NAVISP-EL2-170

STAGER – Sophisticated GNSS Threats Protection

Final Presentation

Contents

Company presentation

GMV

A global technology group

- Founded in **1984**
- Headquarters in **Madrid (Spain)**
- Over **3,000 employees**
- Engineering, development and integration of systems, software, hardware, specialized products and services
- **Sectors:** Aeronautics, Space, Defense & Security, Cybersecurity, Intelligent Transport Systems, Healthcare, Banking & finances, and ICT industries

Mission

Our goal is to support our client's processes by dint of technologically advanced solutions, providing integrated systems, specialized products, and services covering the whole life cycle

AES (Aeronautical Systems) Division

- **GNSS interference (jamming and spoofing) detection** and **localization** solutions
- Provision of GNSS performance prediction services required to support the planning of operations (e.g., **AUGUR** service for EUROCONTROL)
- Improvement of ANSP's operational cost-effectiveness through the implementation of services (e.g., **ADS-B performance monitoring**)

Products

MagicIFP

Web application for validating GNSS-based performance-based navigation (PBN) procedures

SRX-10i

GNSS spectrum monitoring to protect what's most valuable

EMIL

Advanced ground- and UAS-based ILS/VOR inspection

Motivation

Motivation

RFI threat: beyond the military use case

GNSS RFI can affect both **civil** and military users and poses a particularly serious threat to **safety-critical applications**

A general-audience debate

The steady rise in RFI events has prompted **public awareness** of the topic

This demands the development of **solutions** to counteract their effects

Current solutions

RFI monitoring systems with:

- Specific hardware for the digital signal processing
- Third-party IP cores on-board these logic units
- Custom-built RF components

❑ Increased **costs**

❑ Longer **development cycles**

❑ Limitation in **scalability**, **customization** and **modernization**

BBC

EU chief von der Leyen's plane hit by suspected Russian GPS jamming

1 September 2025

Share Save

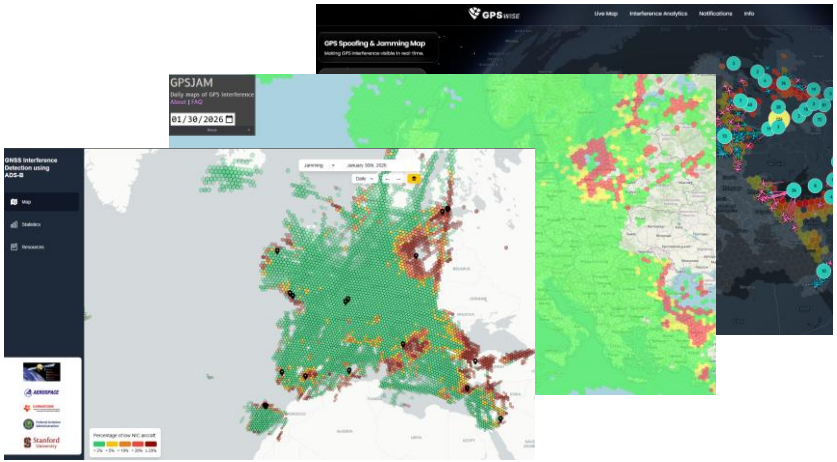
Maia Davies & Will Vernon

BBC News

THE TIMES

Russia 'putting all ships at risk' by jamming navigation systems

The UK and other countries have called for maritime bodies to recognise the threat to safe navigation of GPS jamming and position spoofing



Source: rfi.stanford.edu, gpsjam.org and gpswise.aero

Source: ENAIRE, OHB, Indra

Case study: aviation

Safety first

- Highest levels of **operational safety** ensured by International Civil Aviation Organization (ICAO) recommendations and regulations
- **Performance Based Navigation (PBN)** to utilize GNSS in air navigation operations with different levels of spacing and performance
- **EC Implementing Regulation 2018/1048** (July 2018): providers of ANS to have **contingency measures** to ensure services continuity

+20

FIR regions with jamming or spoofing

Source: EASA SIB No. 2022-02R2

1500

flights per day spoofed in Q3 2024

Source: OPSGROUP – GPS Spoofing Final Report 2024

38.5%

European en route traffic operates through regions affected by RFI

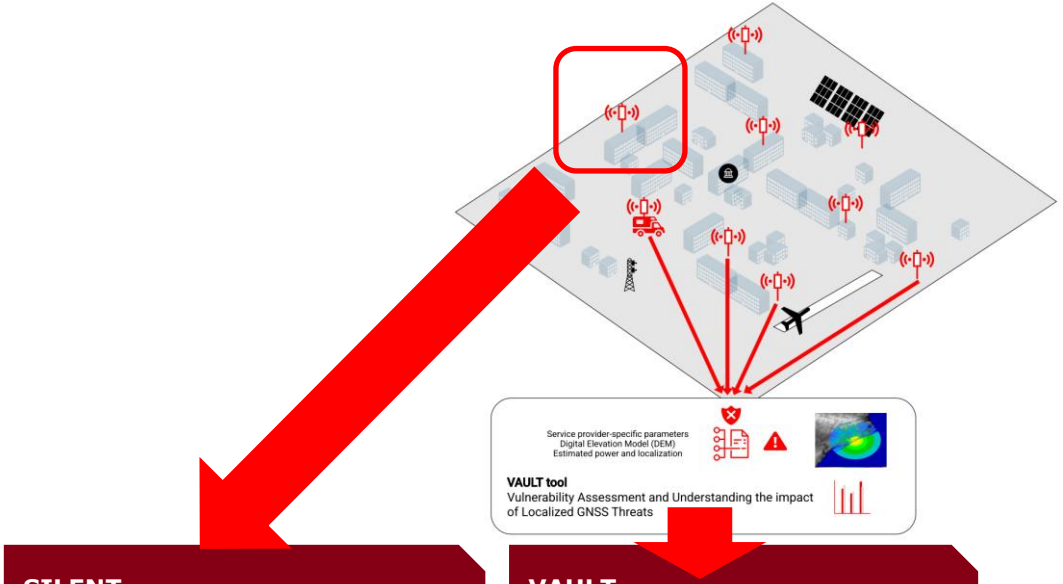
Source: EUROCONTROL – Think Paper #9 (2021)

Project objectives

STAGER: Sophisticated GNSS Threats Protection

- To implement a **cost-effective**, **COTS-based** GNSS RFI monitoring solution intended to be deployed **densely** around **critical infrastructure**
- Two-fold approach:
  - ❑ **SILENT nodes:** sensing nodes (**permanent** installation or **portable**) with a low SWaP for early detection of RFI
  - ❑ **VAULT tool:** server-side application that:
    - ❑ Quantifies **afflicted service volume,** and
    - ❑ Implements **AI** methods to enhance the detection and characterization of RFI
- **Validation** of the end-to-end technology in a relevant environment
- **Involvement** of ENAIRE, an important stakeholder to plan the operational development of the solution

ENAIRE



SILENT
Spoofing Identification and Localization for Enhanced Navigation and Timing

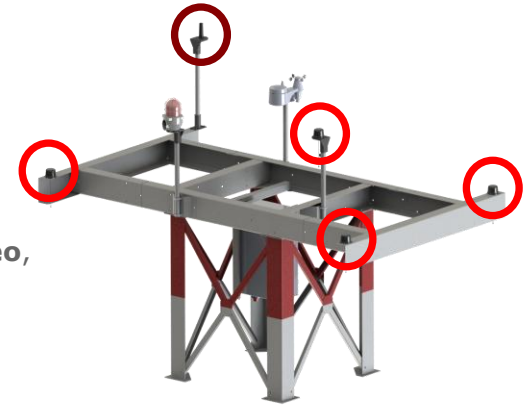
VAULT
Vulnerability Assessment and Understanding the impact of Localized GNSS Threats

