


Spoofing & OSNMA for and risk in autonomous applications

Gustavo Lopez – Senior Market Portfolio Manager

The background of the slide features a dark, blue-toned image of a person's face, partially obscured by a grid of binary code (0s and 1s) that appears to be floating or projected over the image. The person's face is on the right side, looking towards the left. The overall aesthetic is high-tech and digital.

“Time is what determines security.
With enough time,
nothing is **unhackable.**”

- Aniekee Tochukwu Ezekiel

Septentrio, a leading provider of high performance GNSS solutions

- ❑ 25 years of leading GNSS innovation
- ❑ Headquartered in **Leuven, Belgium**
- ❑ **160+ employees, 80+ of which in R&D**
- ❑ **Mission critical GNSS solutions** for the most demanding location and positioning applications globally
- ❑ Serving expanding OEM customer base, in emerging ***Autonomous Systems, industrial & critical infrastructure***
- ❑ Part of **Hexagon** (Sweden) since March 2025



Belgium HQ

Five additional sales and R&D centers globally



Is Jamming or spoofing happening?

Various Recent Incidents:

- GNSS jamming/spoofing in conflict zones
- GNSS jamming/spoofing in maritime navigation
- UAV loss or accidents (e.g. Light drone shows)

Thousands of flights to and from Europe affected by suspected Russian jamming

About 46,000 aircraft have logged GPS problems over Baltic Sea since August, says report



EasyJet a
according to

Flights in and out of the airport were suspended for several hours, and the airport was closed to all traffic.

GNSS Jamming and Spoofing Events Present a Growing Danger

Many reports of jamming and spoofing come from conflict zones



GNSS Jamming and Spoofing Present a Growing Danger

Many reports of jamming and spoofing come from conflict zones



Innovation: Recent GPS jamming in regions of geopolitical conflict

May 24, 2024 - By **Dong L. Wu, Ph.D.**

Click to read Richard Langley's article on GPS jamming and spoofing

May 24, 2024 - By **Dong L. Wu, Ph.D.**

Click to read Richard Langley's Innovation Insights column, "GNSS jamming in political conflict"

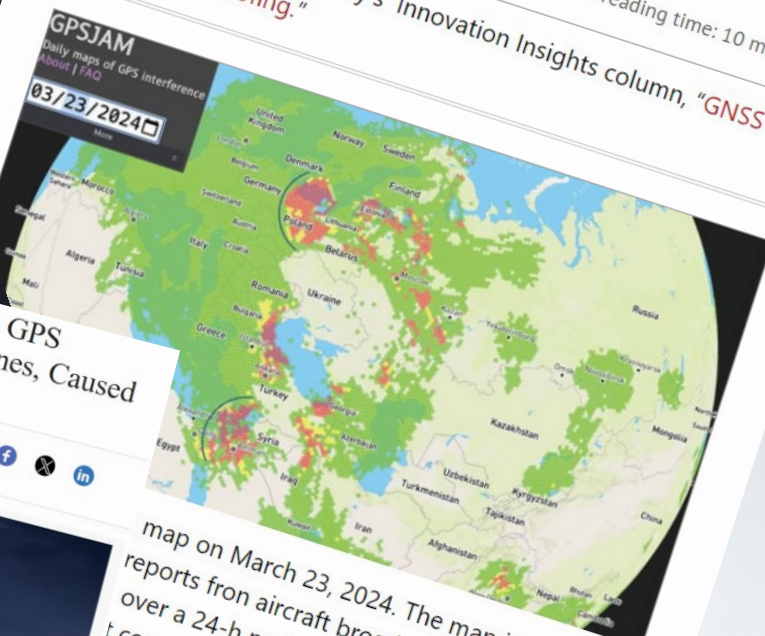
By Dong L. Wu, Ph.D.

Est. reading time: 10 minutes

GPSJAM
Daily maps of GPS interference
About | FAQ
03/23/2024

United Kingdom

Est. reading time: 10 minutes



...port is only 10 kilometers from Norway's border with Russia, and some 50 km from the coast.

a. Photo: Thomas Nilsen

Intensified GPS jamming is side effect of Russia's self-protection of Kola bases

...seen practically every day in airspace over eastern Finnmark is likely a self-defence measure for their own military installations, says Nilsen.

...authority.

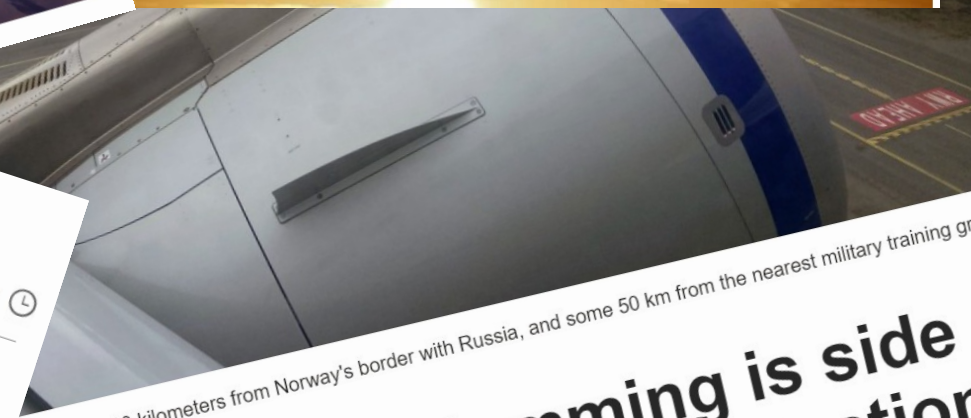
Interference effect of Russia's Kola bases

The jamming now seen practically every day in airspace over eastern Finnmark is likely a side effect of Russian electromagnetic defence measures for their own military installations, says Niels Andersen, director of the Norwegian Communications Authority.

