Block-box

NAVISP-EL1-064 Final Presentation

Michal Pfleger
michal.pfleger@huld.io

07.03.2025

huld

Huld Czech

- Founded in 2015 as Space System Czech
- Transformed to HULD in 2020
- Headquarter in Prague center:
  Nám.Winstona Churchilla 1800/2

- About 20 Employees

- ISO 9001 certified
- ESA financial audit 09/2022
- ESA business code 8000007731

Flight Software development

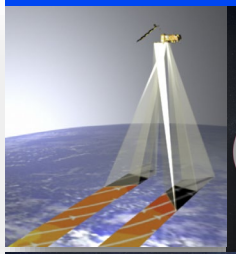
Protocols: CSP, PUS-C, CAN, MIL-STD1553B,
Standards: ECSS, CCSDS, MISRA-C, IEC 65108, EN5010
Languages: C, C++, ADA, Java, Python

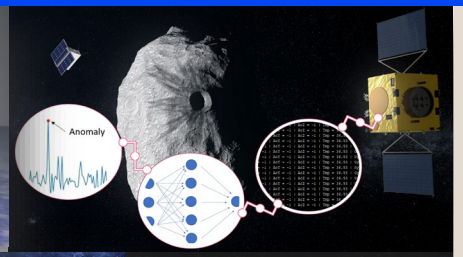
Design & development of safety-Critical software according to the ECSS standards, experience with Software Criticality B, C. Central Software & Application Software.

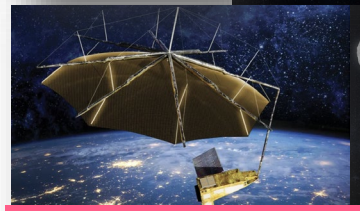
Quantum technologies

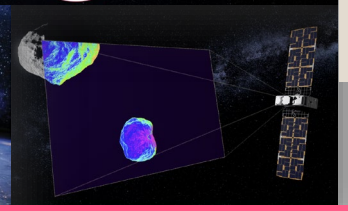
Technologies: Quantum computers, Quantum algorithms, Qiskit, PQC, Image processing,

- Space debris collection optimization
- Post-quantum cryptography
- Quantum-based space data processing









Technology development

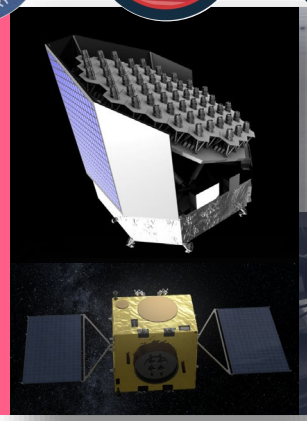
Technologies:
GNSS, AI/ M&L, Kalman filtering, data fusion, FPGA

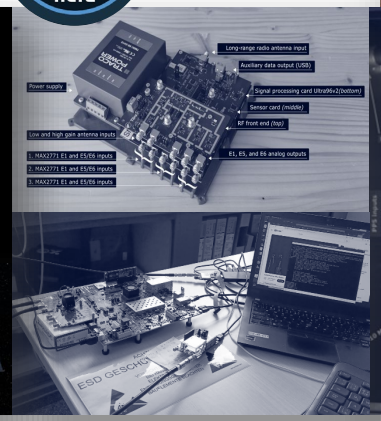
- Anti-spoofing and jamming solution
- Resilient Time Provision platform
- Platform for Cooperative positioning

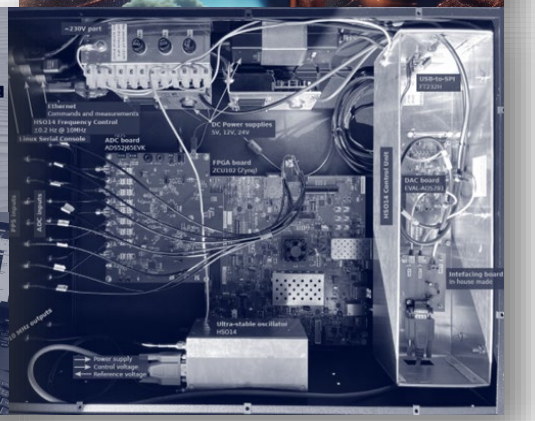
Validation and Verification

Standards: ECSS, CCSDS, MISRA-C, IEC 65108, EN5010

(Independent) Validation and Verification of safety-critical software, including development of Software Validation Facilities.







Introduction

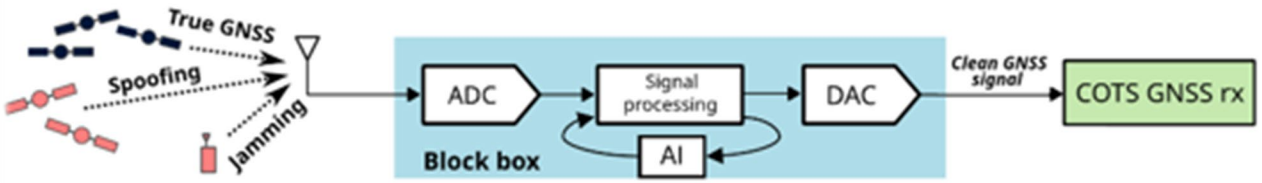
- GNSS based services are omnipresent nowadays (including safety of life and critical infrastructure)
  - PNDs, Transportation, Timing, Finances, Telecommunications, Power grids, Surveying, Civil Engineering
  - Over 6 billions of GNSS receivers deployed worldwide
- GNSS signals are highly vulnerable to interference
- Steep increase of GNSS related attacks can be observed
  - Jamming (denial of service)
  - Spoofing (forged PNT outputs)

Motivation

- Protection of existing receivers against attacks
- Monitoring of GNSS interference

Block-box

- Plug-n-play RF2RF device
- Local GNSS threats detection and classification (AI)
- Signal cleaning (DSP) and retransmission
- Cloud/server app for control and management



huld

Project summary

Summary

- NAVISP Element 1
- 18 months duration
- Huld s.r.o. as the prime contractor

Main tasks

- State of the art review
  - Summary of GNSS signals threats and possible detection & mitigation techniques
- Tradeoffs and requirements consolidation
  - Evaluation and selection of the techniques and algorithms
- End-to-end SW model development and testing
  - Python based SW incorporating all major components of the system
- HW platform development
  - HW procurement, FPGA design and firmware development, integration
- Testing and validation
  - End to end system testing and performance evaluation using synthetic signals
- Experimentation
  - Performance evaluation using in-field collected records from ESA

huld

Block-box HW prototype

Capabilities

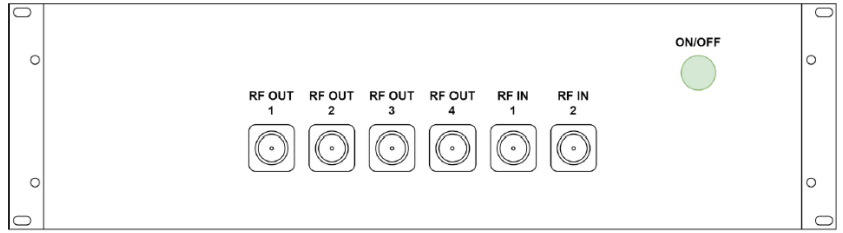
- RF signal retransmission
  - 0 – 3 GHz
  - Up to 2 independent RF inputs/outputs
  - 4 processing channels up to 150 MHz bandwidth each
  - Flexible configuration (e.g. 1 RF path E1/L1, E5a/L5, E5b, E6; or 2 RF paths E1/L1, E5)
- Real-time GNSS Jamming detection, classification and mitigation
  - Any GNSS RF band, constellation and signal type agnostic
  - AI based detection and classification (ResNet and U-net based CNN)
  - DSP based mitigation (FDAF method)
  - Effective against CW (single/multitone), Chirp and pulsed jammers
- Real-time GNSS Spoofing detection (Galileo E1, GPS L1 C/A)
  - Simple ResNet CNN using snapshot of cross ambiguity function
- Record/replay to local SSD storage
  - All 4 channels simultaneously
  - Up to 46 MHz BW each channel
- Server/cloud application
  - Control and management of more units
  - AI retraining scripts

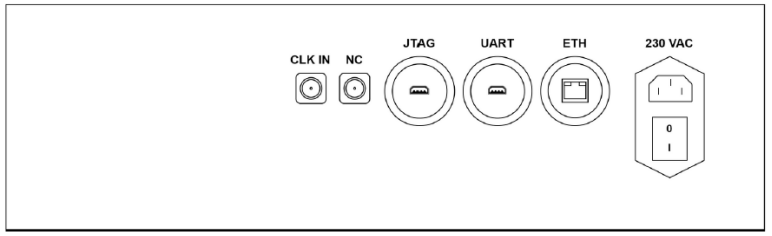
huld

Block-box HW prototype

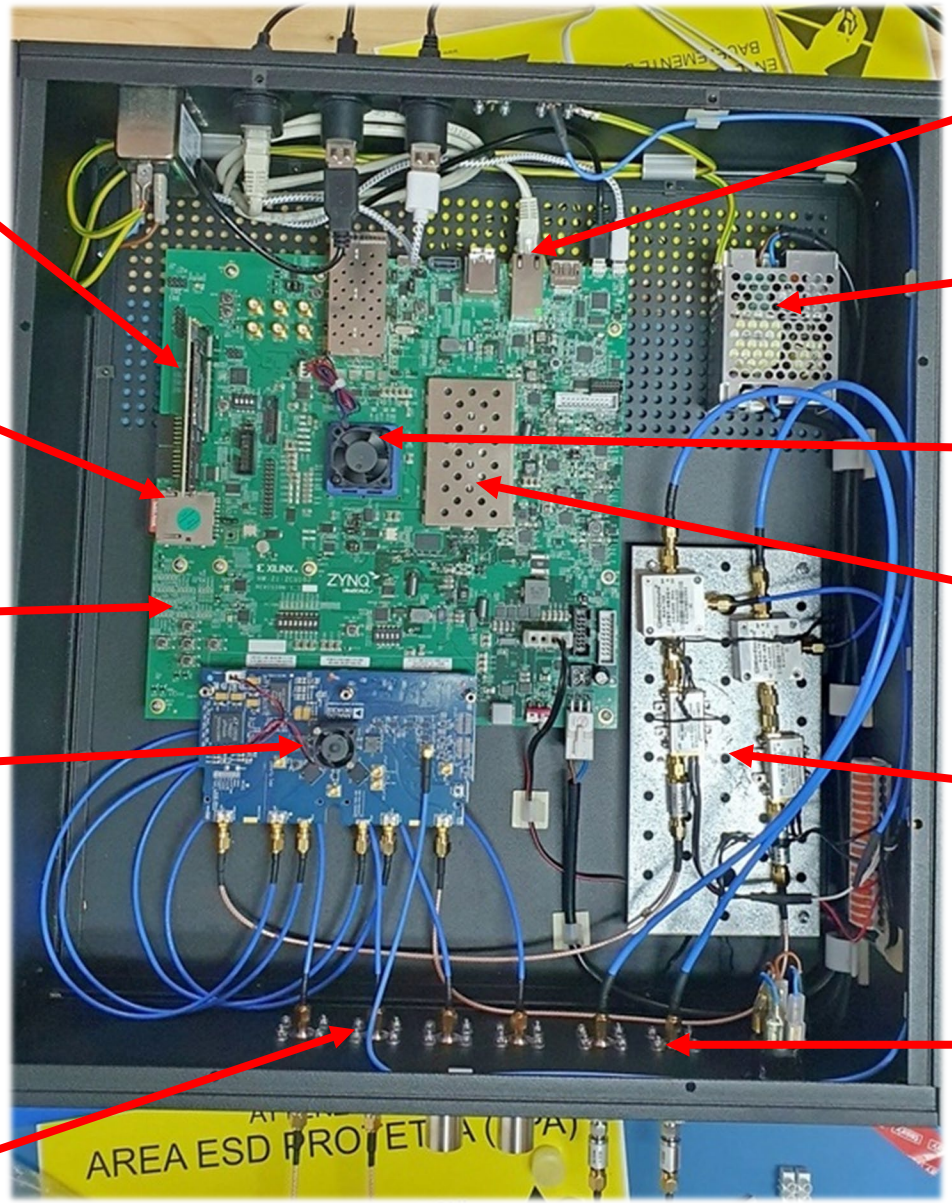
Main HW features

- 3U Rack-mountable case (HxWxD 13x48x45 cm)
- 100-240 VAC power input, 70 W
- Based on Zynq Ultrascale+ MPSoC ZCU102 (XCZU9EG)
  - Quad-core ARM Cortex A53, Dual-core Cortex R5F, Mali-400 GPU
  - FPGA
  - DDR4, PCIe gen 2 x4, SATA, USB 3.0, SGMII, UART, CAN
- AD9082-FMCA-EBZ ADC/DAC board
  - 2 ADC (6 GSPS), 4 DAC (12 GSPS)
  - 8 channel channelizer (DDC, DUC)
  - HMC7044 clock management
- 2 RF inputs, 5 V antenna feed provided
- 4 RF outputs (2 in use)
- 2 TB internal SSD storage
- 1 Gb/s Ethernet





Block-box HW prototype



2TB SSD storage
(Samsung PCIe 4.0 NVMe™ SSD 980 PRO)

SD card with firmware

Zynq ZCU102 board

ADC/DAC
(AD9082-FMCA-EBZ)