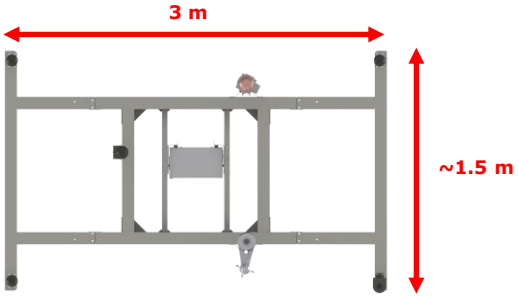
SILENT and VAULT Product Concepts

SILENT

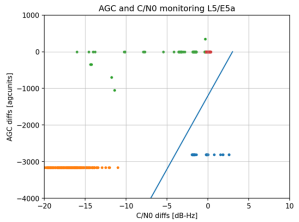
Spoofing Identification and Localization for Enhanced Navigation and Timing

- **COTS** GNSS receivers (u-blox F9P) and antennas
- GNSS monitoring of civilian signals from **GPS**, **Galileo**, **GLONASS**, **BeiDou** and **QZSS**
- **Permanent installation** or **portable**
- **Multilayered** jamming and spoofing detection
- **Angle of arrival determination**
- **Spectrum monitoring:** Wideband (1-2 GHz) and in-band (for L1/E1 and L5/E5)

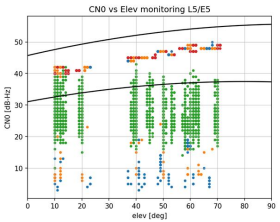




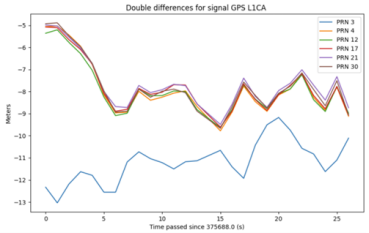
AGC vs C/N0



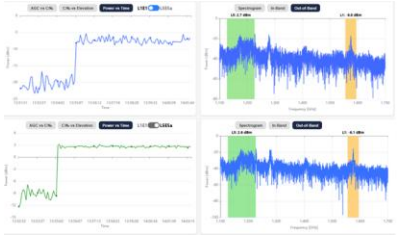
C/N0 vs elevation



Dispersion of double differences



RF spectrum monitoring



SILENT

AGC vs C/N0

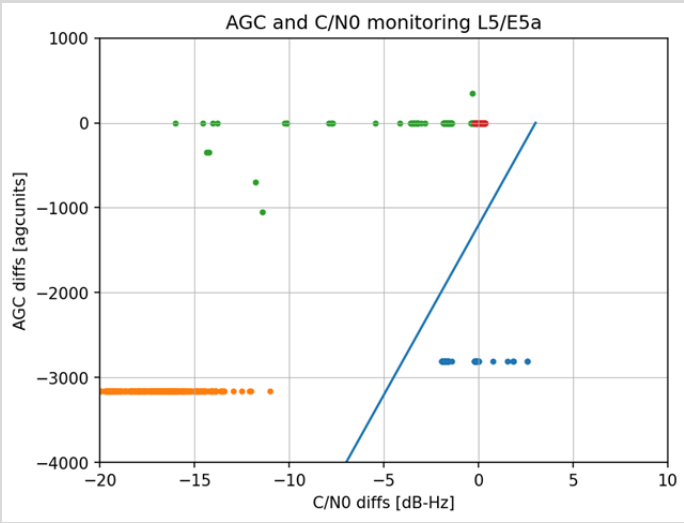
- **Inputs**
- ❑ Average AGC during nominal period
- ❑ Average C/N0 of all satellites and epochs during nominal period
- ❑ Difference between received epochs and average values, for AGC and C/N0:

$$\Delta AGC = AGC - \overline{AGC}$$
$$\Delta C/N_{0,mean} = C/N_{0,mean} - \overline{C/N}_{0,mean}$$

- ❑ Parametrization of the decision line to determine the spoofing region (X axis intercept and slope)
- ❑ Spoofing decision is taken if the (AGC, C/N0,mean) is to the right of the decision line:

$$\Delta AGC < (\Delta C/N_{0,mean} - Line_{C/N_{0,mean}}) \cdot Line_{slope}$$

- ❑ Requires calibration during absence of RFI (nominal)



Jamming (orange), spoofing (blue), nominal before/after test (red/green)

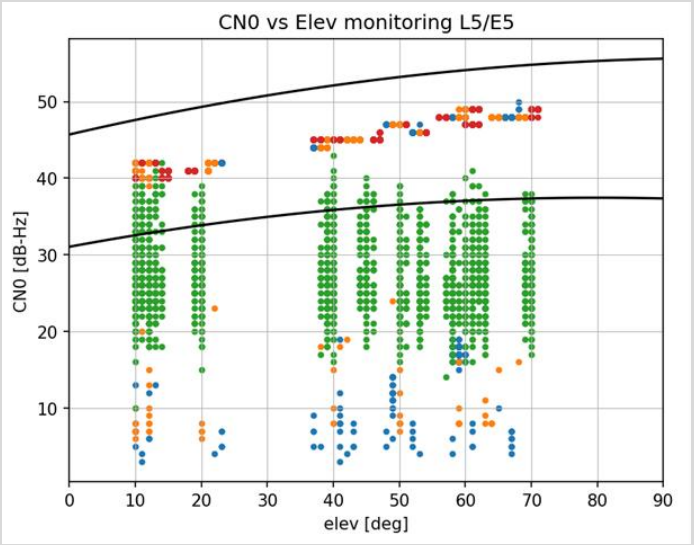
SILENT

C/N0 vs Elevation

▪ Parametrization of upper and lower quadratic curves to de determine the jamming region

$$C/N_{0,up} = a_{0,up} + a_{1,up} el_t + a_{2,up} el_t^2$$
$$C/N_{0,down} = a_{0,down} + a_{1,down} el_t + a_{2,down} el_t^2$$

- a0 is the C/N0 when elevation = 0 deg (vertical offset)
- a1 is the linear term that controls the variation of C/N0 over satellite elevation (slope and horizontal shift)
- a2 defines the curvature and opening
- Requires calibration during absence of RFI (nominal)

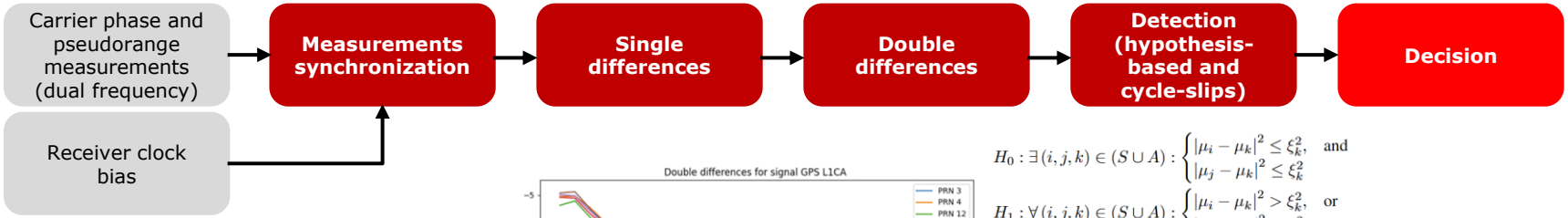


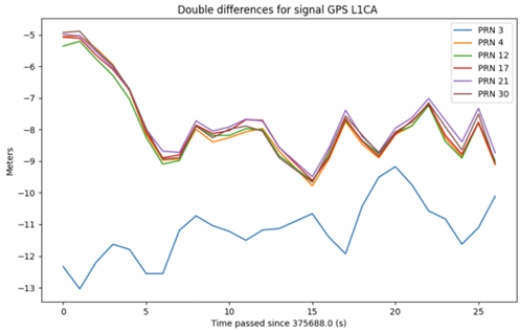
Jamming (green), spoofing (orange) and nominal before/after test (red/blue)

