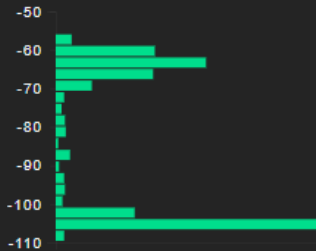
Power Scale



Peak Power (dBm)



Histogram



CNO Average (db)



Histogram



Spectrum, power & gain monitoring



DataStream Authentication

Messages - UBX - RXM (Receiver Manager) - SFRBX (Subframe Data NG)

UBX - RXM (Receiver Manager) - SFRBX (Subframe Data NG) 0 s

denotes data received on subChn Strip Parity Bits

SV	MSG	DATA (* denotes invalid words)
GAL 4 E1B 0	E8	08755555 5550QAAA AAAAAAAAAA AAAAA8000 AAAAA8000 2C17C12A AAAAA4A3E 8BCAC000
GAL 9 E1B 0	E8	08755555 5550QAAA AAAAAAAAAA AAAAA8000 AAAAA8000 0000002A AAAAA5877 ED0AC000
GAL 15 E1B 0	E8	08755555 5550QAAA AAAAAAAAAA AAAAA8000 AAAAA05C 046CC3EA AAAAA51B5 038AC000
GAL 21 E1B 0	E8	08755555 5550QAAA AAAAAAAAAA AAAAA8000 AAAAA8F9D 5B57856A AAAAA4643 984AC000
GAL 31 E1B 0	E8	08755555 5550QAAA AAAAAAAAAA AAAAA8000 AAAAAA07D E48F87EA AAAAA72DC DC8AC000
GLO 5 L10F 1	12 5/490	65C011C4 8D40A6BC 1D534000
GLO 14 L10F -7	12 5/490	65C00FC4 8D40A6BC 1D50A800
GLO 15 L10F 0	12 5/490	65C011C4 8D40A6BC 1D534000
GLO 16 L10F -1	12 5/490	65C011C4 8D40A6BC 1D534000
GLO 23 L10F 3	12 5/490	65C00FC4 8D40A6BC 1D50A800
GPS 1 L1C/A 0	2	22C0ED1B 051A8A47 03C1677B 0A3109B9 8E973FE9 8135C183 2684D56C 02EF2859 8346D2FA 83F44DAF
GPS 10 L1C/A 0	2	22C0ED1B 051A8A47 053E26D1 8B6C3431 95244A5B 3E6E0123 262D4553 01D56867 035FA522 83F49F6C
GPS 12 L1C/A 0	2	22C0ED1B 051A8A47 0EC0EE58 0D073B9E 927971F3 00CD4125 9B4194A9 83A0684E 8387EBD5 83F49F6C
GPS 17 L1C/A 0	2	22C0ED1B 051A8A47 0B81F214 0ADB1FAD 941D700F 01C881F3 0521805E 8436E869 833570AC 03F49FE0
GPS 23 L1C/A 0	4/54/1	22C0ED1B 051A2C17 1D89AAF1 9C365CE4 09A37E8E 8E71060C 25000E87 17B18E0C 35D37852 ADF6AF34
GPS 24 L1C/A 0	2	22C0ED1B 051A8A47 0AC01274 0ED20C91 BDD00D7E 802141E3 21D7AB2F 04F66848 034263B8 03F49FB3
GPS 25 L1C/A 0	1	22C0ED1B 0519C957 0ED40004 13978DF9 A240E727 17CCE3A1 8D920320 0C43F4A5 80000405 8F87C717
GPS 32 L1C/A 0	2	22C0ED1B 051A8A47 033D36D3 0C53E654 3F5FAB38 3D9400F9 A7558168 04A2685E 832DB9BD 83F45F8B