#EUSpace 

UK flights are facing 'extremely dangerous Russian jamming': Report

London, UK • Edited By: Sneha Swaminathan • Updated: Apr 23, 2024, 12:33 AM IST



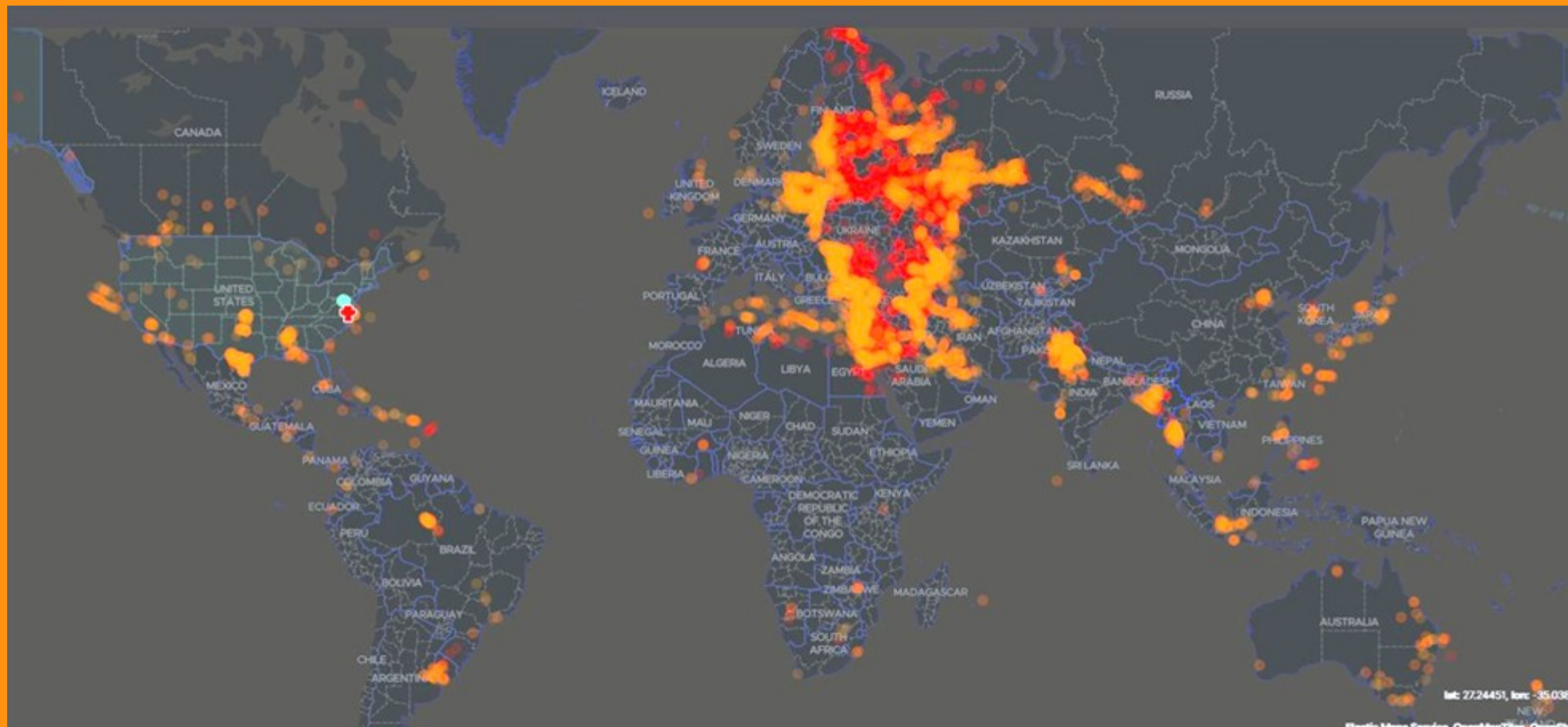
4. Photo: Thomas Nilsen

Effect of Russia's Kola bases

The jamming now seen practically every day in airspace over eastern Finnmark is likely a result of Russian electromagnetic defence measures for their own military installations, says Niels Andersen, director of the Norwegian Communications Authority.