4x RF OUT

Ethernet

Power source 12V

MPSoC
(Zynq Ultrascale+)

DDR4

RF Input stages
(LNA, bias-tee)

2x RF IN

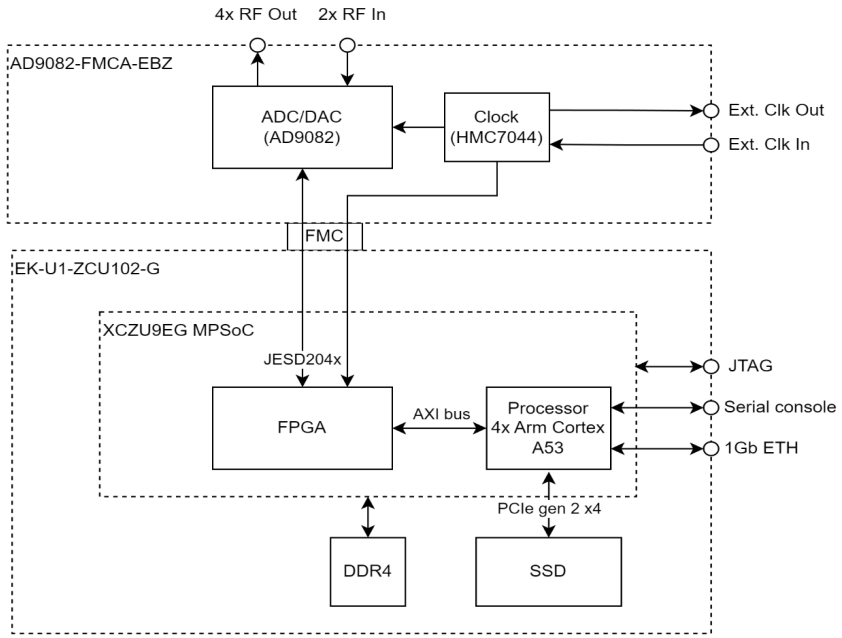
High-level architecture

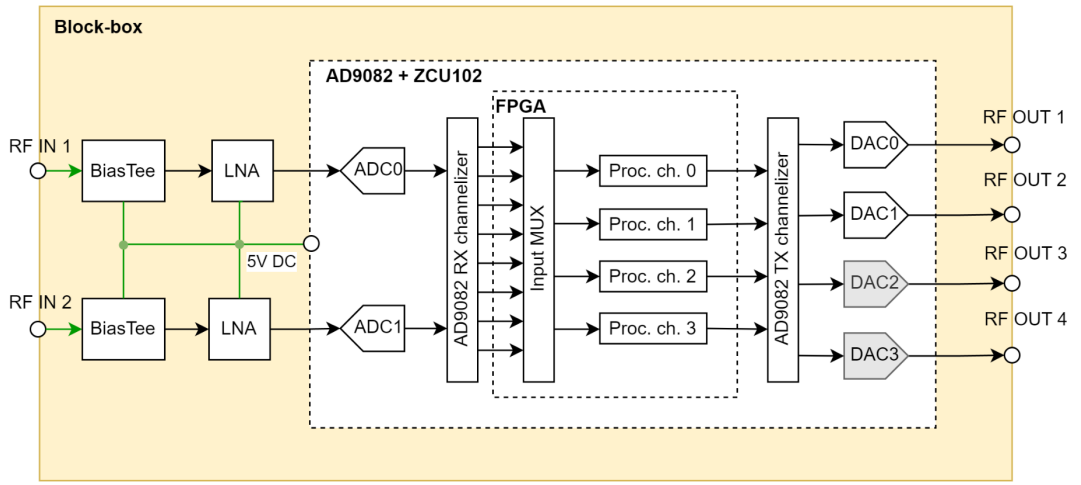
High-level block diagram

- RF input
  - Sinal amplification
  - 5V active antenna power feed

- AD9082 development board
  - ADC, channelizer (down-conversion)
    6 GS/s -> 375 MS/s
  - DAC, channelizer (up-conversion)
    375 MS/s -> 12 GS/s
  - Internal clock generation
  - Ext. clock in (10 MHz clock input)

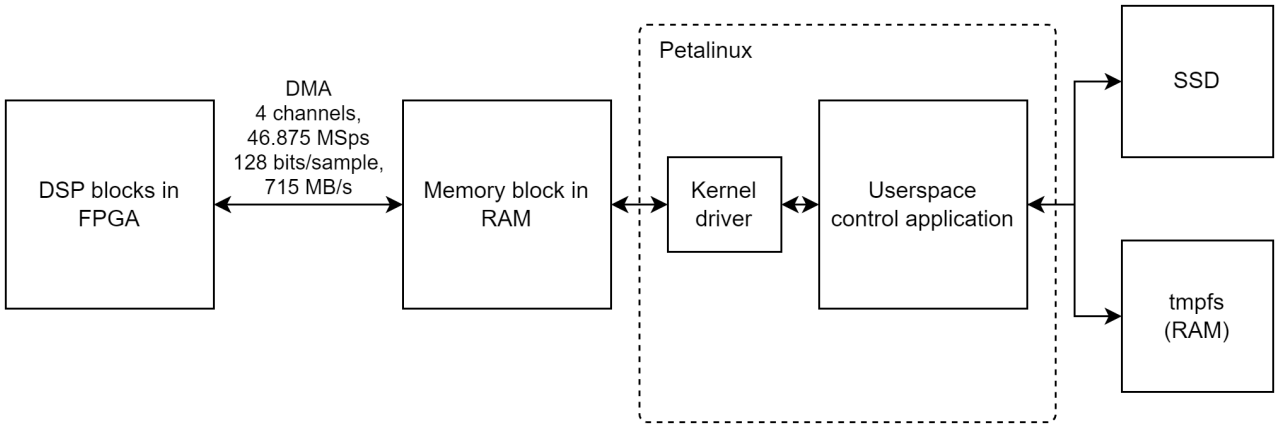
- Zynq ZCU 102
  - FPGA (DSP processing blocks)
  - Processor (Petalinux, comm., control, AI processing)
  - SSD (2 TB storage for recorded data)
  - Serial console, JTAG (debugging)
  - 1 Gb Ethernet (control, data transfer)
  - SD card (firmware image)

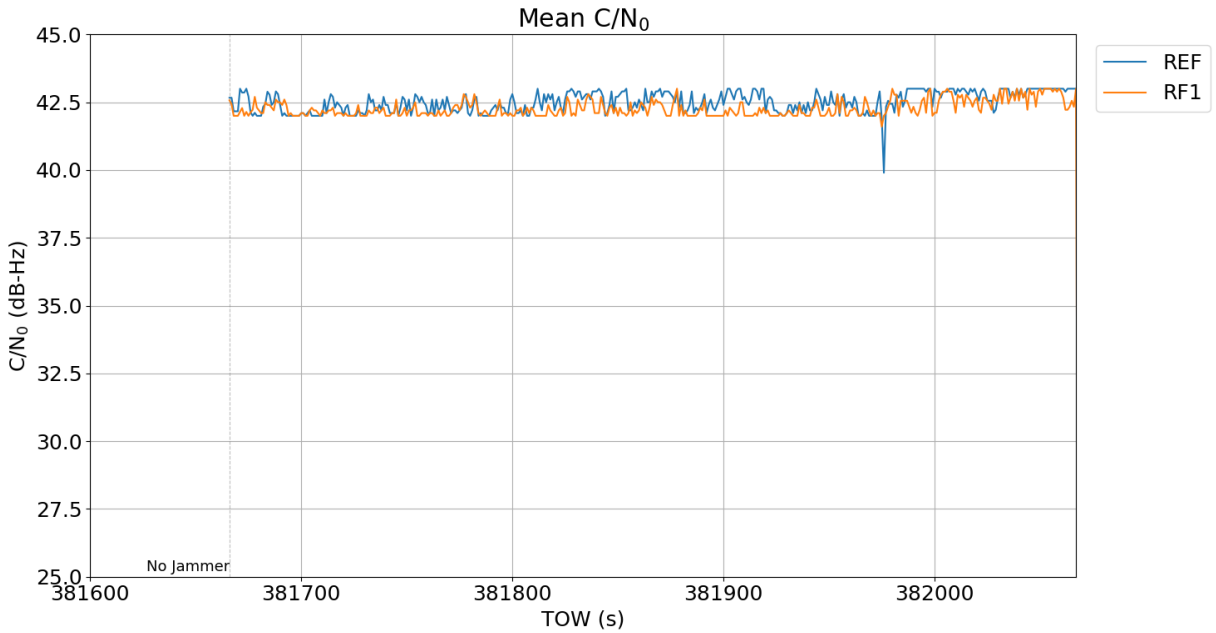


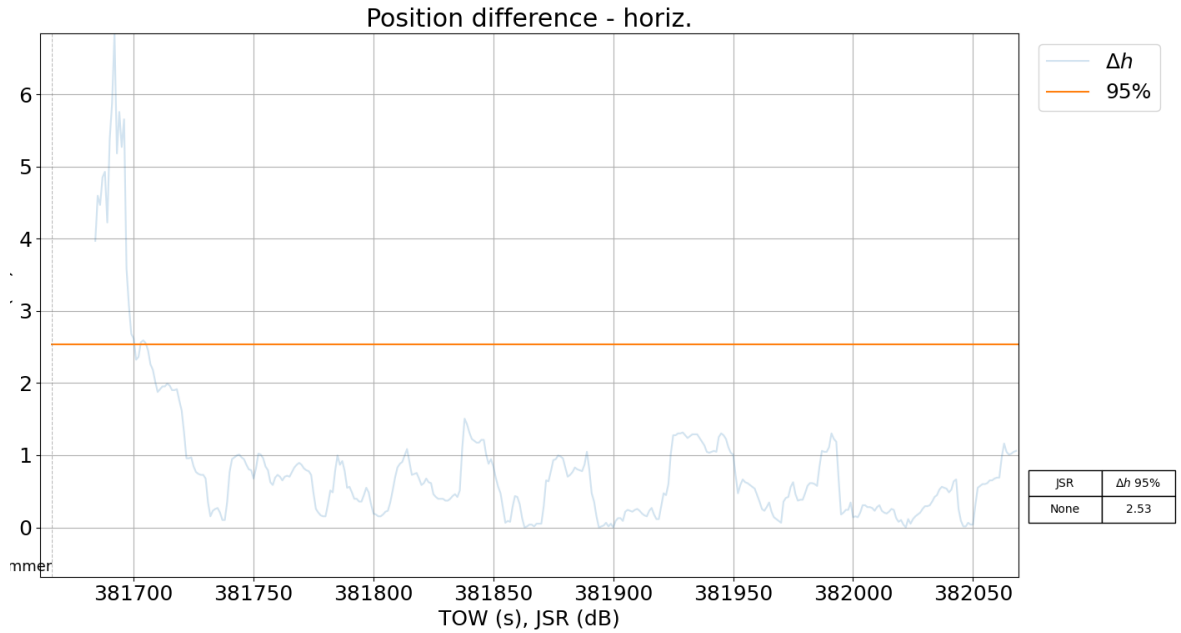


Record & Replay

- Record/replay 4 channels simultaneously
- Up to 46.875 MSps
- 2 TB internal SSD storage
- 1.5 GB tmpfs RAM disk