SILENT

Spoofing Identification and Localization for Enhanced Navigation and Timing

Spoofing Detection





Dispersion of double differences (DDs) during a spoofing attack. Grouped DDs indicate single transmitting source (spoofer)

$$H_0 : \exists\,(i,j,k) \in (S \cup A) : \begin{cases} |\mu_i - \mu_k|^2 \le \xi_k^2, & \text{and} \\ |\mu_j - \mu_k|^2 \le \xi_k^2 \end{cases}$$

$$H_1 : \forall\,(i,j,k) \in (S \cup A) : \begin{cases} |\mu_i - \mu_k|^2 > \xi_k^2, & \text{or} \\ |\mu_j - \mu_k|^2 > \xi_k^2 \end{cases}$$

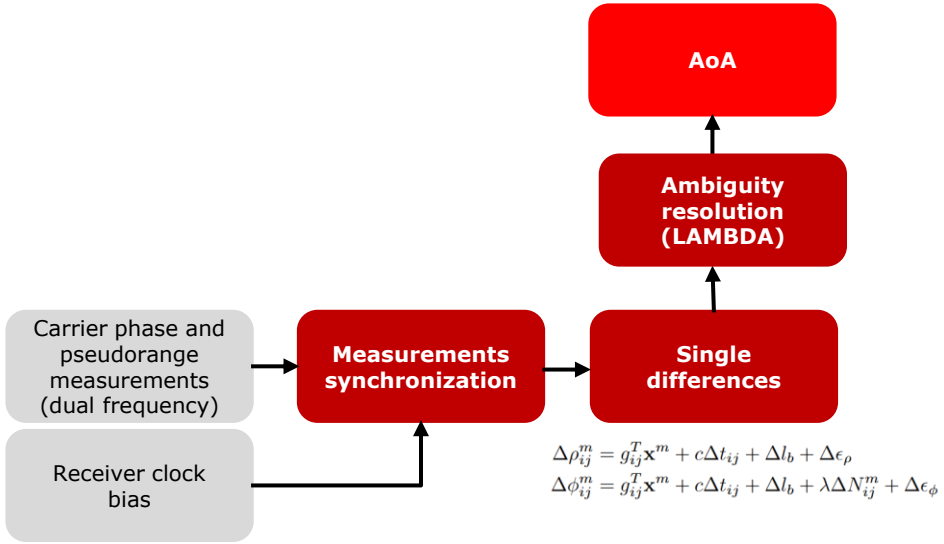
Decision for baseline 2:

svId	Decisions
7	False
8	False
13	True
14	True
17	True
22	False
30	True
21	False

SILENT

Spoofing Identification and Localization for Enhanced Navigation and Timing

Angle-of-arrival estimation



VAULT

Vulnerability Assessment and Understanding the impact of Localized GNSS Threats

- **Server-side** application
- SILENT nodes **configuration:** view and modify
- Stores and processes information from all SILENT nodes
- RFI detailed analysis:

❑ **RFI classification (jamming or spoofing)** using **AI/ML** and **C/N0 with proxies** (e.g., AGC)

❑ **Geolocation**

❑ **Afflicted airspace**

- Internal SW architecture divided into **modules**
- **Publisher-subscriber** paradigm between SILENT and VAULT, and between VAULT modules:

❑ Information is published

❑ Modules subscribe to topics

❑ **Scalability and modularity** for better reuse

VAULT
Vulnerability Assessment and Understanding the impact of Localized GNSS Threats

RFI classification using AI

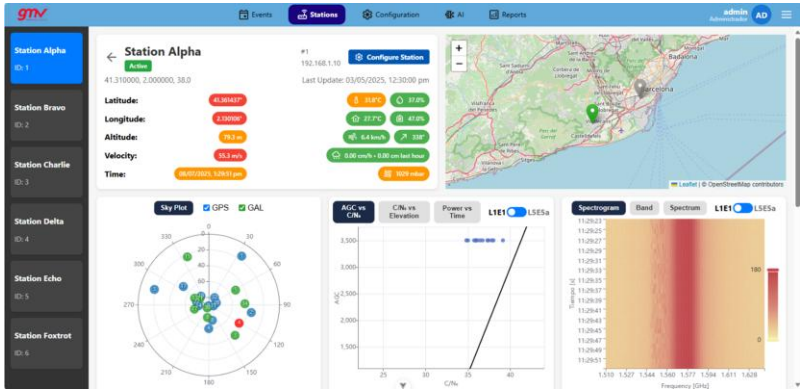
Jamming detection using SVM
Spoofing detection using VAE