#EUSpace 

#EUSpace 



Lots of jammers near French airport

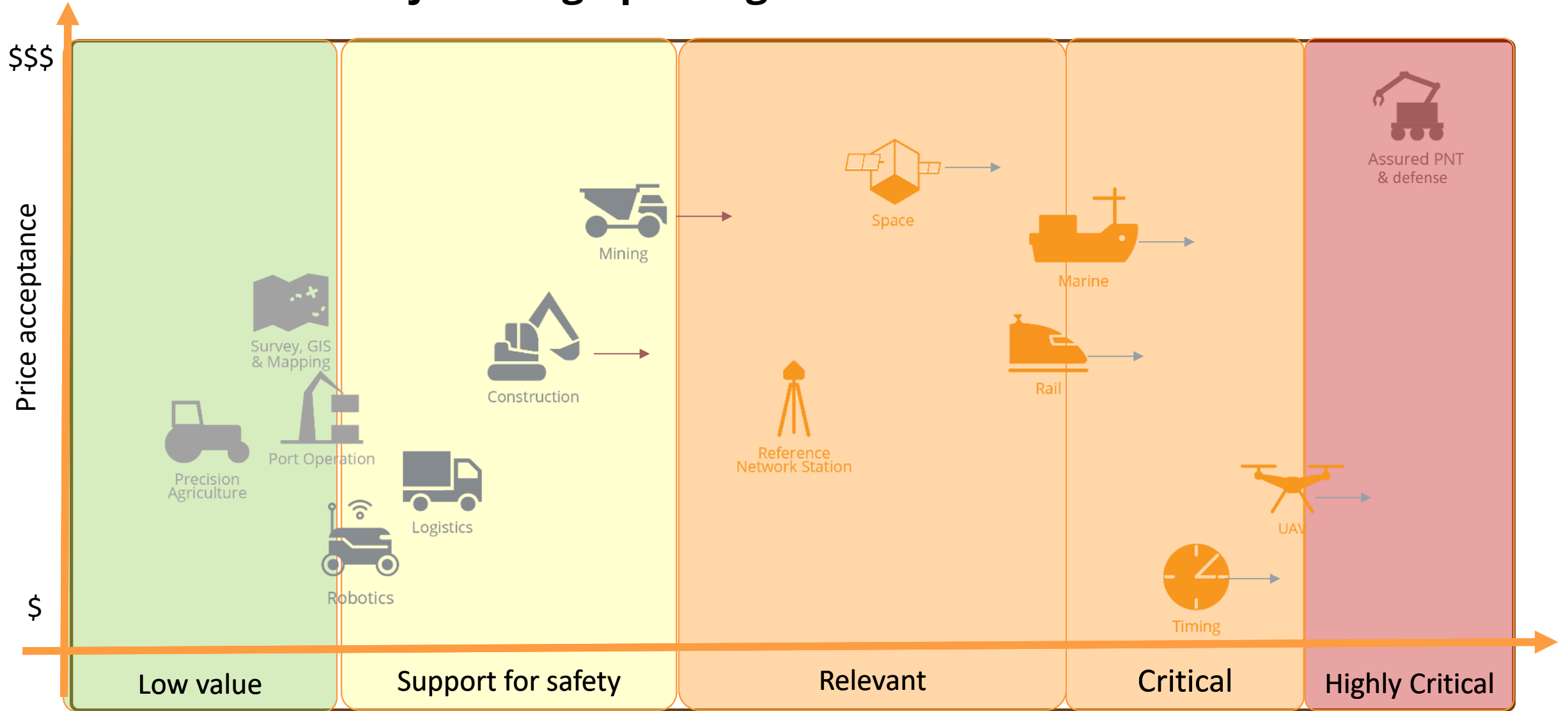
by Editor | Jul 21, 2023 | Blog



Image: Shutterstock

What's New: A media item about **multiple jammers disrupting operations at a French airport**. As soon as the authorities found one, they found another, then another!

Markets and Anti-jamming/spoofing resilience needs



OSNMA & Septentrio

Septentrio has been part of several initiatives with EUSPA & ESA for testing/validating OSNMA

Septentrio started focus on spoofing detection/mitigation thanks to Fantastic EUSPA project

Started with PolaRx5 and mosaic-T GNSS receivers as part of some of these projects

Galileo OSNMA started to be rolled in all Septentrio receivers since 2021

Today OSNMA is integrated (and is being used) in all Septentrio products



**Field Aware Navigation and Timing
Authentication Sensor for Timing
Infrastructure and Centimeter
level positioning**



**ROOT assessed the benefits of OSNMA
to boost 5G sync resilience.**



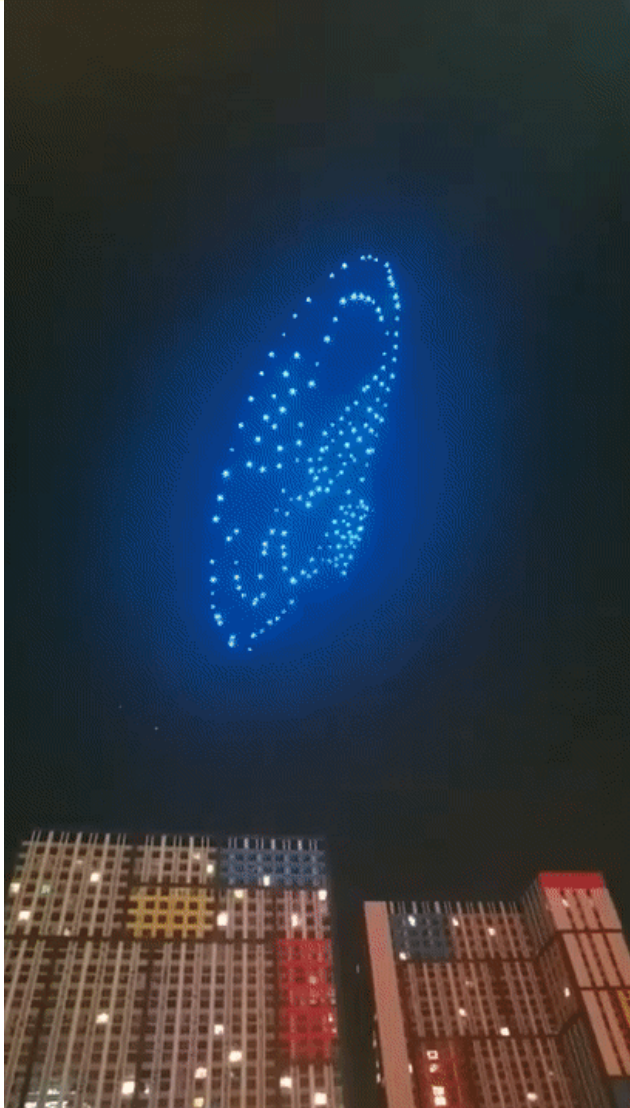
**OSNMA officially deployed and
being used in all Septentrio products**