ToW

GPS Subframe. 6sec

SBAS (SBAS Status)
... SIG (Signal Information)
... SLAS (QZSS SLAS Status)
... SOL (Navigation Solution)
... STATUS (Navigation Status)
... SVIN (Survey-in)
... SVINFO (SV Information)
... TIMEBDS (BDS Time)
... TIMEGAL (Galileo Time)
... TIMEGLO (GLO Time)
... TIMEGPS (GPS Time)
... TIMELS (Leap Second Information)
... TIMEQZSS (QZSS Time)
... TIMEUTC (UTC Time)
... VELECEF (Velocity ECEF)
... VELNED (Velocity WGS84)
RXM (Receiver Manager)
... ALM (Almanac)
... EPH (Ephemeris)
... IMES (IMES Status)
... MEASX (Measurement Data)
... PMP (Point to Multipoint)
... PMREQ (Power Mode Request)
... RAW (Raw Measurement Data)
... RAWX (Multi-GNSS Raw Measurement Data)
... RLM (Return Link Message)
... RTCM (RTCM input status)
... SFRB (Subframe Data)
... SFRBX (Subframe Data NG)
... SVSI (SV Status Info)
SEC (Security)
TIM (Timing)
UPD (Firmware Update Messages)
... ??-?? (Unknown)
... ??-?? (Custom)
UNKNOWN
CUSTOM