Geolocation

Modified PDOA + angle-of-arrival information fusion

Afflicted service volume

RF propagation using DEM

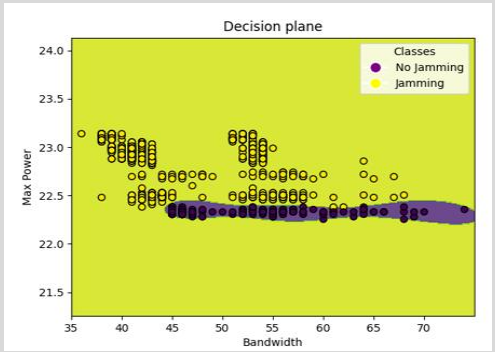


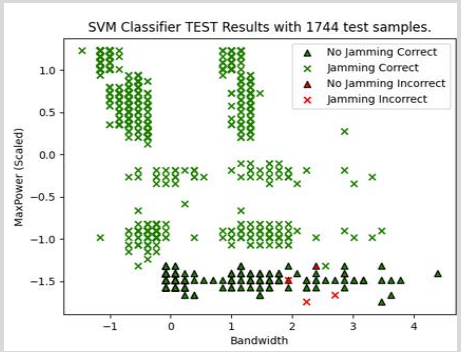
VAULT

RFI classification using AI

- Jamming detection using **Support Vector Machine (SVM)**

SVM

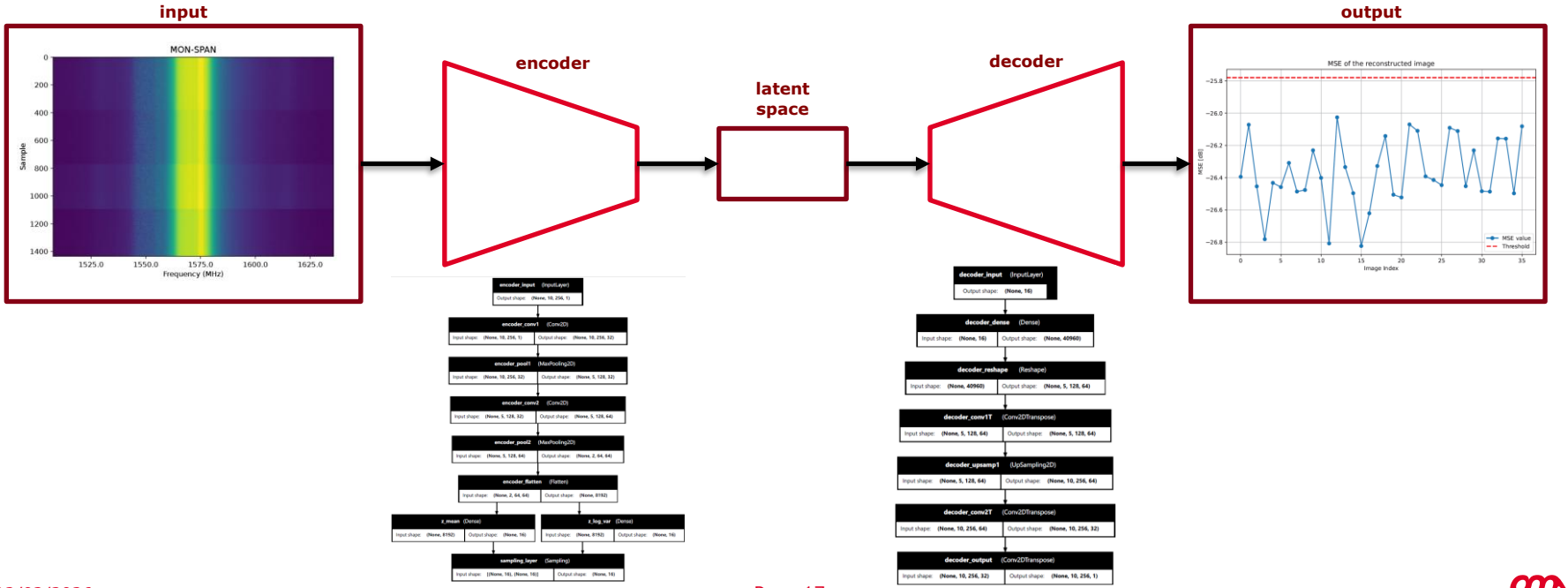




VAULT

RFI classification using AI

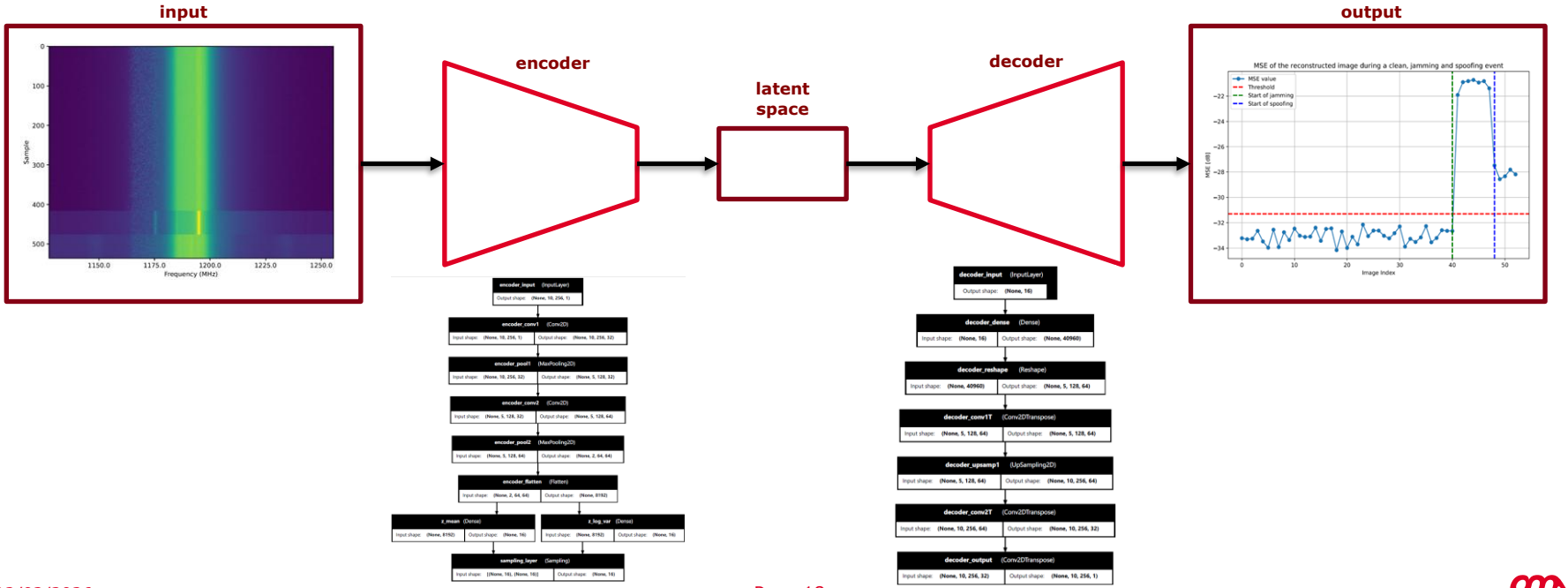
- Spoofing detection using **Variational Autoencoder (VAE)**



VAULT

RFI classification using AI

- Spoofing detection using **Variational Autoencoder (VAE)**

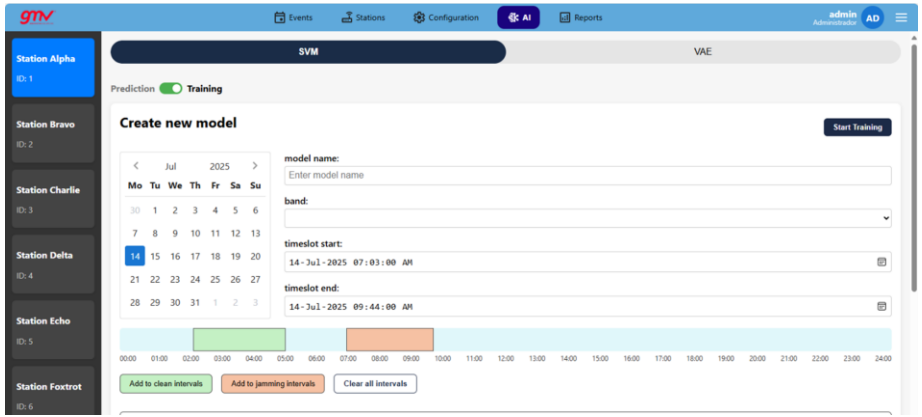


VAULT

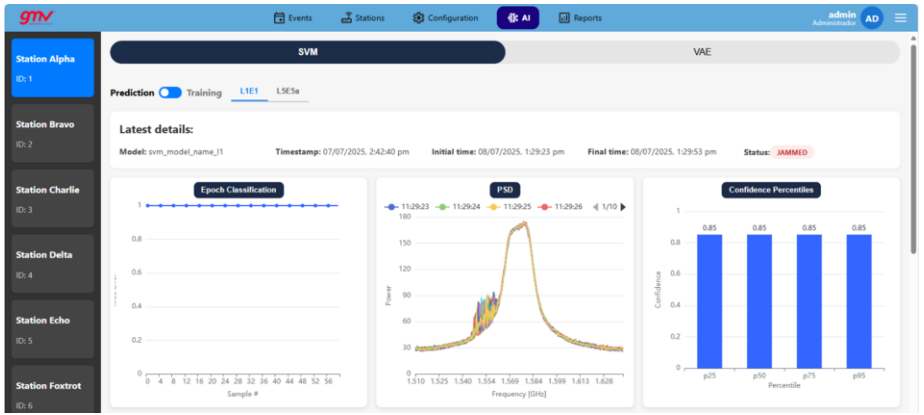
RFI classification using AI

- Interface that allows:
  - ❑ **Training** of different **models** on stored data
  - ❑ Choose which model to apply
  - ❑ Check results on incoming data **(real-time prediction)**