Interference Types

	Jamming <i>Drowning out GNSS Signal</i> → No position	Spoofing <i>Overruling GNSS with fake GNSS signal</i> → Wrong position
Unintentional	<ul style="list-style-type: none">• Other Systems in GNSS bands Radar, Amateur radio,...• EMC Issues Displays, cameras, lidars,... <i>Clock harmonics etc.</i>	<ul style="list-style-type: none">• Repeaters <i>Production tests,</i> <i>Maintenance hangars</i>
Intentional	Devices designed to wipe-out GNSS Personal Protection Devices (web-shops) Military Jammers	<ul style="list-style-type: none">• Commercial SDR (low cost) <u>gps-sdr-sim</u>• GNSS simulator + Amplifier• GNSS Repeaters (meaconing)
	Increased occurrences More sophisticated attacks	Increased occurrences Easier to replicate Attention needed (not many solutions)

Not this :(



JAMMING Light drones

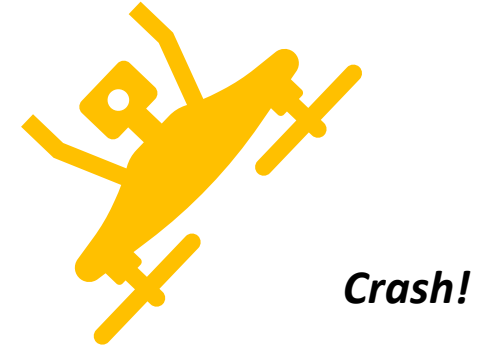
Drones are seen forming
Chinese characters (left)
before they fell out of the sky

Spoofing Detection: Goal => Authentication has a key role

- Problem:

- Spoofing injects fake GNSS signal into receiver
 - **Wrong position or timing**
 - Potentially catastrophic system malfunction

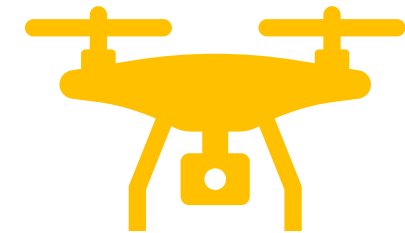
Hacked GNSS



- Solution:

- Spoofing Detection: Receiver alerts user to attack
 - User switches to backup system
 - Relative position or timing:
 - **Position attack → Dead reckoning with INS**
 - **Timing attack → Holdover to high accuracy oscillator (OCXO)**

Hacked GNSS → INS



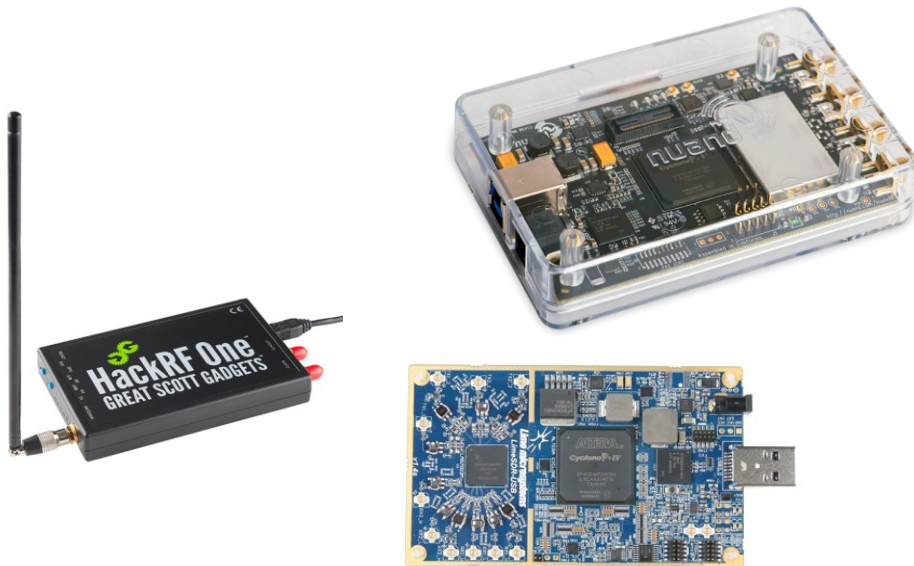
How can SPOOFING be done?

GNSS Spoofers (GPS Simulators):

\$

\$\$\$

SDR + Free Software



Portable Simulator



Highly Advanced Simulator



How can SPOOFING be detected?