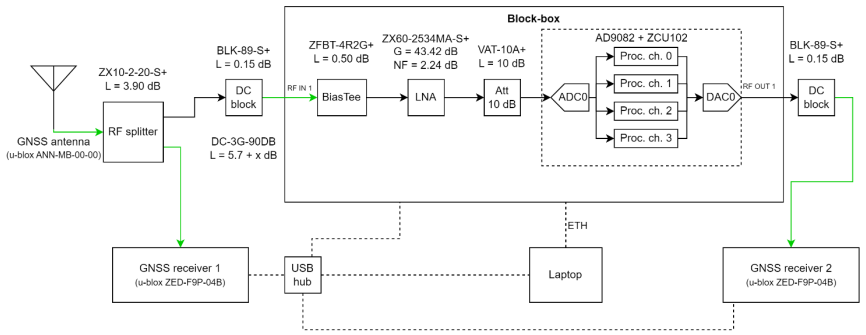


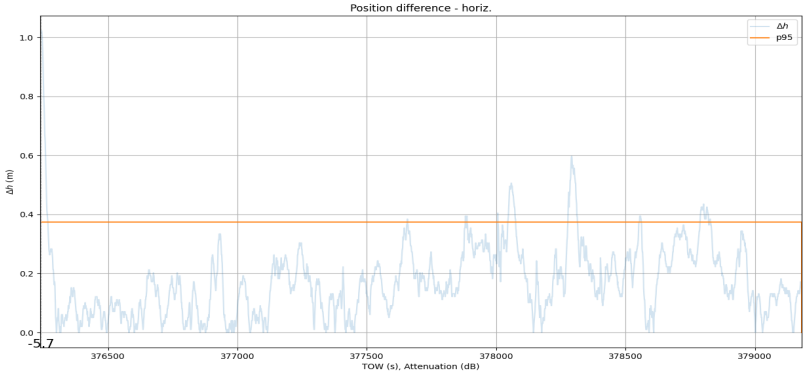




Fault-free signal degradation

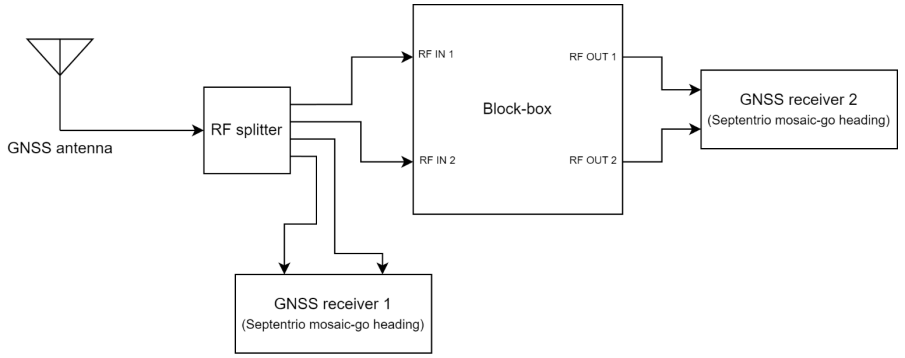
Signal degradation

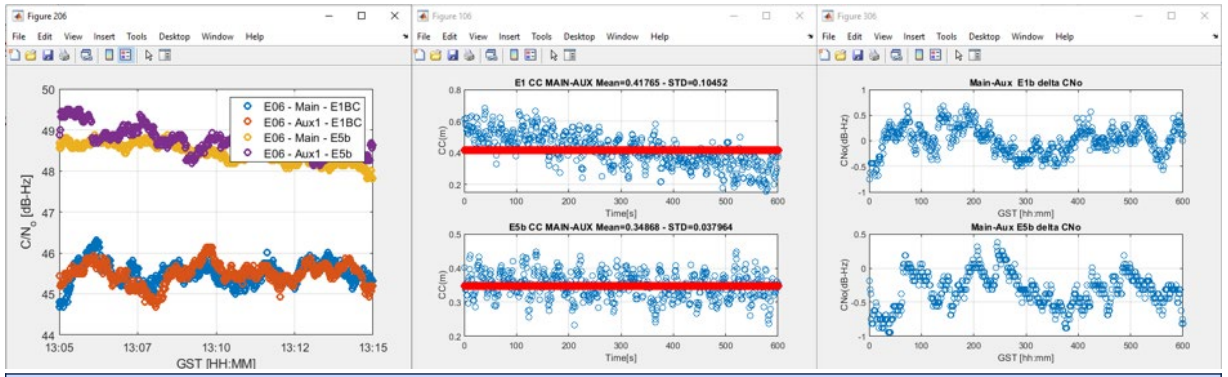




Test part	TOW	Duration (s)	Δh_{p95} (m)	Δv_{p95} (m)	$\Delta C/N_0$ E1 (dB)	$\Delta C/N_0$ E5b (dB)	ΔPR E1 (m)	ΔPR E5b (m)
Test A	380538	3629	0.22	0.40	0.02	0.04	0.43	0.43
Test B	376241	2940	0.37	0.81	-0.48	-0.23	0.47	0.22

RF1, RF2 retransmission coherency



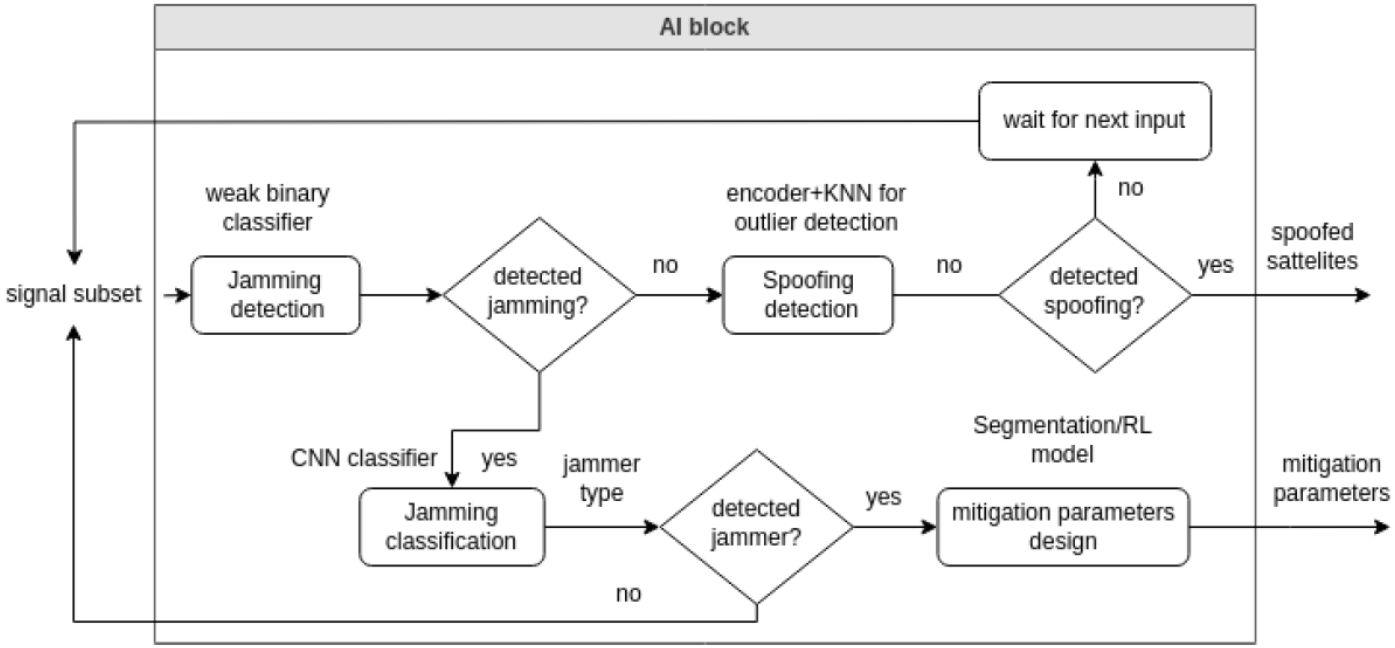


Criteria	Signal	Rcvr 1	Rcvr 2	Difference (Rcvr2 - Rcvr 1)
Mean $\Delta C/N_0$ Main - Aux (dB)	E1	-0.3	0.1	0.4
	E5b	-0.2	-0.4	-0.2
Mean ΔPR_{code} Main - Aux (m)	E1	0.473	0.418	-0.055
	E5b	0.631	0.349	-0.282

AI models, processing and training data

Onboard AI processing

- Python based high-level control application
- Tensor flow
- No AI HW accelerator for now



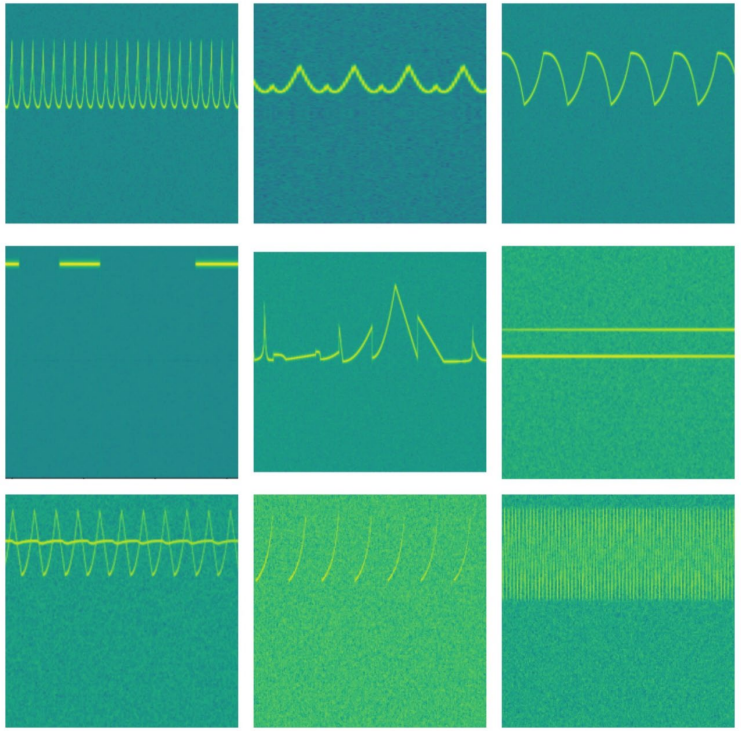
4 independent AI models

- 3 for jamming detection and classification
- 1 for spoofing detection
- Details on following slides

Models training and training datasets

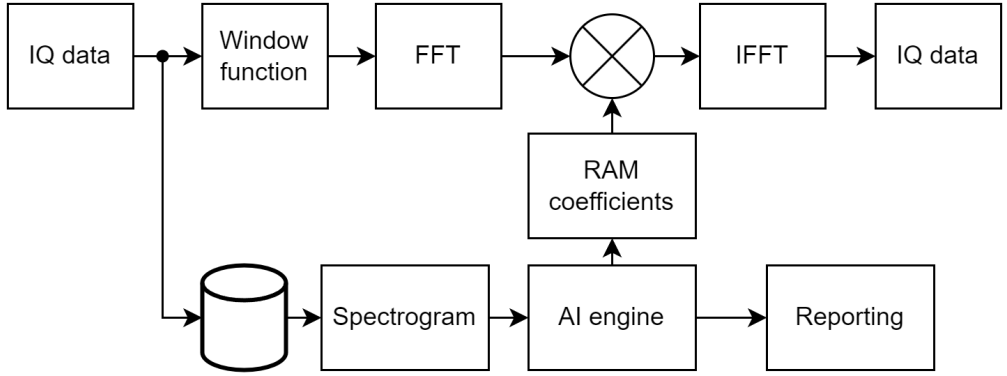
- Dedicated scripts as part of the server application
- Training data mainly generated based on the GNSS threats models
- For jamming also in-field collected data are used

Jamming detection & mitigation



FDAF (Freq. Domain Adaptive Filtering)

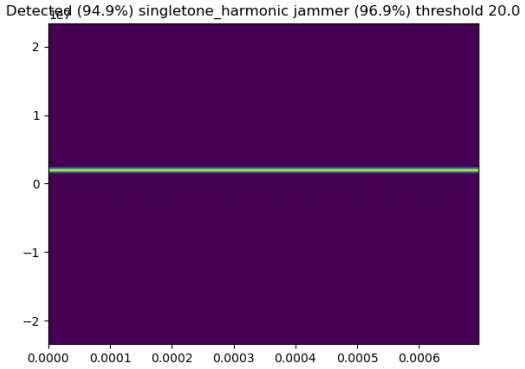
- AI detection and classification
  - Spectrogram as the inference input
  - CW (single/multitone), Chirp and pulsed jammers
  - Simple weak detection (small ResNet binary CNN classifier)
  - Classification (Resnet CNN classifier)
    - No jammer, CW single-tone, Chirp, Pulse harmonic, CW multi-tone
  - Segmentation (U-net CNN)
  - Training data
    - Model-based synthetic data
    - Real in-field collected data

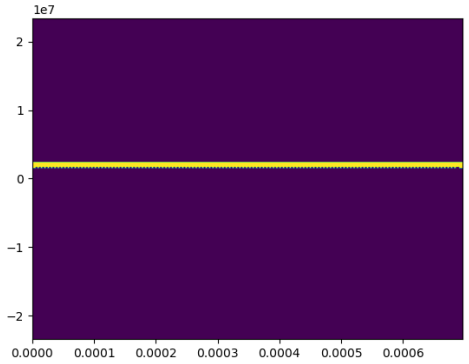


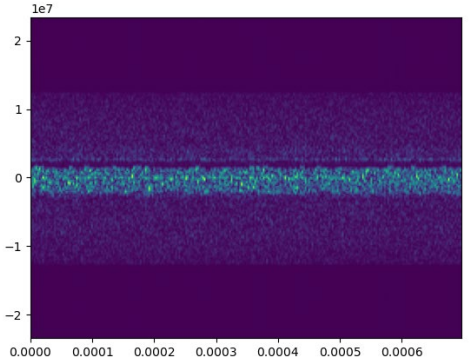
- DSP mitigation
  - Windowing function
  - FFT size 32, 64, 128, 256
    (jammer type and sample rate)
  - Blanking all bins above threshold
    (segmentation, noise levels)