GUI: new model training



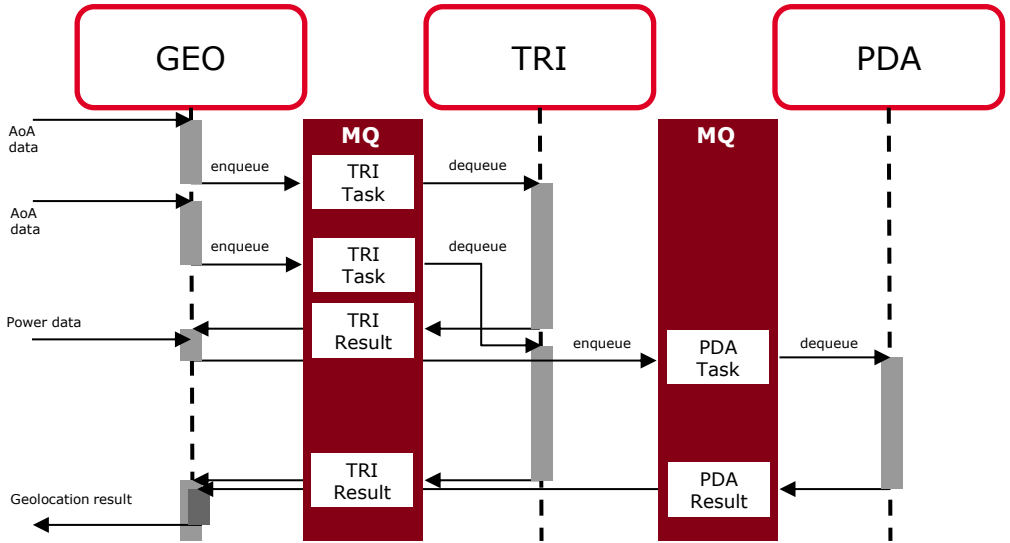
GUI: prediction output



VAULT

Geolocation

- Three modules:
  - **TRI:** Triangulation using Angle Of Arrival algorithm
  - **PDA:** Precise estimation using Power Difference Of Arrival algorithm
  - **GEO:** Orchestrator

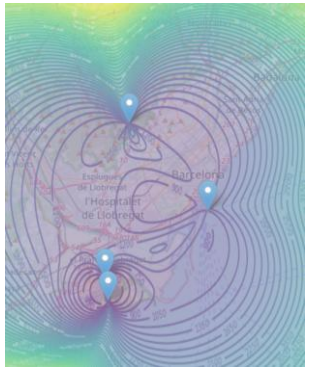


VAULT

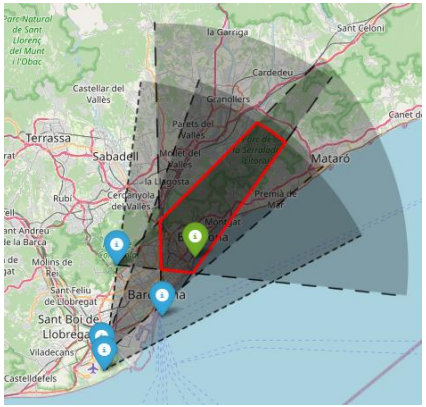
Geolocation

- **AoA measures** are used to determine a **polygon** that must contain the interference source
- **Power measures** are used to compute difference of arrival between nodes and possible source locations
- A modified approach using **attenuation maps** based on terrain DEM instead of FSPL for propagation

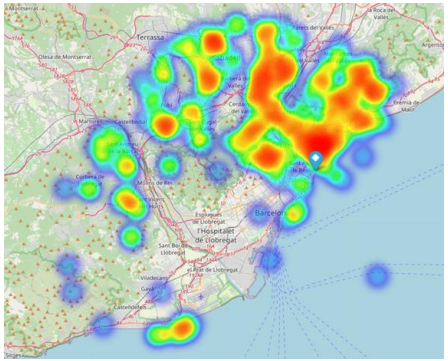
- **Validation** via simulations including GDOP calculation (for AoA only) for optimal deployment configuration



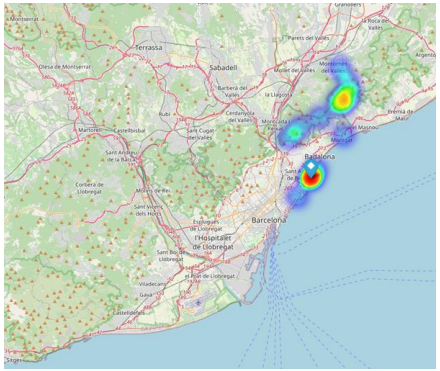
AoA result



PDA result



Combined result



VAULT
Vulnerability Assessment and Understanding the impact of Localized GNSS Threats

RFI classification using AI

Geolocation

Afflicted service volume

VAULT

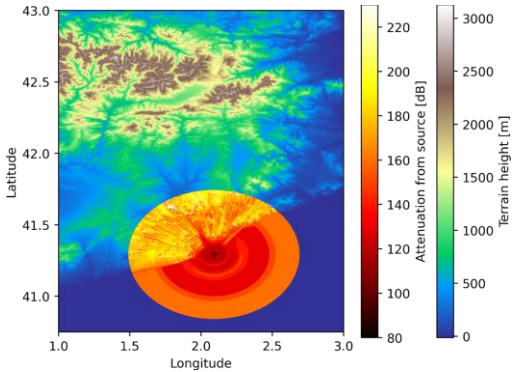
Afflicted service volume

- Combines
  - ❑ Position obtained from **geolocation**
  - ❑ **Digital Elevation Model** (DEM) of the area

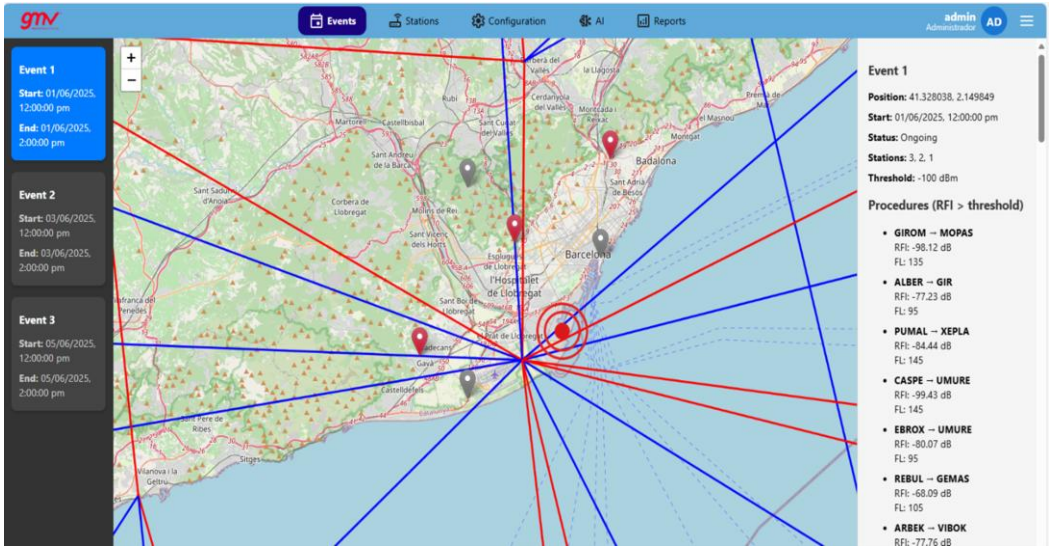
- Computes afflicted service volume using **ITWOM** 3.0 RF propagation