SDR + Free Software



Portable Simulator



Highly Advanced Simulator



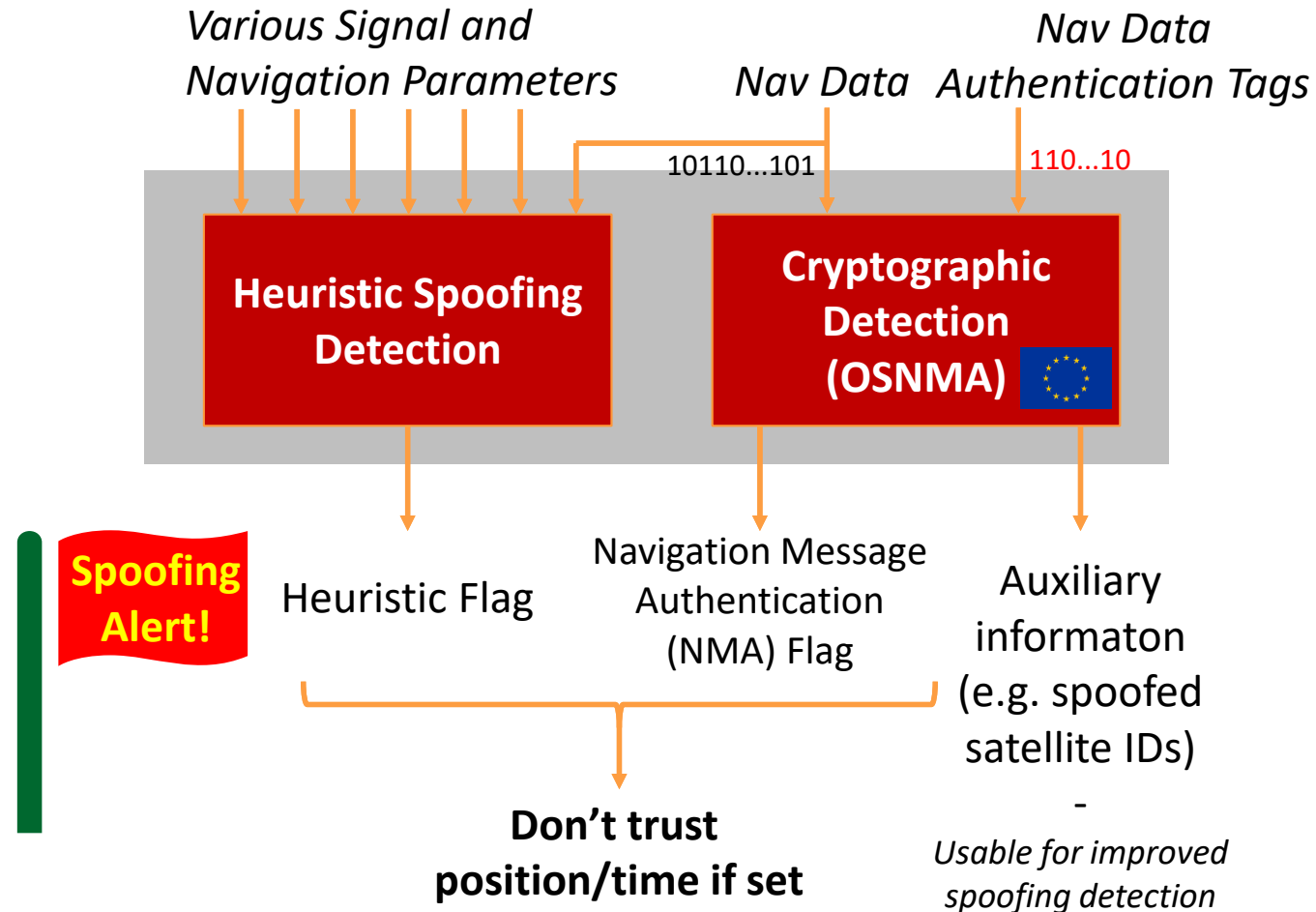
→ **Detect Signal Anomalies & Inconsistencies**

→ **Spoofing Flag**

But don't make it react on the real thing



Septentrio's Spoofing Detection Architecture



Easy OSNMA configuration on Septentrio GNSS & Galileo enabled receivers



TV101+_failingMacSeq_0000 - RxControl - S/N 3604546

File View Tools Logging Help

Position Information

Position Velocity

Geodetic ϕ : S 00°00'00,00005" σ_{ϕ} : +1,467m
WGS84/ITRS λ : W 000°00'00,00013" σ_{λ} : +1,757m
h: +0,019m σ_h : +4,924m

Satellite Status

GPS GLONASS Galileo BeiDou SBAS QZSS

E01 E02 E03 E04 E05 E06 E07 E08 E09
E13 E14 E15 E16 E17 E18 E19 E20 E21
E25 E26 E27 E28 E29 E30 E31 E32 E33

Search: 4 OG OR 3E OC 1S OJ OI Track: 9 OG OR
Sync: 0 OG OR 0E OC 0S OJ OI PVT: 8 OG OR

Receiver Status

Time RxClock DOP PL RAIM PVT

GNSS time frame PDOP: 2,53 Uptime:
vr 20-okt-2017 TDOP: 1,39 CPU Usi:
00:22:17,600 HDOP: 1,12 Through:
+18s offset to UTC VDOP: 2,27 Temp./A

SBF Status ExEvent ExSensor

Overview GNSS Communication Corrections NMEA/SBF Out Logging Admin

GNSS > OSNMA

OSNMA

Authenticating: OK

Galileo (Authentic: 10, Spoofed: 0)

OSNMA Configuration

OSNMA Mode ☐ off ☒ loose ☐ strict

NTP Client Configuration

Mode ☐ on ☒ off
Server default

Advanced Settings

OSNMA Configuration

Merkle Tree root 0E63F552C8021709043C23

OSNMA Public Keys

Key

Key0
Key1 MFkwEwYHKaZlZj0CAQYIK
Key2

OSNMA Status

Status	Authenticating
Trusted Time Delta	N/A
Trusted Time Source	N/A
Galileo Authentic Mask	0x124040E4A
GPS Active Mask	0x0
GPS Authentic Mask	0x0

Key from step 4b

Key from step 4a

Spoofing Detection



Receiver

mosaic-X5 S/N 3603240

IP Address: 0.0.0.0

Uptime: 0d 00:04:10

Position

Lat: N0°0'0.0000" 0.289m

Lon: E0°0'0.0008" 0.330m

Hgt: -0.439m 0.779m

Status

Tracked Sats: 23

Time: 2022-10-24 00:04:52

Temp: 37.00 °C

Standalone

Overall Quality

Corrections

OSNMA

Internal

Logging

Spoofing!