huld

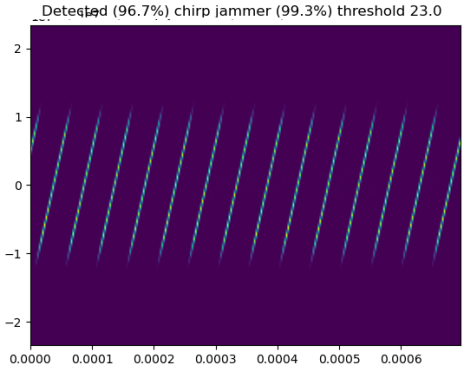
Validation results

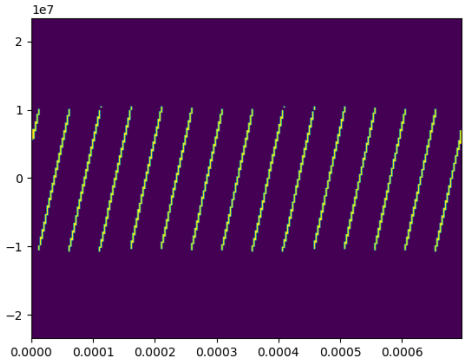


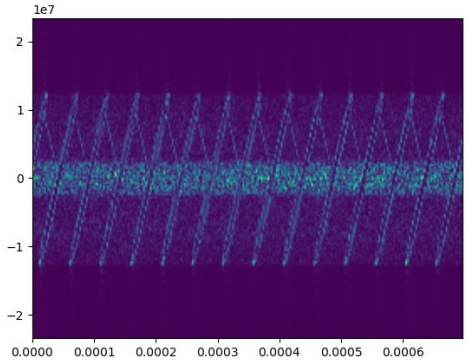


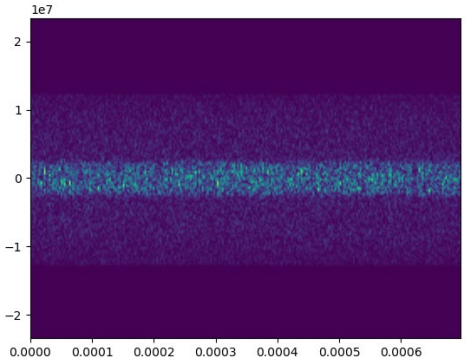


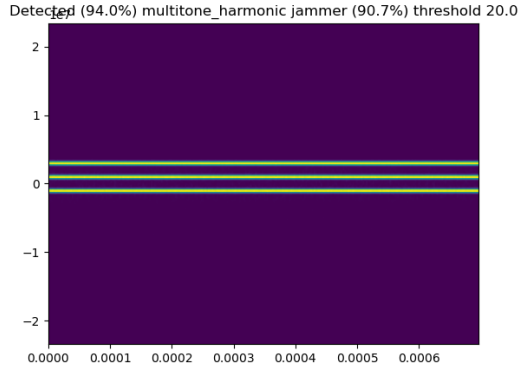
Clean OAKBAT signal

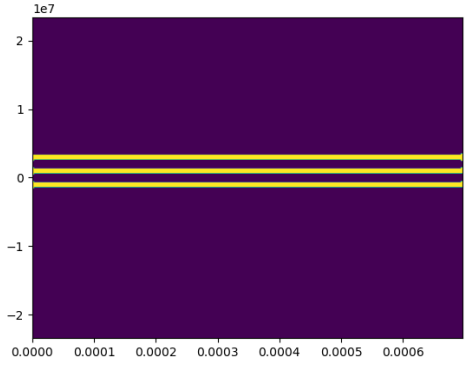


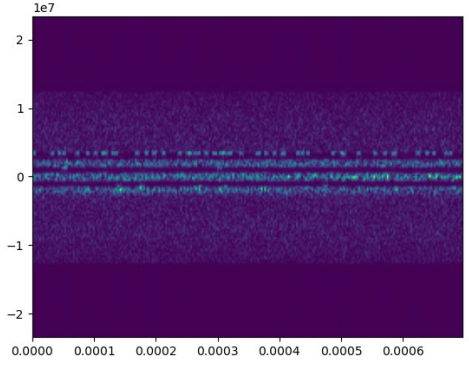










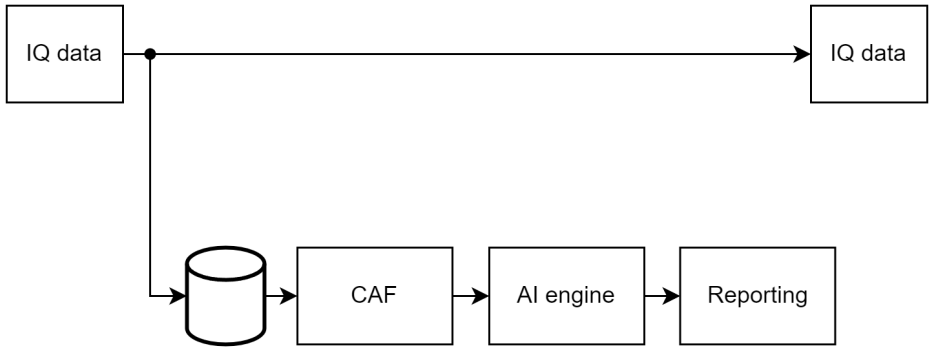


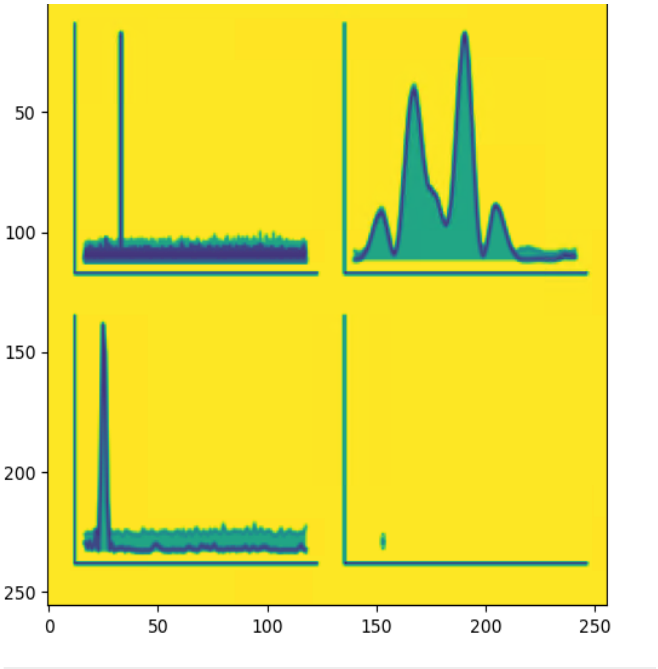
huld

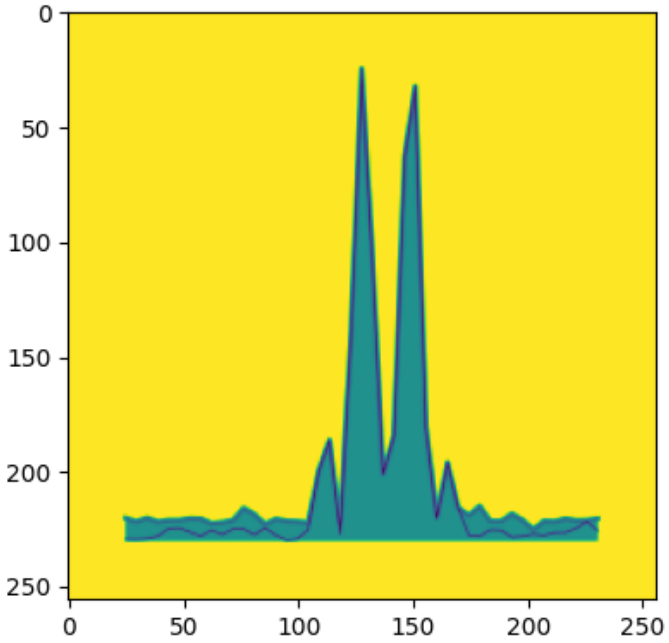
Spoofing real-time detection

Simple spoofing detector

- AI detection
  - CAF snapshot as the inference input
  - Galileo E1, GPS L1 C/A
  - ResNet binary CNN classifier
  - Training data:
    - Model-based generated synthetic IQ data



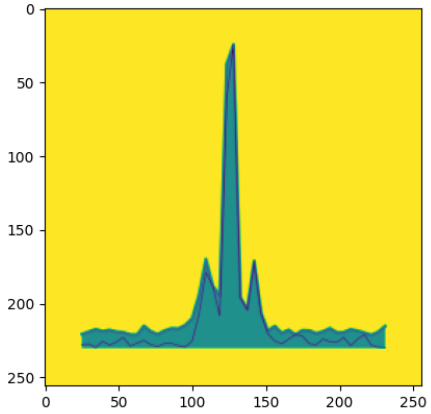




Spoofing real-time detection

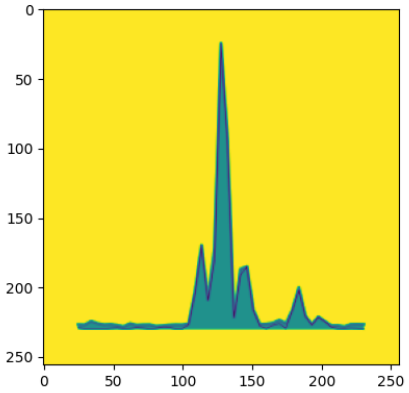
OAKBAT clean signal

No spoofer detected.Clean data with 91.50 % confidence.
0: C/N0 41.3 fD -2540.7 tau 2.710



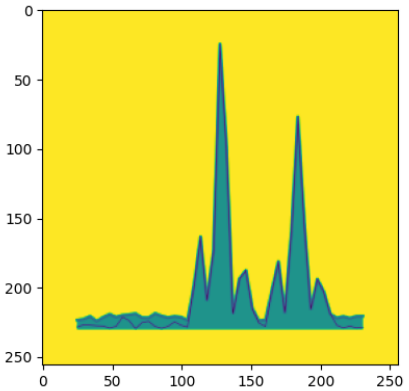
OAKBAT os10

Spoofing threat detected (2 distant corr. peaks)
0: C/N0 47.5 fD -2548.2 tau 2.799
1: C/N0 39.0 fD -2557.7 tau 2.801



OAKBAT os11

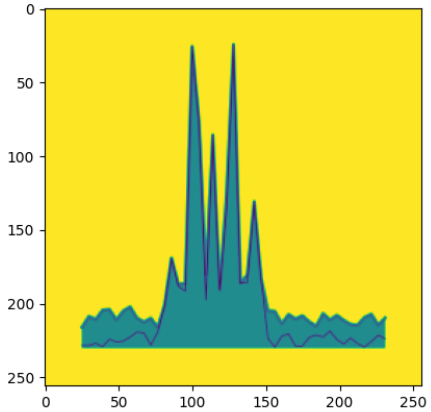
Spoofing threat detected with 98.02 % confidence (corr. peak shape).
0: C/N0 43.0 fD -2586.5 tau 0.628
1: C/N0 41.7 fD -2573.5 tau 0.630



Detection	100 %
Missed det.	0
False alarms	0

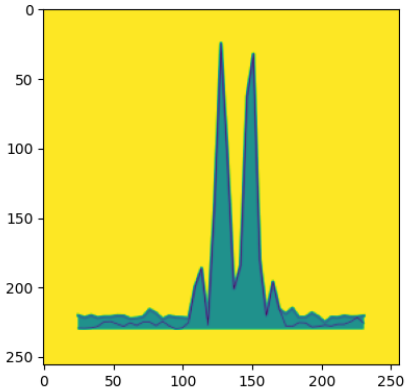
OAKBAT os12

Spoofing threat detected with 98.95 % confidence (corr. peak shape).
0: C/N0 39.8 fD -2547.8 tau 2.755



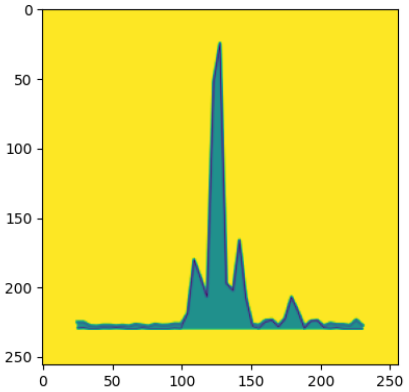
OAKBAT os13

Spoofing threat detected with 97.03 % confidence (corr. peak sh
0: C/N0 42.4 fD -2531.7 tau 2.129
1: C/N0 36.1 fD -2553.0 tau 2.130



OAKBAT os14

Spoofing threat detected (2 distant corr. peaks)
0: C/N0 47.4 fD -2484.1 tau 2.950
1: C/N0 37.8 fD -2468.1 tau 2.952



Verification and Validation testing

- Test campaign run in Huld Prague offices

Goal

- Verification of the HW platform function
- Validation of the performance with synthetic RF signals (GNSS, jamming, spoofing)

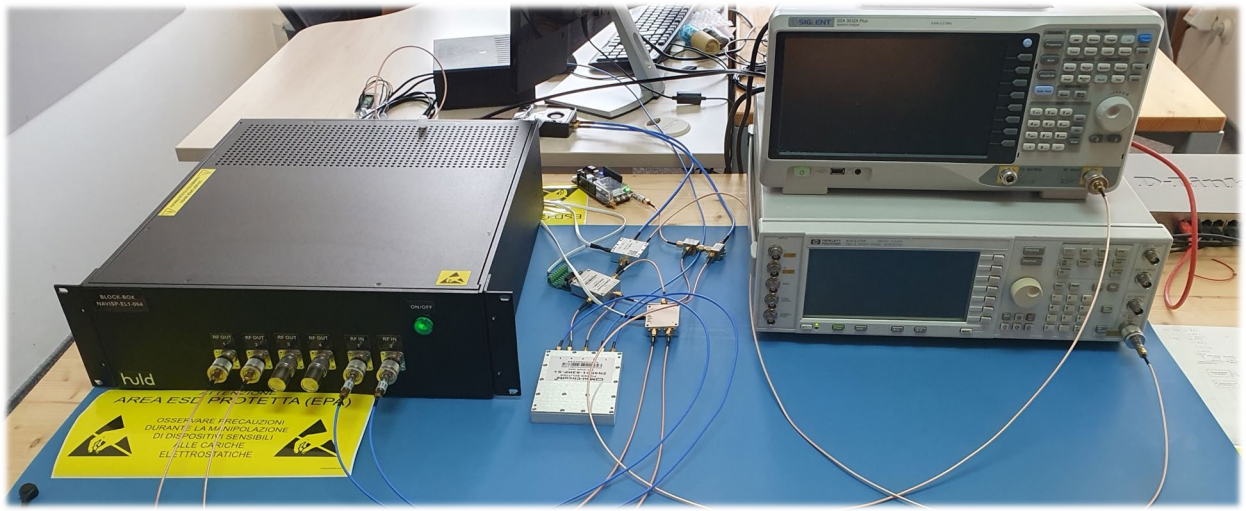
Test categories

- Hardware testing
- Algorithms testing (E2E SW model)
- E2E System performance testing
- Local interface testing
- Server application interface testing