- Evaluates maximum radiation affecting flight procedures

Digital Elevation Model



Afflicted procedures



Validation

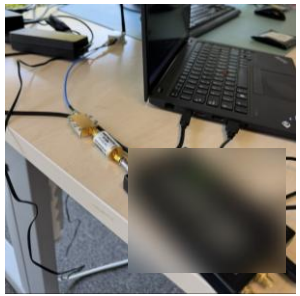
Validation

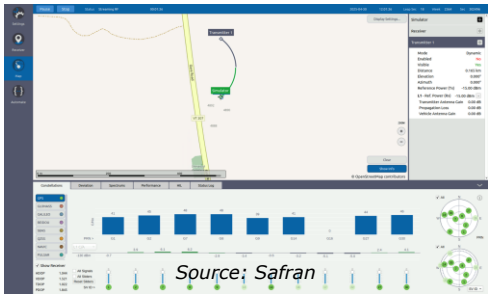
Phase I: Lab tests

SW module-level tests using simulated jamming and spoofing datasets

Phase II: Open air tests

Jammertest 2025 test campaign





Source: Safran

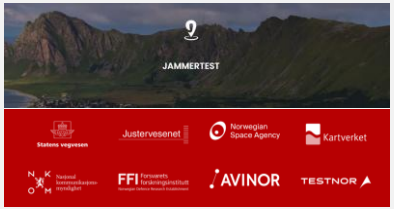
Jammertest 2025 – Figures

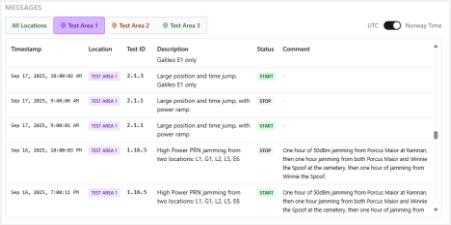
15-19
September 2025

+400
participants

+50
planned tests of jamming, spoofing and meaconing along the week in Test Area 1 (from 09:00-22:00)

Source: Testnor





Source: jammertest.no

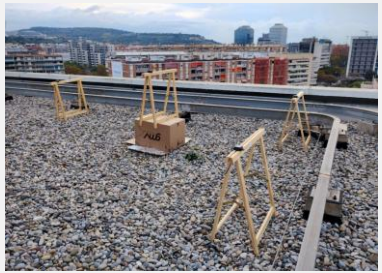
Validation

Phase I: Lab tests

Phase II: Open air tests

Setups

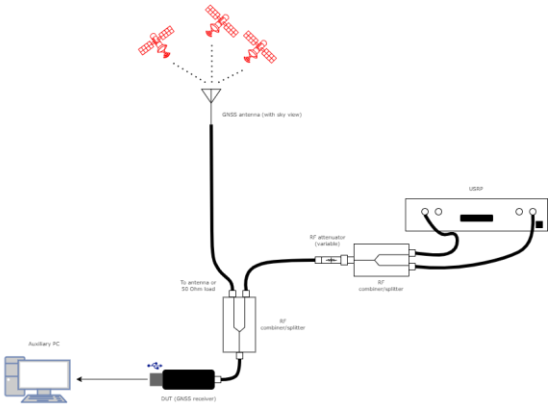
- **Signal-in-space only**
  - ❑ **Detection** characterization in terms of Pfa
  - ❑ **Angle-of-arrival estimation** for different azimuth and elevation angles



File	Receiver body-fixed frame coordinates [m]
COM4___9600_241112_091448.ubx	(0.0, 0.0, 0.0)
COM6___9600_241112_091448.ubx	(4.5, 0.0, 0.0)
COM5___9600_241112_091459.ubx	(0.0, -2.4, 0.0)
COM7___9600_241112_091458.ubx	(1.667, -0.833, 0.350)

Authentic recorded signal with u-blox receivers and their body-fixed frame coordinates

- **Simulated spoofing scenario (Skydel)**
  - ❑ **Detection** characterization in terms of Pmd and Pfa
  - ❑ **Angle-of-arrival estimation**



Parameter	Value
Constellations	GPS+Galileo
Bands	L1/L5 + E1/E5a
Spoofed PRN	13, 14, 22
Reference power	Default
Simulation start time and date	23/02/2024 18:30:00 UTC
Sampling	25 Msps, 16 bits
Duration	180 s
Simulated lat/lon/h	45.0000º, -73.0000º, 2.0 m

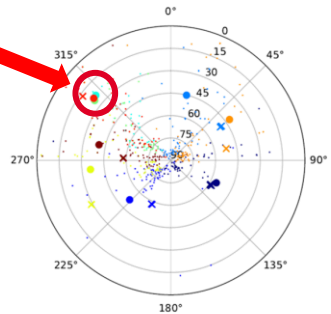
Validation

Results

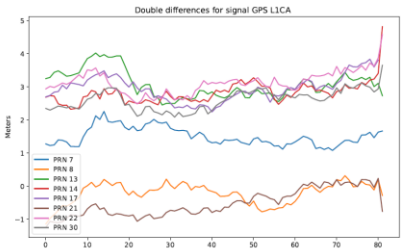
- Spoofing **detection**
  - ❑ **M-over-N** over three baselines
  - ❑ **Dual-frequency** (L1 and L5)
  - ❑ PRNs 13, 14 and 22 correctly identified as spoofed
  - ❑ PRN 30 and 17 wrongly detected due to very close double differences

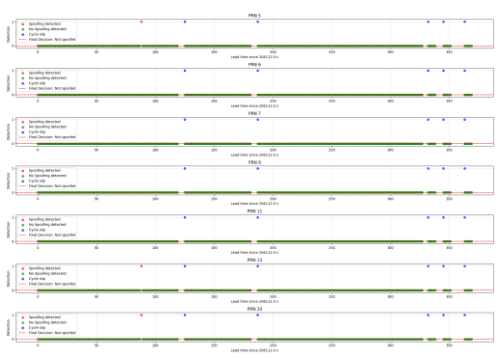
- Spoofing **localization**
  - ❑ Three modes: **2D, 2.5D** and **3D**
  - ❑ Actual constellation (NAVSAT) vs estimated AoA
  - ❑ **Grouped PRNs** indicate single source (simulated spoofer location)

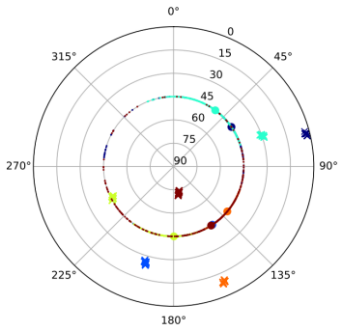
	Azimuth	Elevation
Error (°)	<5	<17



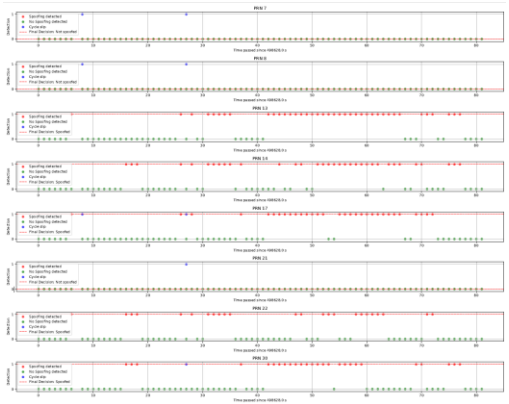
3D mode (azimuth + elevation, L1+L5)