GNSS receiver glitches due to spoofing



Dataset from Ublox

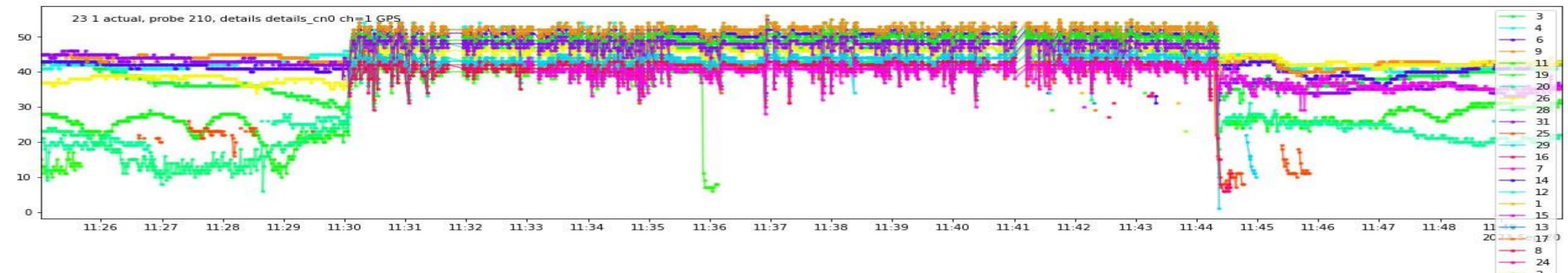
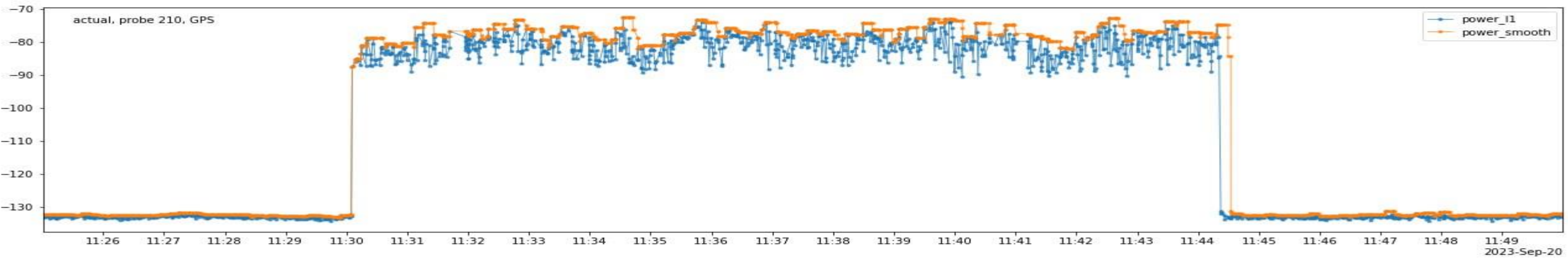
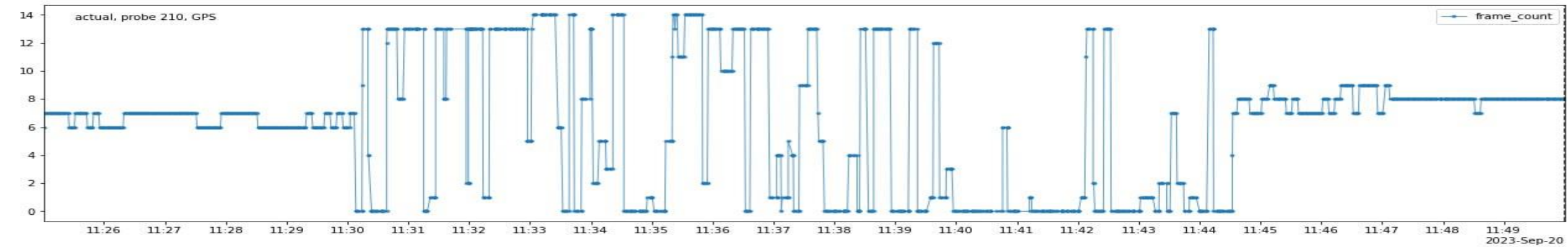
```
1 [
2 {
3   "AGC": 3354,
4   "UTC": "2023-09-26T23:59:58Z",
5   "gDOP": 1.51,
6   "hAcc": 2.082,
7   "hDOP": 0.81,
8   "hMSL": 100.488,
9   "magI": 150,
10  "magQ": 156,
11  "ofsI": 9,
12  "ofsQ": 50,
13  "pDOP": 1.31,
14  "sAcc": 0.02,
15  "tAcc": 5,
16  "tDOP": 0.75,
17  "vAcc": 2.001,
18  "vDOP": 1.03,
19  "velD": -0.029,
20  "velE": -0.016,
21  "velN": -0.027,
22  "Noise": 100,
23  "NumSV": 19,
24  "Glo_N4": 7,
25  "Glo_Mt": 1366,
26  "Height": 134.793,
27  "BDS_SOW": 259202,
28  "FixType": 3,
29  "Gal_Tow": 259216,
30  "Gal_Wno": 1257,
31  "Glo_TOD": 10798,
32  "Jamming": 13,
33  "BDS_Week": 925,
34  "BDS_fSOW": -201329,
35  "BDS_tAcc": 3341,
36  "GPS_Week": 2281,
37  "GPS_fTOW": -201329,
38  "GPS_itOW": 259216000,
39  "GPS_tAcc": 5,
40  "Gal_fTow": -201343,
41  "Gal_tAcc": 6,
42  "Glo_fTOD": -201381,
43  "Glo_tAcc": 6,
44  "Latitude": 52.1567885,
45  "BDS_LeapS": 4,
46  "BDS_Valid": true,
47  "GPS_Valid": true,
48  "GPS_leapS": 18,
49  "Gal_Valid": true,
50  "Gal_leapS": 18,
51  "Glo_Valid": false,
52  "Longitude": 21.075326099999998,
53  "ChannelError": false,
54  "ChannelNumber": 1,
```