Test scenarios

- Live-sky clean signal testing
- Jamming
  - OAKBAT cleanStatic Galileo
  - Synthetic jamming signals
- Spoofing
  - OAKBAT Galileo data files (os10 – os14)
  - Combination of cleanStatic and cleanDynamic data

Test setup:



Equipment:

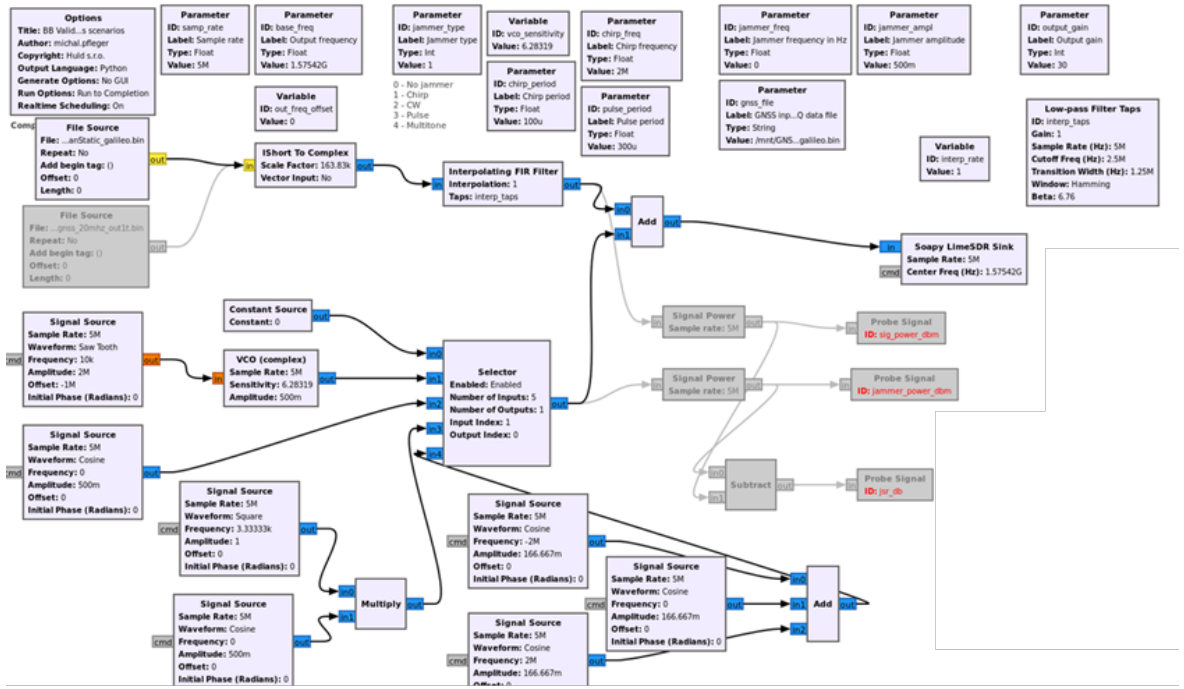
- Block-box HW platform
- Replay device Lime SDR Mini 1.0
- Signal Generator HP E4433B
- Spectrum Analyzer Siglent SSA3032X PLUS
- 2x u-Blox ZED-F9P-04B GNSS receivers
- 1x Septentrio Mosaic-T receiver
- RF splitters, RF switches
- Attenuators, DC blocks
- Control Server

huld

Testing signals and data

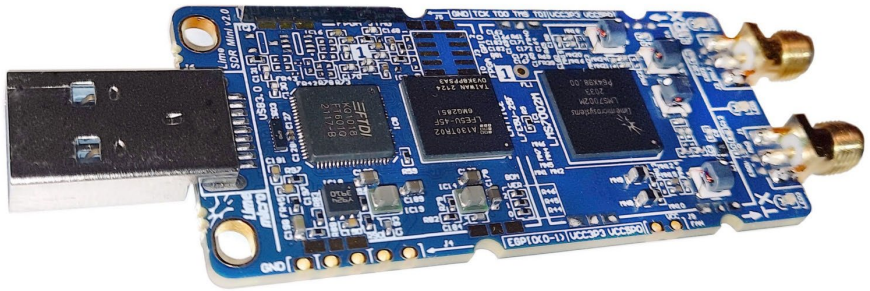
IQ Data generation

- OAKBAT datasets
  - Simulated signals, 5 MS/s
  - Galileo and GPS datasets
  - Static & dynamic spoofing scenarios
  - Clean reference scenarios
  - 480 seconds duration
- GNU Radio toolkit
  - OAKBAT datasets as source of clean/spoofed GNSS signals
  - Signal interpolation to 20 MS/s
  - Addition of jamming signals (CW, chirp, pulsed)



Signal replay

- Lime SDR Mini 1.0



Lime SDR Mini 1.0

- 10 MHz to 3.5 GHz
- 1x RX, 1x TX channel
- 40 MHz BW
- Max 30.72 MS/s
- 12 bits
- ± 1 ppm oscillator

Automated Python control environment

- Scenarios definition
- Automatic execution
- Block-box commanding
- Data collection, processing and evaluation

huld

Performance metrics

AI

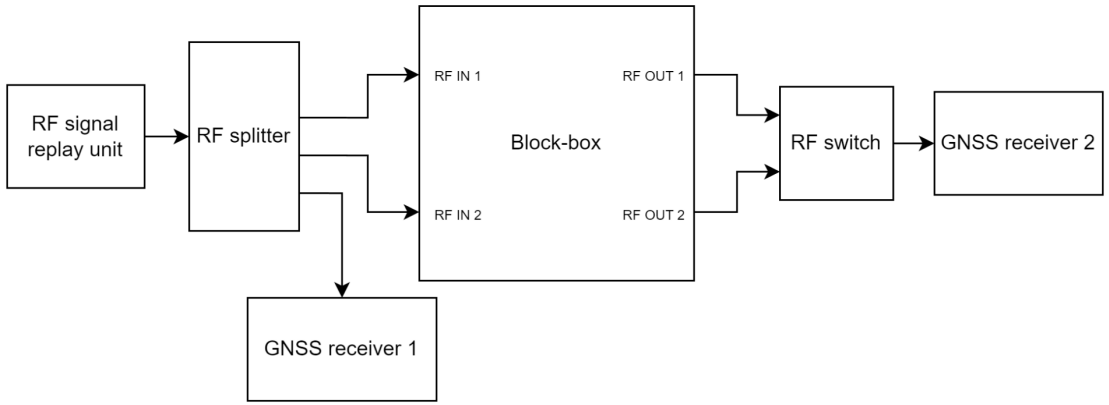
- Accuracy $Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$
- Missed detection rate $MD = \frac{FN}{TP+TN+FP+FN}$
- False alarm rate $\mathrm{FA} = \frac{FP}{TP+TN+FP+FN}$
- Classification accuracy

	Predicted Positive	Predicted Negative
Actual Positive	True Positive (TP)	False Negative (FN)
Actual Negative	False Positive (FP)	True Negative (TN)

Mitigation

- Mean C/N0 difference
- Mean Pseudorange RMS difference
- Number of tracked satellites
- Position accuracy

Common test configuration

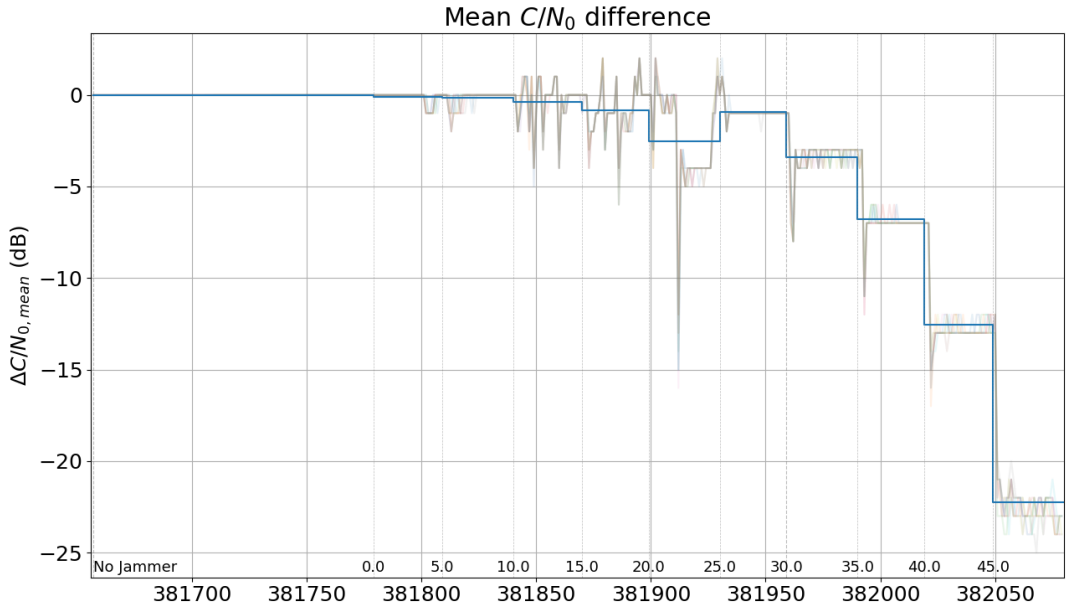


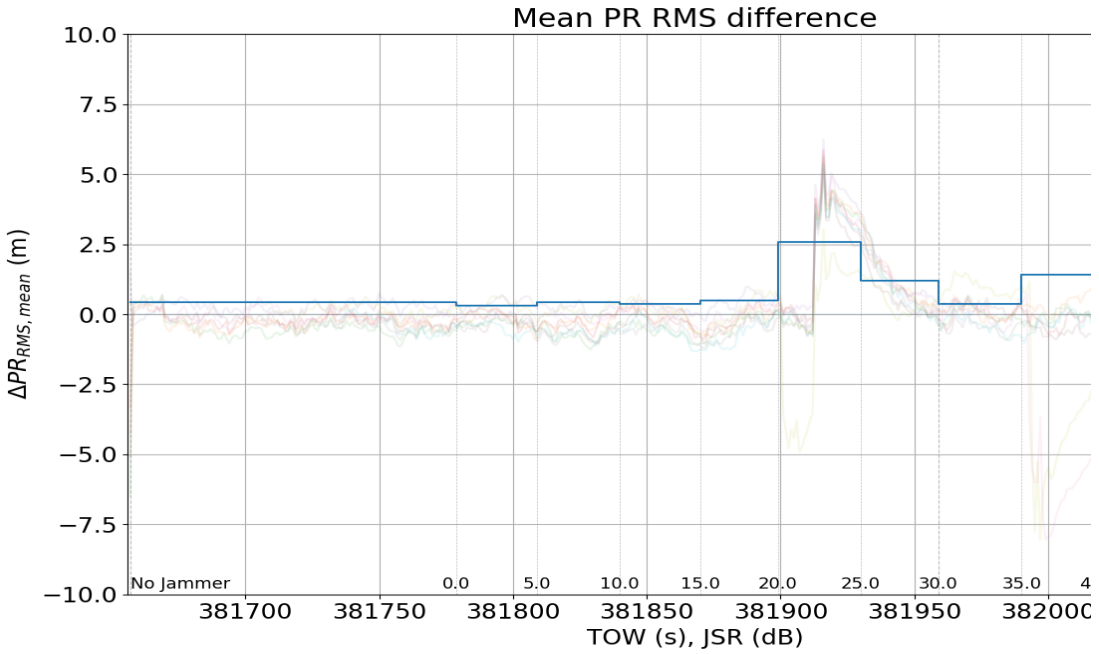
1. Reference run (clean signal)
2. Test run (interference present)

Validation results

Case ID	Jamming type	Detection Accuracy (%)	False alarms events (%)	Missed det. events (%)	Classification accuracy (%)
0	No jammer	100	0	0	-
1	CW, 45 dB, E1	99.7	0	0.3	100
2	CW, 40 dB, E1	99.5	0	0.5	100
3	CW, 20 dB, E1	99.7	0	0.3	100
4	CW, 10 dB, E1	99.7	0	0.3	100
5	Pulsed, 40 dB, E1, 50 % d. c.	99.7	0	0.3	100
6	CW multitone, 40 dB, E1	99.7	0	0.3	100
7	Chirp, E1, 20 MHz 500 µs	99.7	0	0.3	100
8	Chirp, E1, 20 MHz 200 µs	99.7	0	0.3	100
9	Chirp, E1, 20 MHz 100 µs	99.7	0	0.3	100
10	Chirp, E1, 20 MHz 50 µs	99.7	0	0.3	100
11	Chirp, E1, 20 MHz 20 µs	99.7	0	0.3	100
12	Chirp, E1, 20 MHz 10 µs	99.6	0	0.4	100
13	Chirp, E1, 20 MHz 5 µs	99.4	0	0.6	100