Overview

GNSS

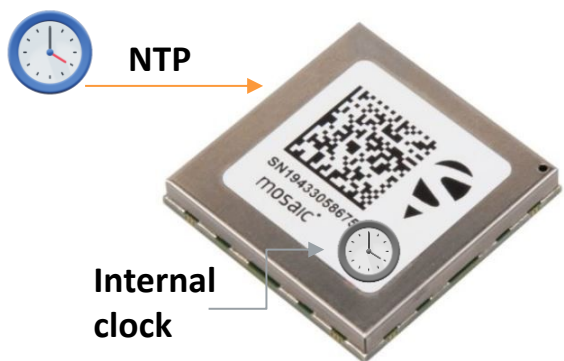
Communication

Corrections

NMEA/SBF Out

Logging

Admin



Authentication of GALILEO L1 Signal Failed!
Cryptographic method to authenticate navigation data
Network Time Protocol (NTP) for OSNMA time synchronization

Spoofing Detected with Heuristic Methods:
Waveform anomalies, navigation data anomalies, inconsistencies

OSNMA modes on mosaic

OSNMAmode = **off** :

- All PVT modes supported
- All constellations used
- All satellites used

OSNMAmode = **loose** :

- All PVT modes supported (standalone, SBAS, DGPS, RTK, PPP, ...)
- All constellations used
- Unauthentic satellites removed

OSNMAmode = **strict** :

- Most PVT modes supported (standalone, DGPS, RTK, ...)
- Galileo-only
- Only authentic satellites used

The screenshot displays the Septentrio software interface for a device labeled 'TV101+_failingMacSeq_0000 - RxControl - S/N 3604546'. The interface includes a menu bar (File, View, Tools, Logging, Help) and a toolbar with various icons. The main content area is divided into several sections:

- Position Information:** Shows geodetic and WGS84/ITRS coordinates with their respective standard deviations.
- Satellite Status:** Displays a grid of satellite status icons for various constellations (GPS, GLONASS, Galileo, BeiDou, SBAS, QZSS, NavIC, L-Band). The Galileo section is highlighted, showing satellites E04 through E36.
- Receiver Status:** Provides details about the receiver's search and sync status, including a table of DOP (PDOP, TDOP, HDOP, VDOP) and PL values.
- Receiver Information:** Lists receiver details such as 'mosaic-XS S/N 3058694', IP address, uptime, and position coordinates.
- Status Summary:** A table showing overall quality, corrections, and spectrum clean status.

The bottom of the interface features a navigation bar with tabs for Overview, GNSS, Communication, Corrections, NMEA/SBF Out, Logging, and Admin. The 'GNSS' tab is selected, showing the 'OSNMA' configuration page.

The screenshot shows the 'OSNMA' configuration and status page. The 'OSNMA Configuration' section includes a status indicator (a green checkmark) and a progress bar. Below this, the 'OSNMA Mode' is set to 'loose' (selected), with options for 'off' and 'strict'. The 'NTP Client Configuration' section shows the mode set to 'on' and the server address as '192.168.109.4'. The 'OSNMA Status' section displays the current status as 'Authenticating', along with various masks and time delta values.

Norway Jammertest

- **Advanced outdoor jamming & spoofing tests**
 - Very remote location avoids impact
 - Multi-constellation, multi-frequency spoofing!
 - Large variety of jamming and spoofing scenarios
- **Organized by Norwegian governmental agencies**