Common module data

```
54   "ChannelNumber": 1,
55   "SpoofDetState": 1,
56   "UBLOX_Reseted": false,
57   "AntennaCurrent": 9.84,
58   "ChannelEnabled": true,
59   "MeasurementMode": 0,
60   "ChannelPowerEnabled": true,
61   "RAW": [
62     {
63       "CP": 114521463.55281612,
64       "PR": 21792712.931179166,
65       "CNO": 27,
66       "SQI": 0,
67       "Azim": 329,
68       "Elev": 6,
69       "SV_Id": 4,
70       "prRes": 3.4700000000000006,
71       "FreqId": 0,
72       "svUsed": true,
73       "Band_Id": 0,
74       "Doppler": -473.7751159667969,
75       "GNSS_Id": 0,
76       "HalfCyc": false,
77       "cpStdev": 0.02,
78       "cpValid": true,
79       "doStdev": 0.512,
80       "prStdev": 2.56,
81       "prValid": true,
82       "AlmAvail": false,
83       "EphAvail": true,
84       "LockTime": 1460,
85       "Smoothed": false,
86       "svHealth": 1,
87       "TimeValid": 1,
88       "SubHalfCyc": false,
89       "crCorrUsed": false,
90       "doCorrUsed": false,
91       "prCorrUsed": false,
92       "OrbitSource": 1,
93       "FrameReceived": false,
94     },
95     {
96       "CP": 0,
97       "PR": 0,
98       "CNO": 19,
99       "SQI": 0,
100      "Azim": 94,
101      "Elev": 26,
102      "SV_Id": 5,
103      "prRes": 8.38,
104      "FreqId": 0,
105      "svUsed": false,
```

Data per satellite

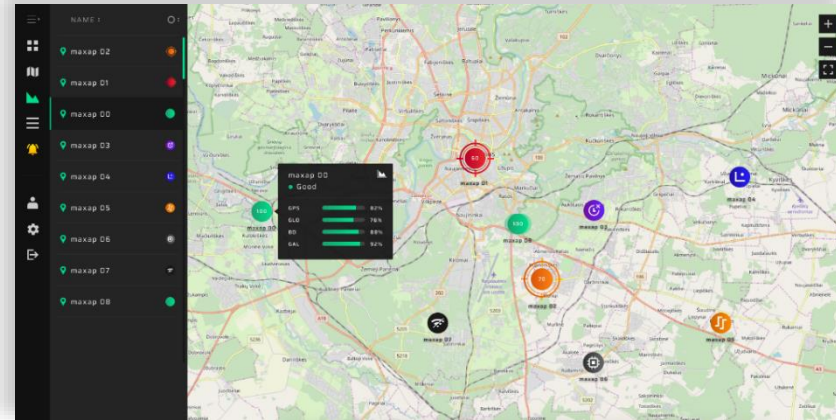
Data correlation example



GPSPATRON Concept of Operation

GP-Probe conducts GNSS signal measurements and transmits raw data to the GP-Cloud for real-time processing. GP-Cloud uses advanced anomaly detection and classification algorithms.

GP-Cloud



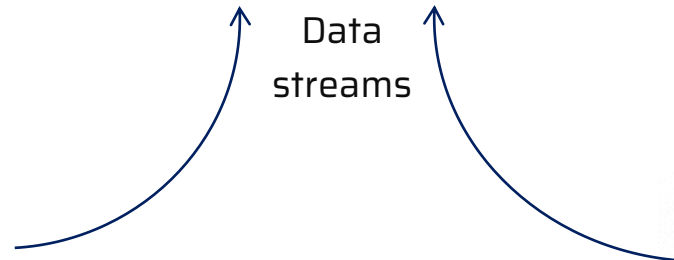
Statistics
User notification
API for integration



High-performance 3-channel probe



Data streams



One-channel probe



GP-Probe DIN L1

Designed for telecom to monitor GNSS interference and synchronization quality



Cost-effective GNSS probe with built-in RF blocker, onboard GNSS interference/anomaly detection and LUA scripting.