Case ID	Jamming type	C/N_0 res, degrad. (dB)	C/N_0 mitig. gain (dB)	$\Delta PR_{RMS,mean}$ res. degrad. (m)	$\Delta PR_{RMS,mean}$ mitig. gain (m)	Δh_{p95} jammed (m)	Δh_{p95} mitigated (m)	Δh_{p95} no jammer (m)
1	CW, 45 dB, E1	0.1	-	0.6	-	No PVT	2.4	3.3
2	CW, 40 dB, E1	0.1	12.6	0.6	2.3	1.9	1.8	3.3
3	CW, 20 dB, E1	0.0	2.5	0.5	2.0	2.7	3.8	3.3
4	CW, 10 dB, E1	0.0	0.1	0.5	0.3	1.9	3.7	3.3
5	Pulsed, 40 dB, E1, 50 % d. c.	2.0	9.6	0.9	12325.4	25904.1	2.6	3.3
6	CW multitone, 40 dB, E1	7.7	4.7	6.2	6.5	2.1	3.0	5.2
7	Chirp, E1, 20 MHz 500 µs	0.3	-	0.6	-	No PVT	2.5	3.3
8	Chirp, E1, 20 MHz 200 µs	0.7	-	0.5	-	No PVT	2.0	3.3
9	Chirp, E1, 20 MHz 100 µs	1.0	-	0.6	-	No PVT	1.7	3.3
10	Chirp, E1, 20 MHz 50 µs	1.0	-	0.6	-	No PVT	4.5	3.9
11	Chirp, E1, 20 MHz 20 µs	1.1	-	0.6	-	No PVT	9.2	3.9
12	Chirp, E1, 20 MHz 10 µs	2.1	-	0.7	-	No PVT	2.0	3.8
13	Chirp, E1, 20 MHz 5 µs	3.1	-	0.9	-	No PVT	1.5	3.8





Experimentation

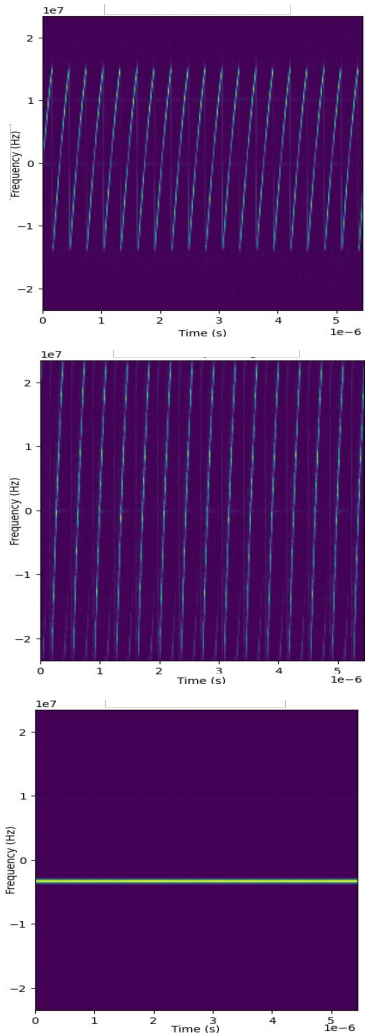
- Test campaign run in ESTEC Nav lab

Goal

- Test Block-box performance with real in-field collected data

Scenarios

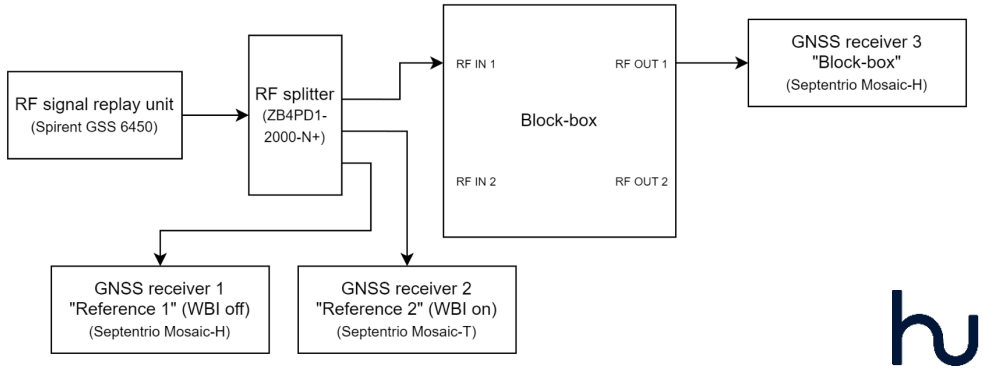
- **J11**
  - Low power L1 sawtooth chirp
  - 1577.40 MHz, 30 MHz BW, 37 µs sweep
  - < 0.03 W
- **J12**
  - Low power L1 & L2 sawtooth chirp
  - 1581.59 MHz, 85 MHz BW, 41 µs sweep
  - 1198.05 MHz, 97 MHz BW, 42 µs sweep
  - < 0.1 W
- **J15**
  - High power L1 CW frequency sweep
  - 1545 – 1620 MHz in 15 min.
  - 50 W



Test setup:

Equipment:

- Block-box HW platform
- Spirent GSS 6450 replay device
- 2x Septentrio Mosaic-H receivers
  - Ref. 1 WBI mitigation OFF
  - Ref. 2 WBI mitigation ON
- 1x Septentrio Mosaic-T receiver
- 1x Mini-circuits ZB4PD1-2000-N+ splitter
- 1x Mini-circuits BLK-89-S+ DC block



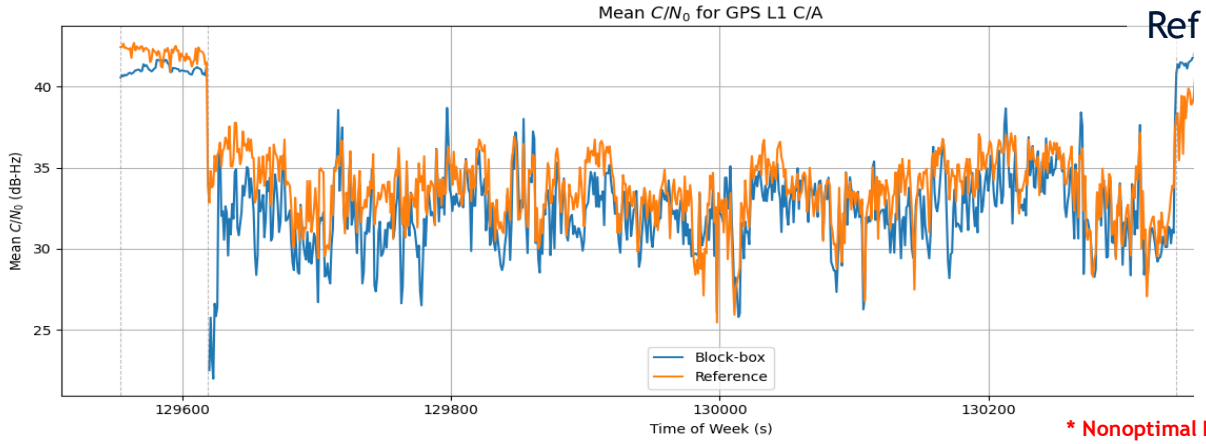
Experimentation results - J11

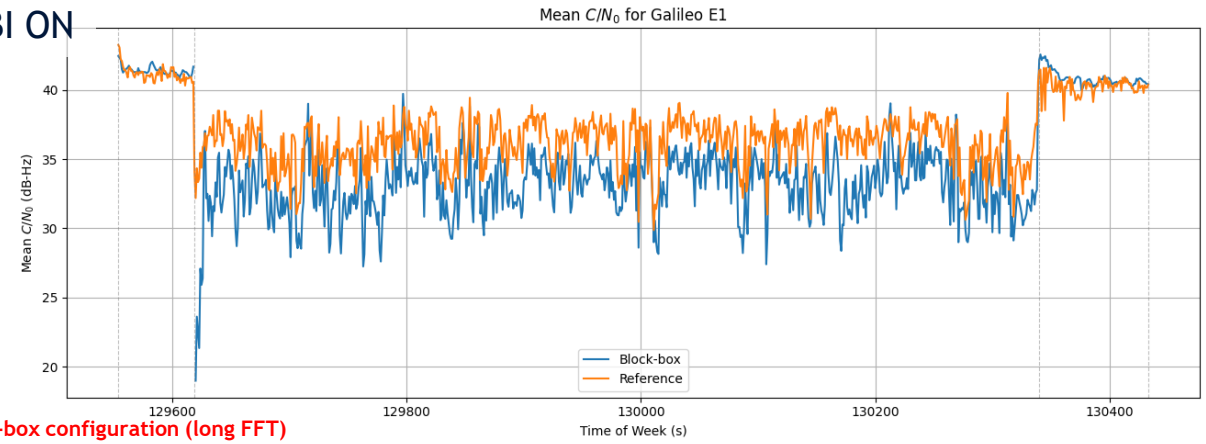
Results

- Clear improvement of C/N_0 over the unprotected ref. receiver
- Similar results as Septentrio's WB interference mitigation (with optimal configuration … shorter FFT)

J11 C/N_0 (dB-Hz)	GPS		Galileo	
	Jammer OFF	Jammer ON	Jammer OFF	Jammer ON
Reference – WBI on	42.1	33.6	41.2	36.1
Reference – WBI off	42.1	22.5	41.2	22.1
Block-box	41.0	34.2	41.3	36.4
BB vs. Ref WBI on (dB)	**-1.1**	**0.6**	**0.1**	**0.3**
BB vs. Ref WBI off (dB)	**-1.1**	**11.7**	**0.1**	**14.3**

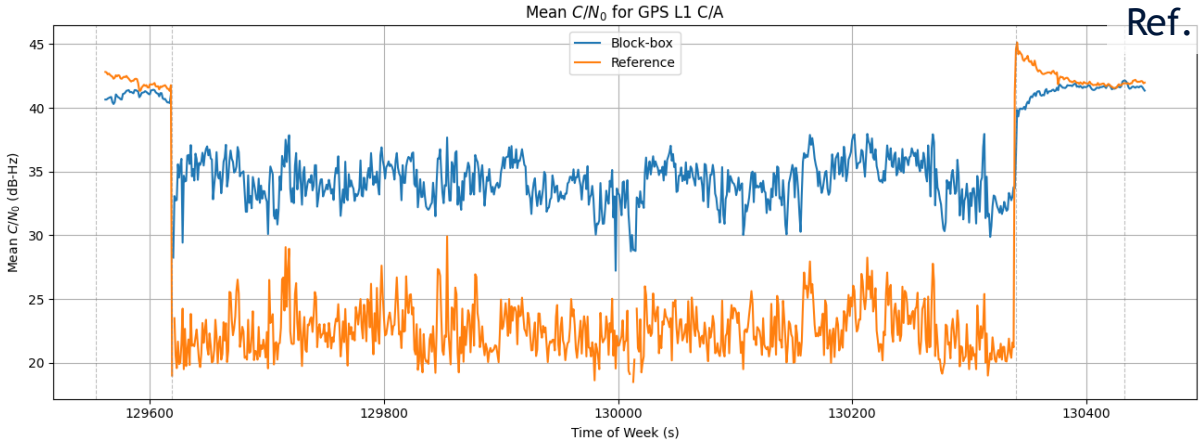
Ref WBI ON

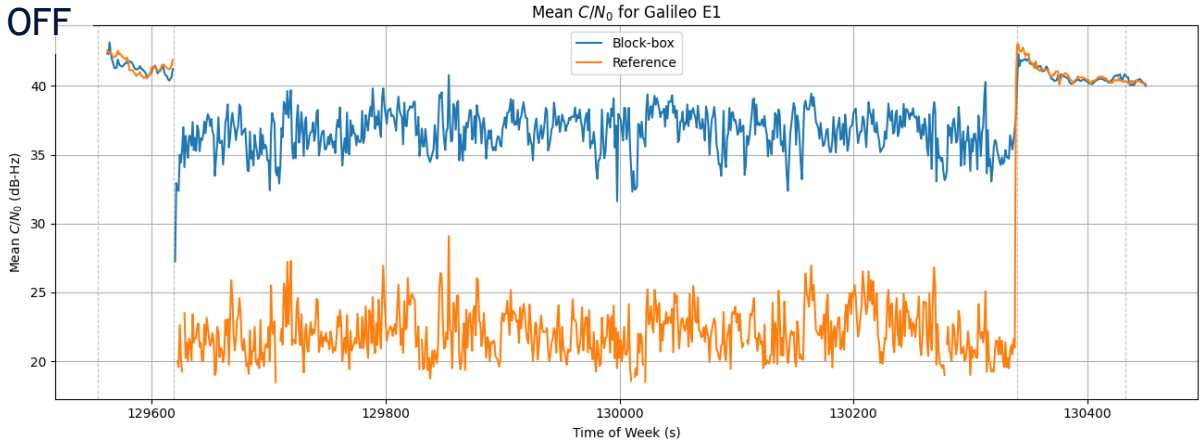




* Nonoptimal Block-box configuration (long FFT)