- **Participants:**
 - Authorities
 - Industry
 - Academia

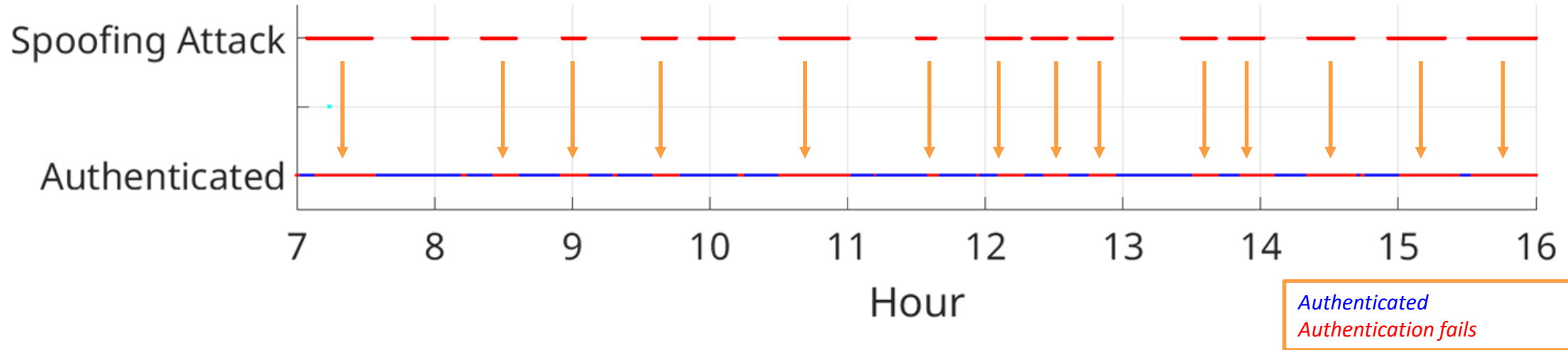


Norway Jamming Test: Time Spoofing

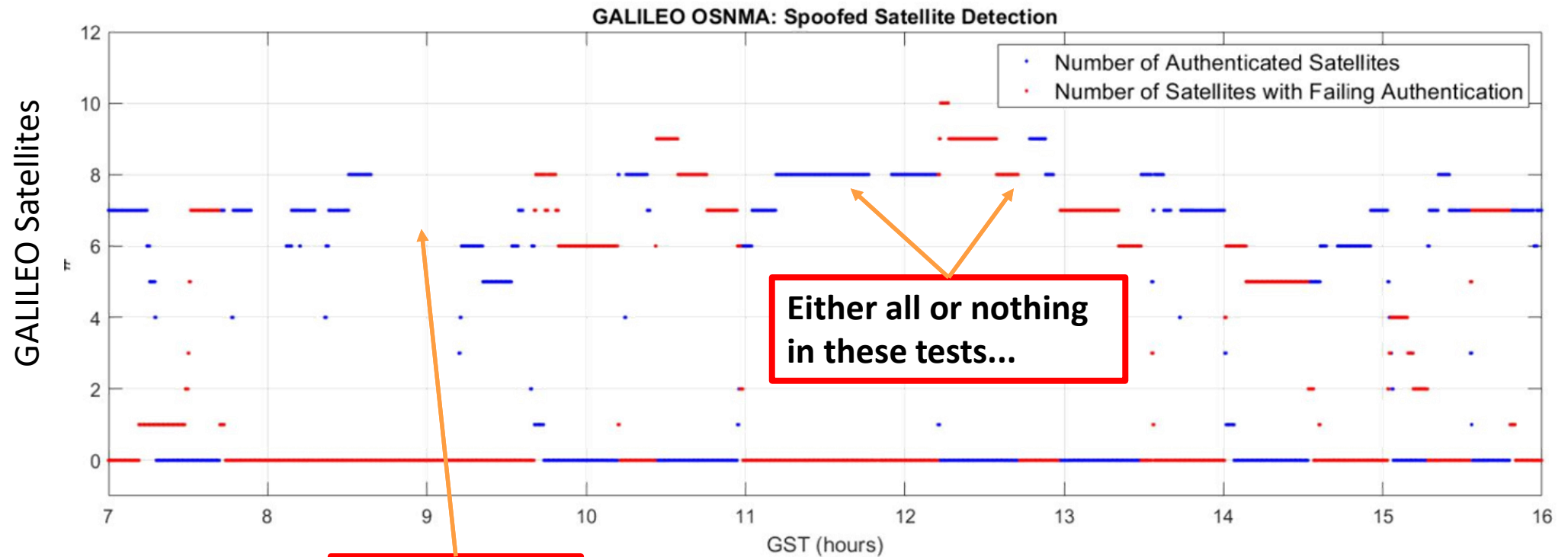
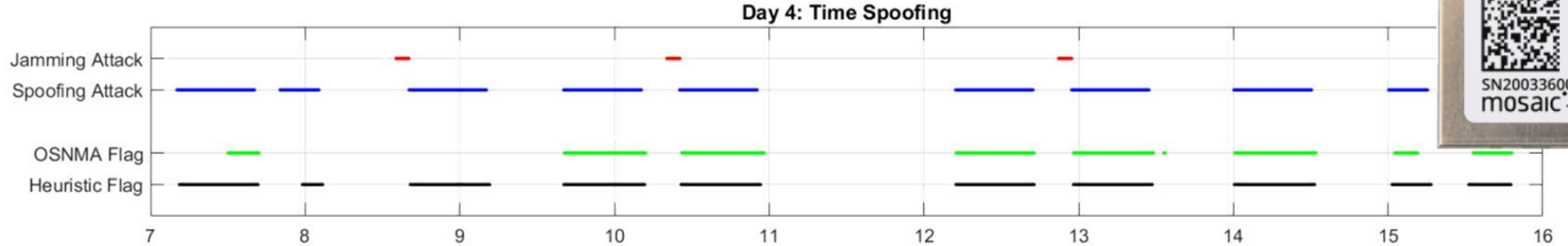
GALILEO Open Service Navigation Message Authentication (OSNMA):

As expected = Authentication fails during spoofing helping to properly notify end-user

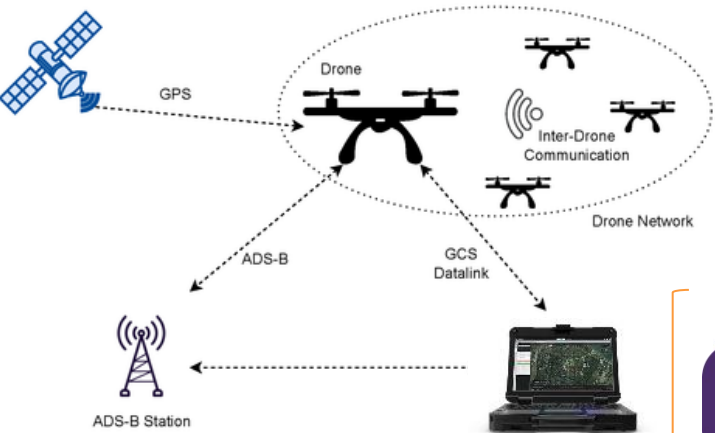
2024, Thursday (Time Spoofing)



Time Spoofing: Cryptographic Detection with OSNMA



Authentication (integration in Autopilots for UAV)



promoting & driving OSNMA integration within open-source autopilot ecosystems.