GP-Probe TGE2

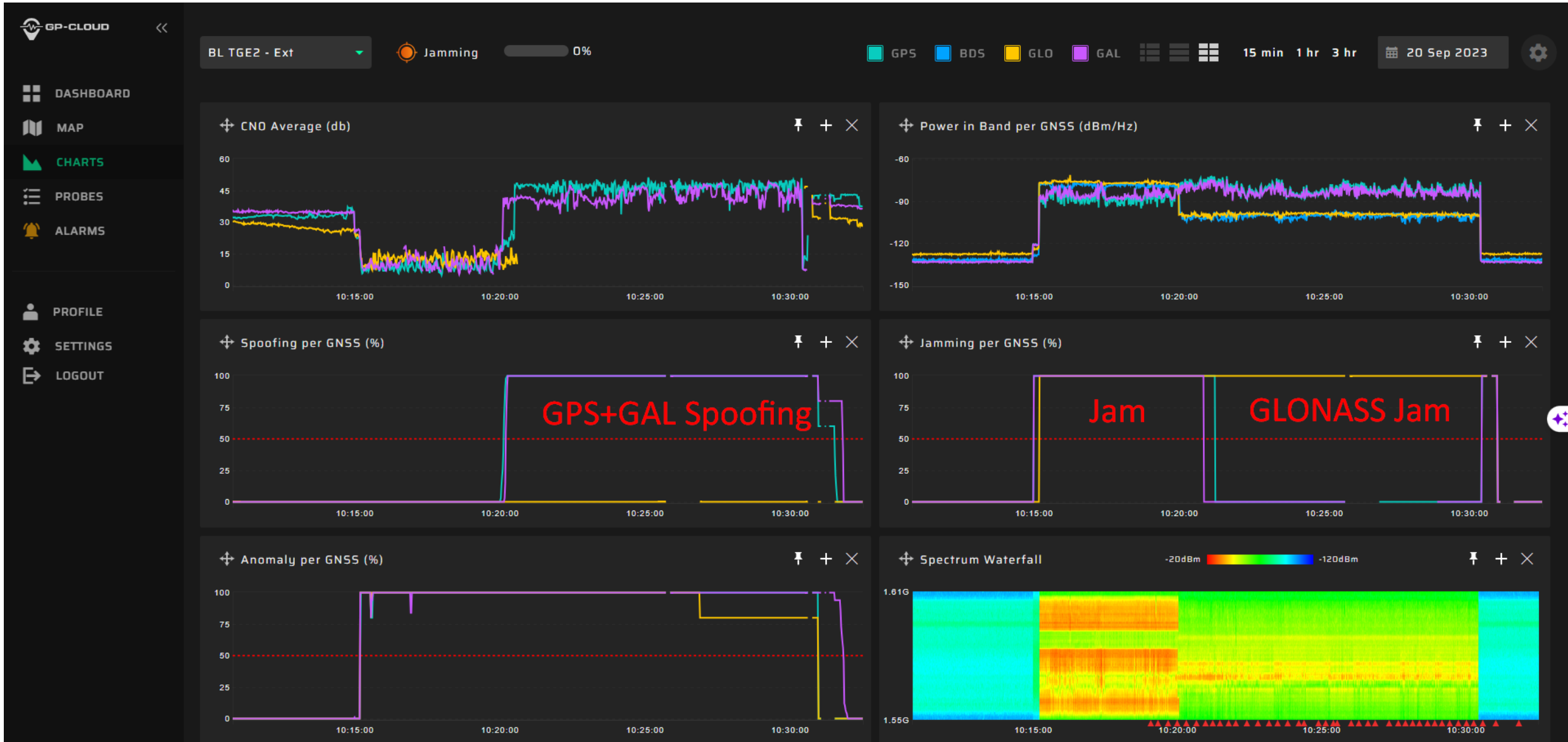
Three-channel GNSS probe with an embedded RF signal analyzer



- Three RF channels enable spatial signal analysis to ensure detection of all sophisticated GNSS spoofing attack scenarios.
- 60 MHz real-time RF signal analyzer for spectrum monitoring, interference classification and localization with TDOA.

An example of proper classification

5 minutes of initial jamming. Then spoofing GPS + Galileo in combination with GLONASS jamming



Low power spoofing detection





THANK YOU

for your attention

Contacts

www.gpspatron.com

mb@gpspatron.com

www.youtube.com/c/GPSPATRON

twitter.com/gpspatron

Maksim Barodzka

CEO @ GPSPATRON