2.5D mode (azimuth only, L1+L5) – Signal-in-space signal only



Validation

Phase I: Lab tests

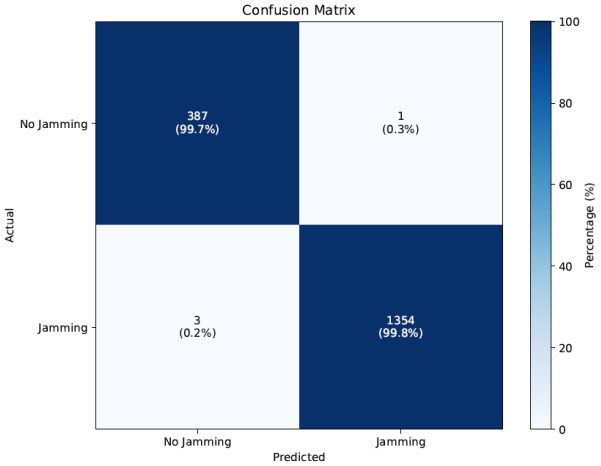
Phase II: Open air tests

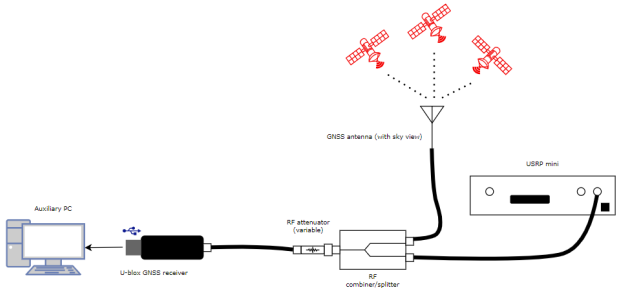
Results (continued) – AI methods

- **Signal-in-space only**

- **Jamming scenario**
  - ❑ Clean signal mixed with conducted interference signal transmitted using an USRP B205mini

- ❑ **Confusion matrix** to check the probability of false alarm (Pfa) and miss detection Pmd





Clean dataset					
U-blox file	**Duration (minutes)**	**Jammer Type**	**Jammer Gain (dB)**	**Jammer Center frequency (MHz)**	**Jammer Bandwidth (MHz)**
COM6___9600_241125_075453.ubx	30	-	-	-	-
Jamming dataset					
U-blox file	**Duration (minutes)**	**Jammer Type**	**Jammer Gain (dB)**	**Jammer Center frequency (MHz)**	**Jammer Bandwidth (MHz)**
COM6___9600_241125_083055_L1_sine_6db.ubx	30	CW	6	1575.42	-
COM6___9600_241125_090049_L1_sine_12db.ubx	30	CW	12	1575.42	-
COM6___9600_241125_090049_L1_gauss_12db.ubx	30	GWN	12	1575.42	2 MHz
COM6___9600_241125_090049_L1_sweep_12db.ubx	30	Chirp	12	1575.42	2 MHz

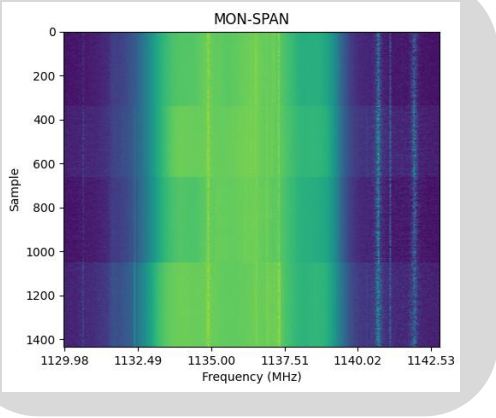
Clean dataset					
U-blox file	**Duration (minutes)**	**Jammer type**	**Jammer gain (dB)**	**Jammer centre frequency (MHz)**	**Jammer bandwidth (MHz)**
COM6___9600_241125_075453.ubx	30	-	-	-	-
Jamming dataset					
U-blox file	**Duration (minutes)**	**Jammer type**	**Jammer gain (dB)**	**Jammer centre frequency (MHz)**	**Jammer bandwidth (MHz)**
COM6___9600_241125_083055_L5_sine_6db.ubx	30	CW	6	1176.45	-
COM6___9600_241125_083055_L5_sine_12db.ubx	30	CW	12	1176.45	-
COM6___9600_241125_090049_L5_sweep_12db.ubx	30	Chirp	12	1176.45	2 MHz

Validation

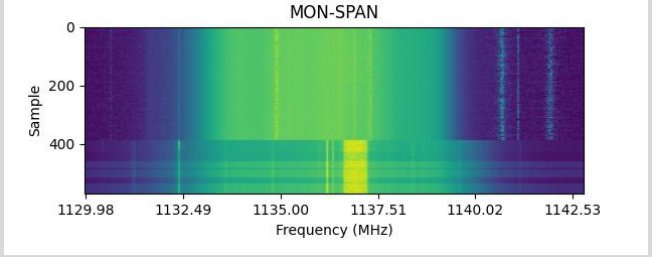
Results (continued) – AI methods

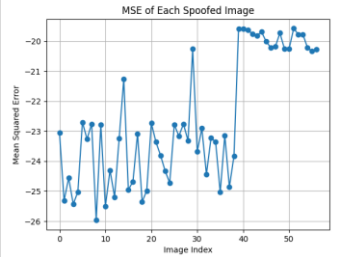
- **Signal-in-space only**
  - ❑ Concatenation of data from 4 receivers
- **Prediction dataset is clean data followed by spoofing samples**
- **Algorithm training**
  - ❑ The VAE model performs anomaly detection by calculating the mean squared error (MSE for each reconstructed image, marking as "anomaly" the images where MSE>threshold)
  - ❑ The threshold is the mean MSE plus its standard deviation:

$$\text{Threshold} = \mu_{\text{MSE}} + \gamma\,\sigma_{\text{MSE}}$$



Training spectrogram with clean-only samples





Prediction spectrogram and computed MSE for each image.

Validation

Results (continued)
Jammertest 2025

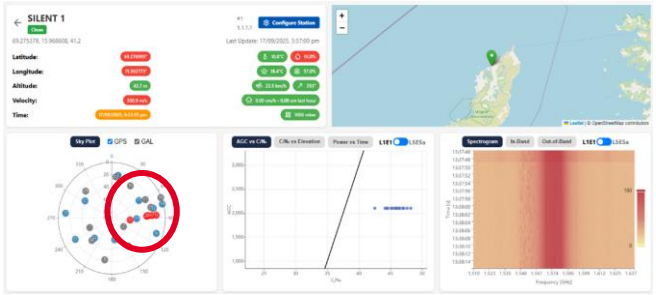
- **Setup**
  - ❑ 1 fully assembled SILENT node
  - ❑ 1 minimal functioning SILENT node
  - ❑ Deployed SW working in **real-time**

- **Spoofing scenario**
  - ❑ Spoofed signals, ranging in several complexity types, were radiated from the antenna mounted at the top of the black crane

- **Spoofing detection and localization**
  - ❑ VAULT panel correctly marked the spoofed SVs in red, showing the estimated AoA in the skyplot
  - ❑ Good performance in azimuth, poor performance in elevation
  - ❑ Combining multiple AoA snapshots with PDOA between SILENT nodes, the position of the source is estimated

Fully assembled SILENT 1 (with spoofer located in the NE)

Minimal functional SILENT 2



VAULT: SILENT 1 panel. Skyplot correctly indicating source position NE and 20-30º in elevation.

	Geolocation (Haversine distance in km)
Best	0.5
Worst	11.81
Mean	3.5

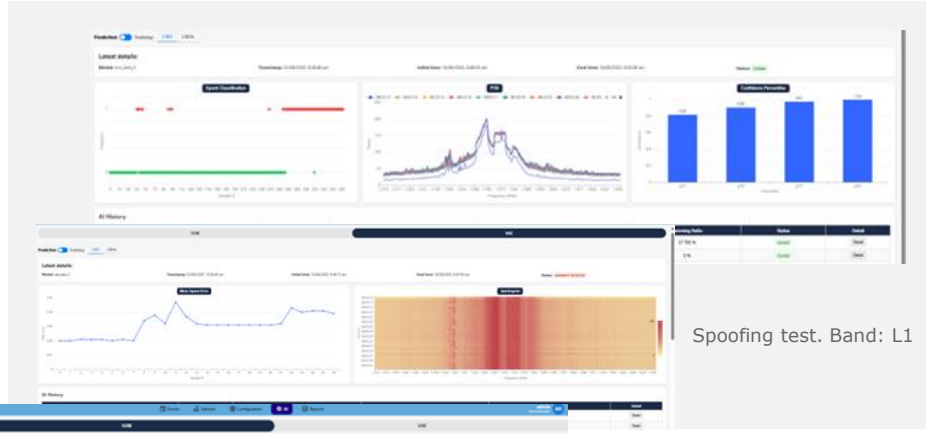
Position localization using joint triangulation and PDOA from SILENT 1 and 2.