QGroundControl



Not Ready

GPS Authentication

Status Disabled

Shield Icon	n/a	Disabled	Unknown
	OK		
	Initializing		
	Failed		

MissionPlanner



Thomas suggested

Altitude (m) 0,00
Dist to WP (m) 0,00
GPS Status 0,00
Yaw (deg) 0,00
Yaw (deg) 0,00
Sat Count 0,00

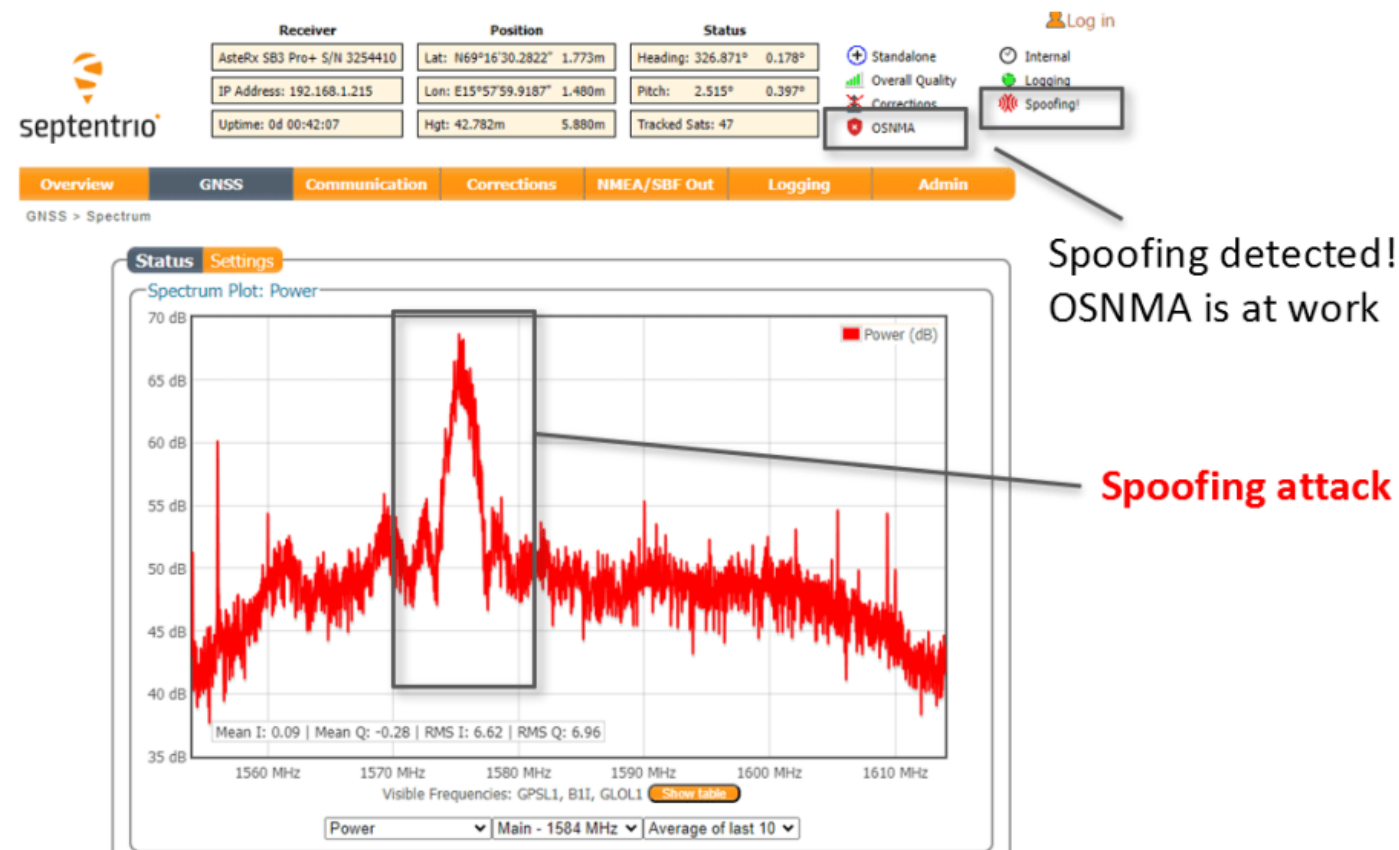
OSNMA status: 0 = disabled, 1 = initializing, 2 = error, 3 = fine

Authentic: yes

Gps authentication 0



Monitoring of GNSS jamming & Spoofing – in receiver



Conclusions

- OSNMA is an important step towards addressing security concerns in **different market applications**

Septentrio is **committed to resilient products**, making OSNMA a key milestone

OSNMA is now available in commercial Septentrio products

- Housed products, OEM boards, mosaic GNSS modules
- OSNMA is **being used** by customers in various industries (additional resilience)
- While OSNMA alone is not sufficient, it provides **a crucial additional layer of anti-spoofing** alongside heuristics and other techniques
- While Spoofing is an important threat, this one goes **often along jamming**
 - => GNSS equipment requires other protection mechanisms beyond pure OSNMA alone

Thank you



For questions contact: septentrio.com/contact

EMEA (HQ)

Greenhill Campus
Interleuvenlaan 15i,
3001 Leuven, **Belgium**

Espoo, **Finland**

Americas

2601 Airport Drive, Suite 360
Los Angeles (Torrance),
CA 90505, **USA**

septentrio.com/contact

Asia-Pacific

Shanghai, **China**
Yokohama, **Japan**
Seoul, **Korea**

septentrio.com