Ref. WBI OFF





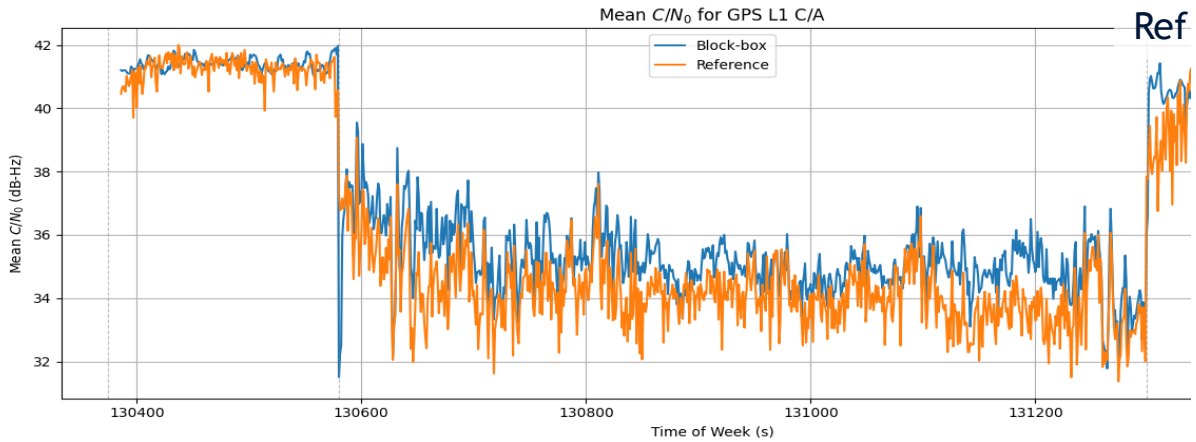
Experimentation results - J12

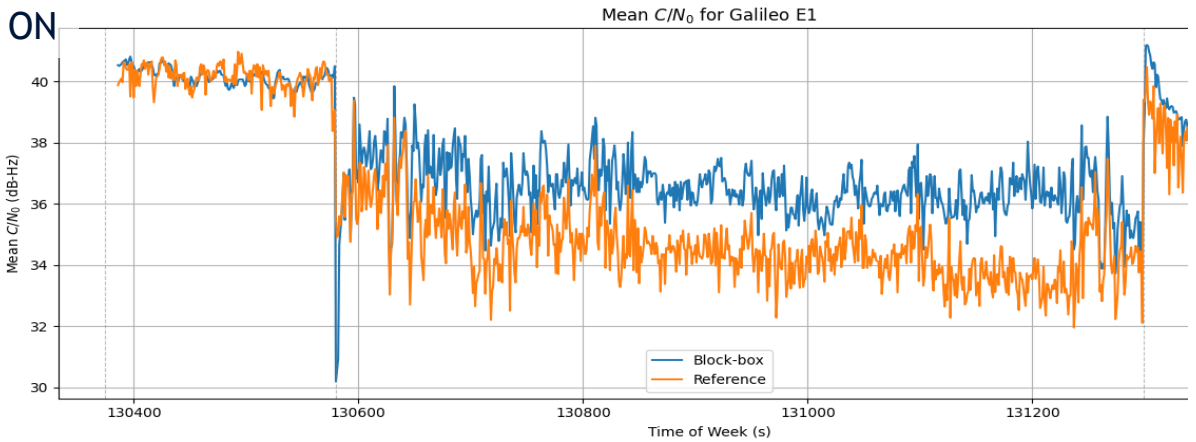
Results

- Clear improvement of C/N_0 over the unprotected ref. receiver
- Slightly better results than Septentrio's WB interference mitigation

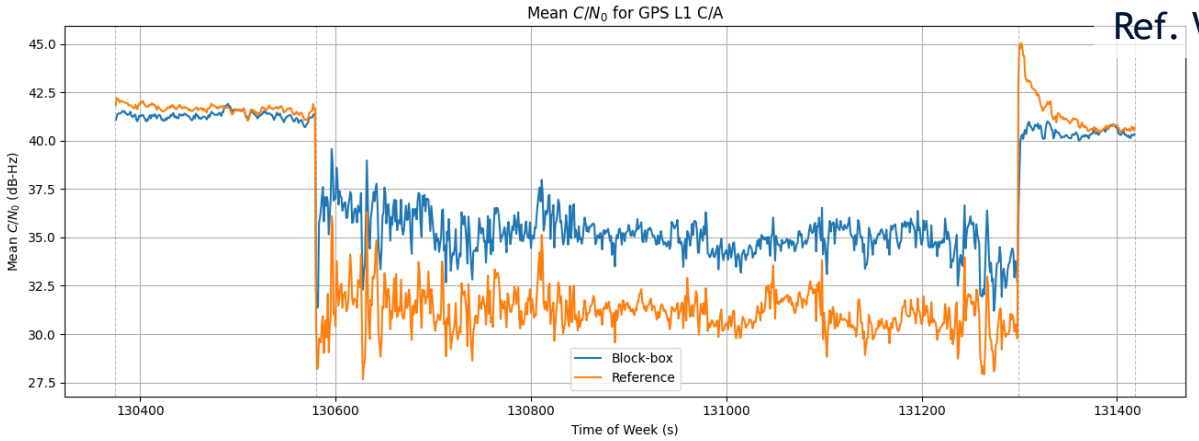
J12 C/N_0 (dB-Hz)	GPS		Galileo	
	Jammer OFF	Jammer ON	Jammer OFF	Jammer ON
Reference – WBI on	41.3	34.2	40.3	34.6
Reference – WBI off	41.7	31.1	40.3	30.3
Block-box	41.4	35.2	40.3	36.5
BB vs. Ref WBI on (dB)	**0.1**	**1.0**	**0.0**	**1.9**
BB vs. Ref WBI off (dB)	**-0.3**	**4.1**	**0.0**	**6.2**

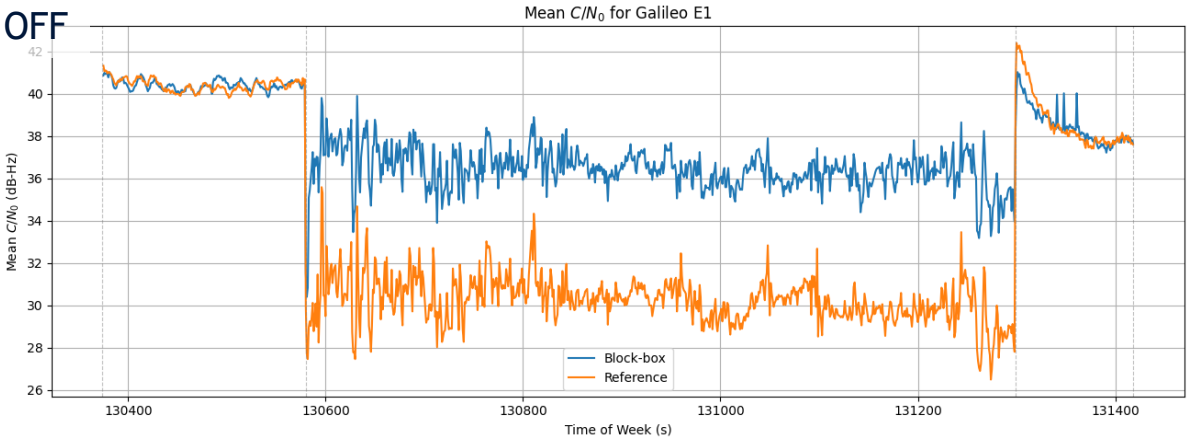
Ref WBI ON





Ref. WBI OFF



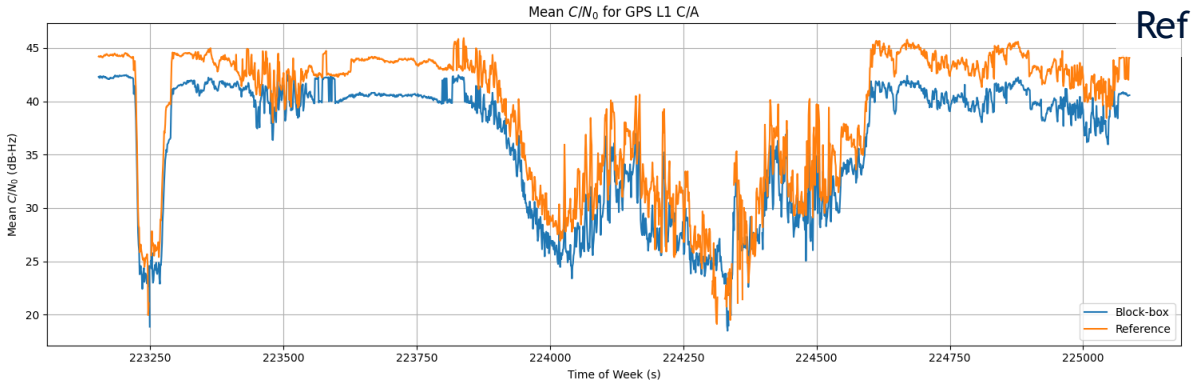


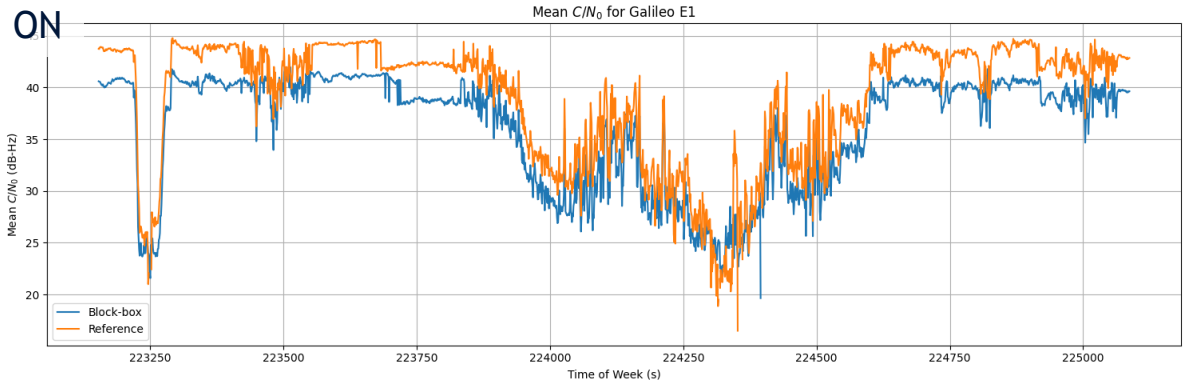
Experimentation results - J15

Results

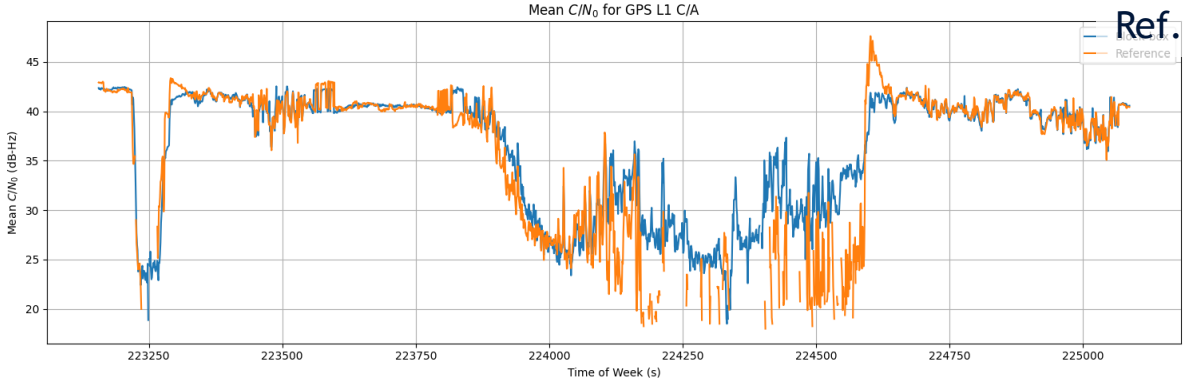
- Clear improvement of C/N_0 over the unprotected ref. receiver
- Slightly worse results than Septentrio's WB interference mitigation and notch filtering