Validation

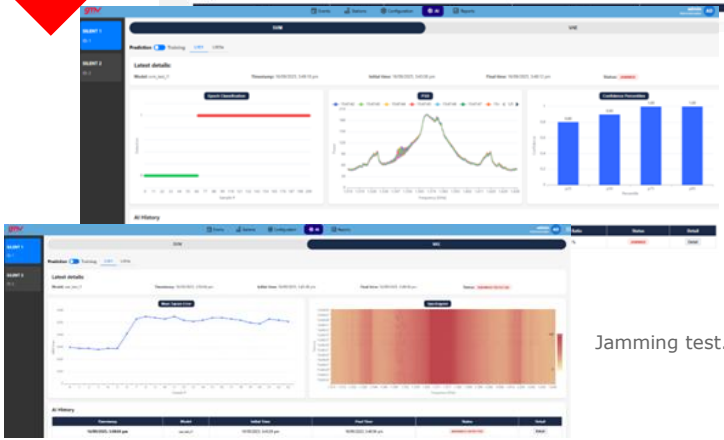
Results (continued) – Jammertest 2025

- **Spoofing detection**
  - ❑ SVM was triggered by the start of a spoofing event (in red)
  - ❑ VAE correctly notified the transition from clean to spoofing periods (rise in MSE values)

- **Jamming detection**
  - ❑ SVM perfectly differentiated between clean and jammed intervals
  - ❑ VAE MSE values were also incremented at the start of the jamming event



Spoofing test. Band: L1

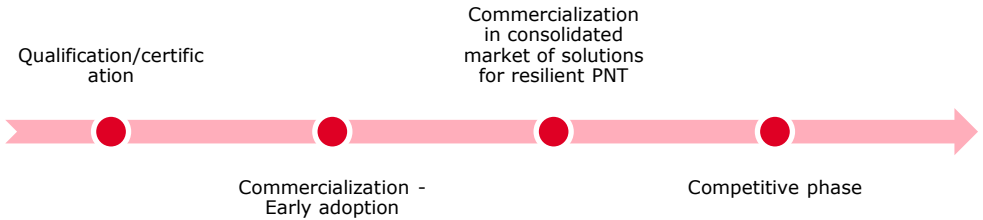


Jamming test. Band: L1

Conclusions and future product roadmap

Conclusions and future product roadmap

- COTS-based RFI monitoring solution with remarkable good performance for **cost-effective**, **dense** deployments
- Promising AI methods performance in real-time with **retraining capabilities** by the operator
- **Multi-layered RFI detection** (C/N0 vs elevation, AGC vs C/N0, dispersion of double differences, cycle slips)
- **TRL7** achieved



Market	Segment(s)	Applicability of SILENT and VAULT
Aviation	ANSPs, U-Space	Provision of PNT, EGNSS implementation for UAVs
Maritime	Port authorities	Assisted docking, SAR protection/integrity
Telecoms	Service providers	Synchronization of e.g., 5G networks
Automotive	Road authorities	Automated driving
Energy grid	Transport companies	Smart grid synchronization
Finance	Markets authorities	Synchronization (interoperability)
Governmental	Spectrum agencies, state law enforcement	GOVSATCOM resilience, spectrum protection

Acknowledgements

This **STAGER – Sophisticated GNSS Threat Protection** activity has been carried out under the **NAVISP** program of the **European Space Agency (ESA)**

ENAIRE

TESTNOR

Thank you

stager@gmv.com

INNOVATING SOLUTIONS

SILENT

Spoofing Identification and Localization for Enhanced Navigation and Timing

Augmented decision

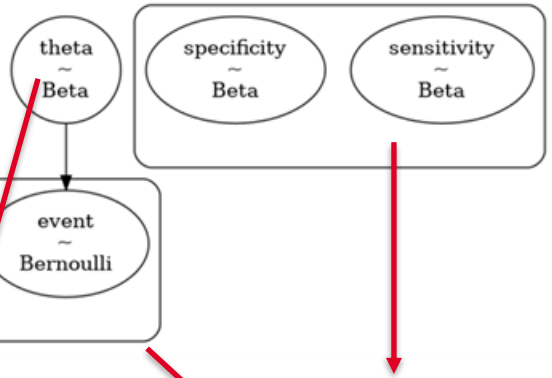
```
# Simulated outputs from 2 models (1 = event predicted, 0 = no event)
model_outputs = []
for _ in np.arange(2):
    actual, predicted = generate_labels(N=, prevalence=0.9, sensitivity=0.75, specificity=0.8)
    model_outputs.append(predicted)
```

```
(.venv) stager-mgga@stager-mgga:~/workspace/STAGER$ /home/stager-mgga/workspace/STAGER/.venv/bin/python /home/stager-mgga/workspace/STAGER/exp/hierarchical_model.py
Multiprocess sampling (4 chains in 2 jobs)
CompoundStep
>NUTS: [theta, sensitivity, specificity]
>BinaryGibbsMetropolis: [event]
```

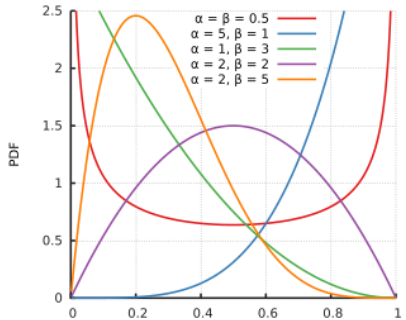
Progress	Draws	Divergences	Step size	Grad evals	Sampling Speed	Elapsed	Remaining
	11000	0	0.28	15	679.28 draws/s	0:00:16	0:00:00
	11000	0	0.21	7	653.18 draws/s	0:00:16	0:00:00
	11000	0	0.18	31	322.26 draws/s	0:00:34	0:00:00
	11000	0	0.18	7	321.83 draws/s	0:00:34	0:00:00

```
Sampling 4 chains for 1_000 tune and 10_000 draw iterations (4_000 + 40_000 draws total) took 34 seconds.
Posterior P(event is true | outputs) = 0.721
```

	mean	sd	hdi_3%	hdi_97%	mcse_mean	mcse_sd	ess_bulk	ess_tail	r_hat
theta	0.714	.232	0.283	1.000	0.006	0.005	1542.0	1729.0	1.0
sensitivity[0]	0.721	.109	0.532	0.937	0.001	0.001	8030.0	9528.0	1.0
sensitivity[1]	0.697	.113	0.499	0.920	0.001	0.001	6333.0	6907.0	1.0
specificity[0]	0.667	.164	0.376	0.952	0.002	0.001	5109.0	13354.0	1.0
specificity[1]	0.679	.157	0.397	0.956	0.002	0.001	6111.0	13312.0	1.0



Prior on the prevalence of a spoofing attack as a Beta distributed function



Specificity and **sensitivity priors**

Sensitivity = P(detection true | spoofing)

Specificity = P(detection false | no spoofing)

Spoofing attack per epoch as a **Bernoulli** distributed events (30 seconds) with parameter theta (prevalence) as a hyperparameter

Validation

Setups