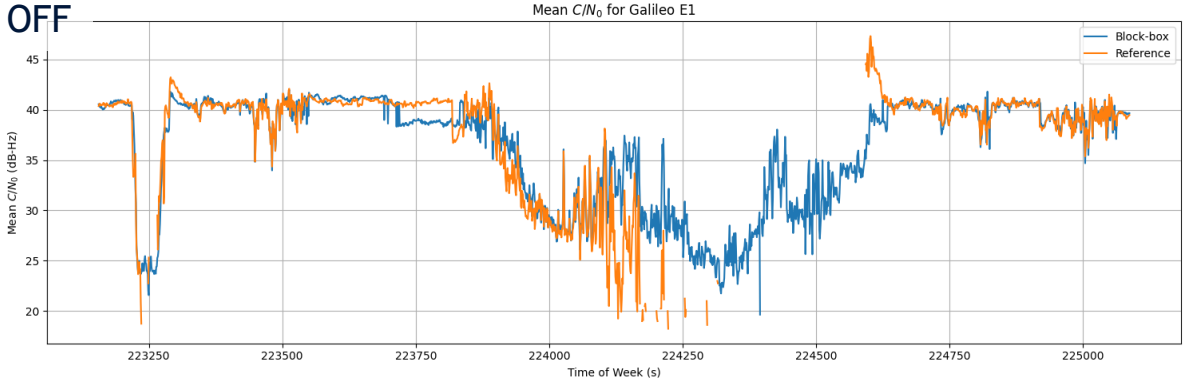
Ref WBI ON





Ref. WBI OFF





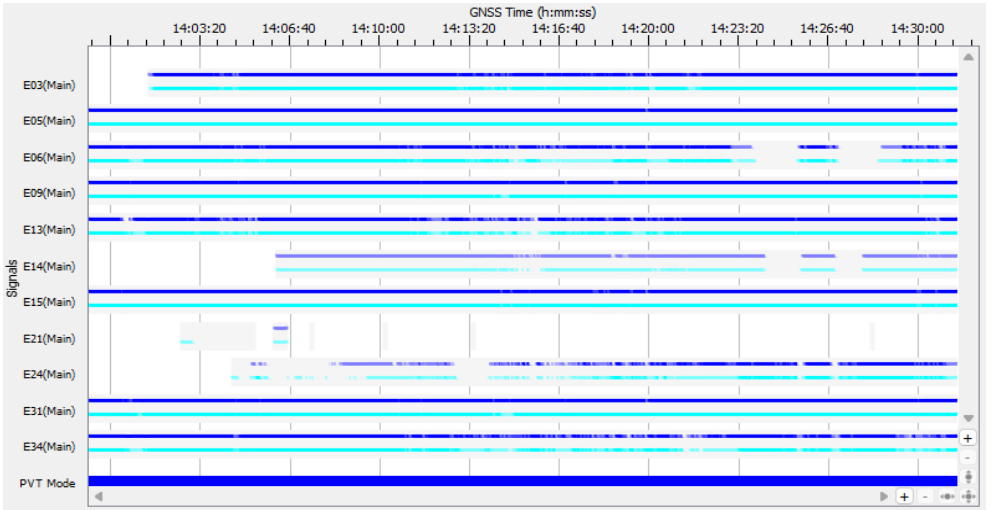
Experimentation results - J15

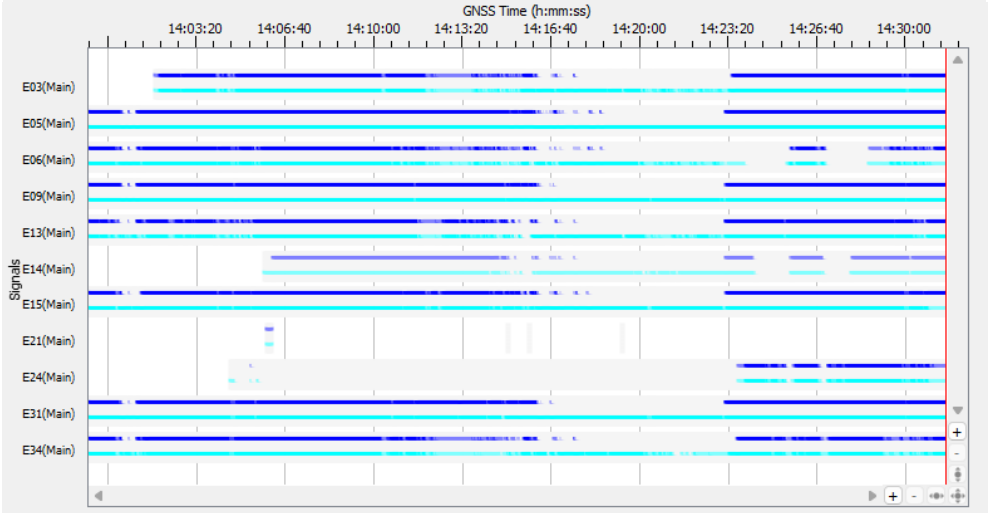
J15 position

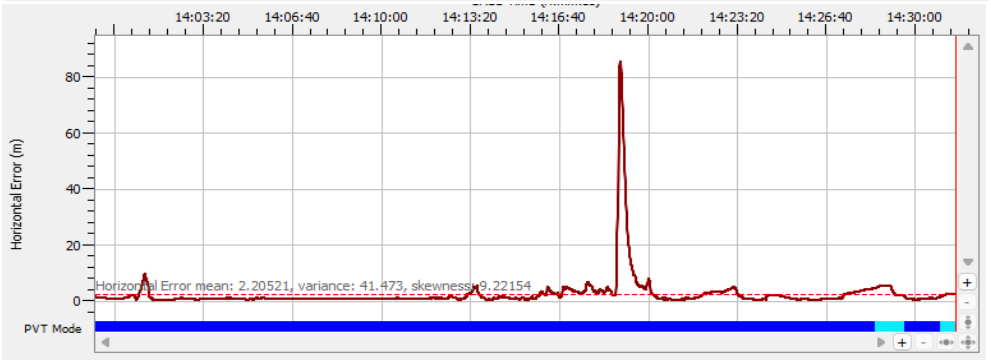
- Dynamic scenario
- Jamming effects on C/N_0
  - around 14:01
  - 14:15 – 14:23
- Jamming effects on PVT
  - Only the accuracy degradation
- Receiver was in dual frequency PVT mode
  - Only L1 signals affected
  - Receiver continued on E5

Block-box ptotected receiver

Reference receiver



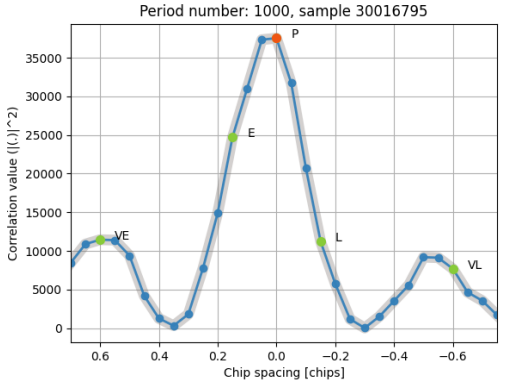


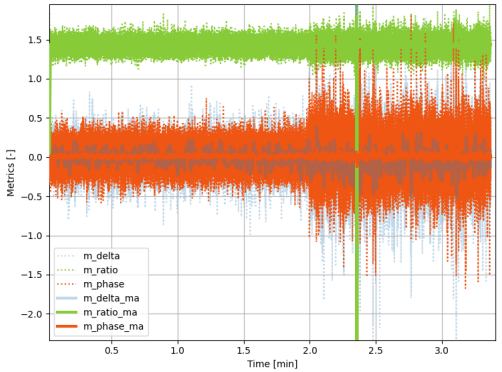


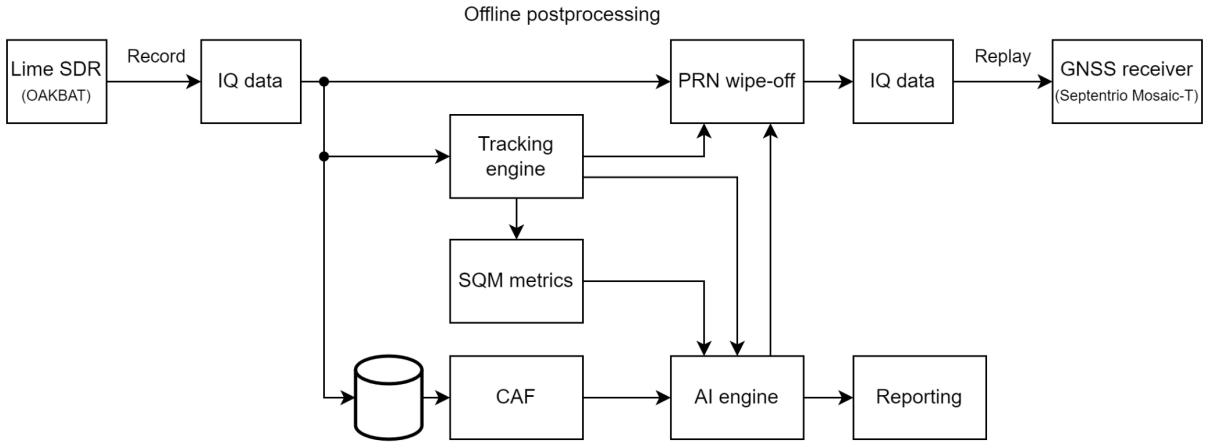
Spoofing detection & mitigation (offline E2E model)

AI detection

- Inference input:
  - Multi-correlator (30 taps)
  - SQM
    - Delta Metric $m_{delta} = \frac{I_{-d} - I_{+d}}{I_p}$
    - Ratio Metric $m_{ratio} = \frac{I_{-d} + I_{+d}}{I_p}$
    - Early Late Phase Metric $m_{elp} = \tan^{-1}\left(\frac{Q_{-d}}{I_{-d}}\right) - \tan^{-1}\left(\frac{Q_{+d}}{I_{+d}}\right)$
- Galileo E1
- Outlier detector / MLP
- Training data: Synthetic signals







DSP mitigation

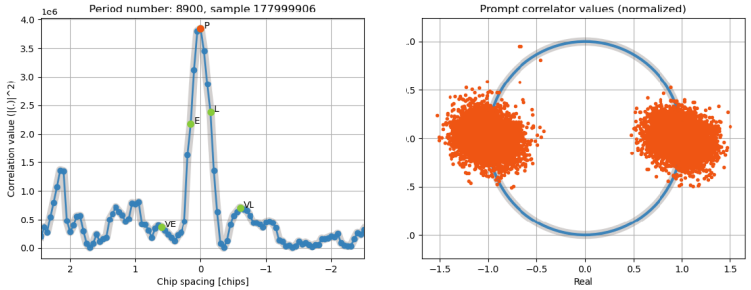
- Spoofer tracking
- PRN code wipe-off (both pilot and data component)
- Further development: tracking engine and mitigation unit in HW platform

Spoofing detection & mitigation (E2E model)

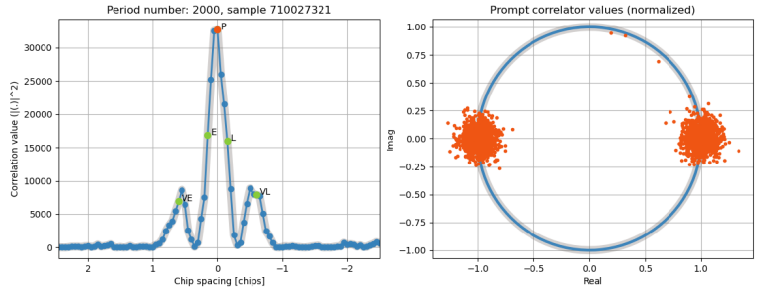
OAKBAT os10

- Static time push ~600 m
- 10 dB power advantage
- Spoofer detection and mitigation for SVID 21

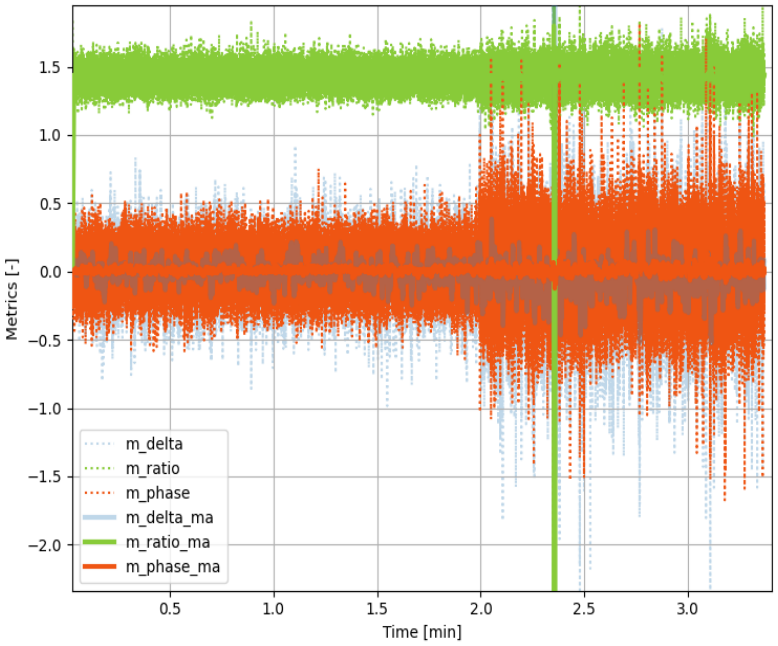
Detail: OAKBAT os10 mitigated

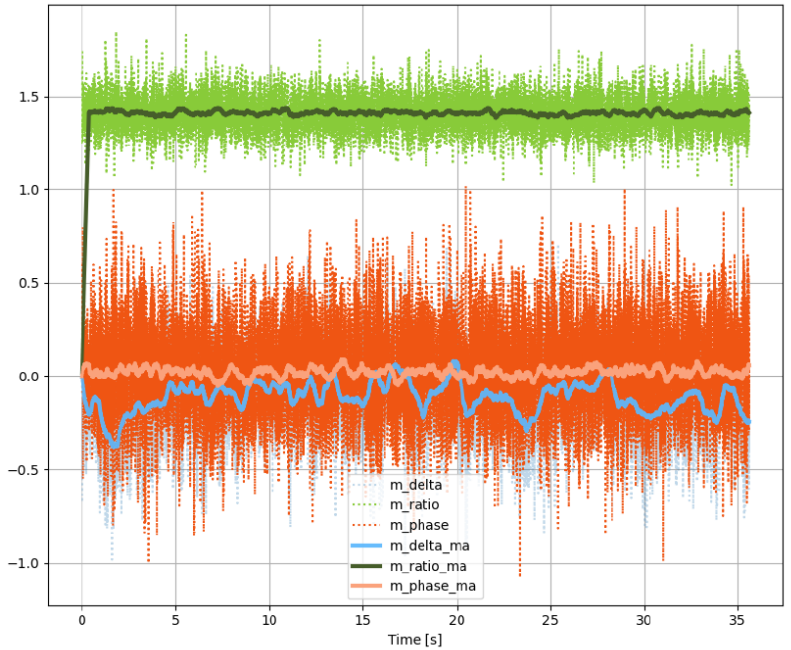


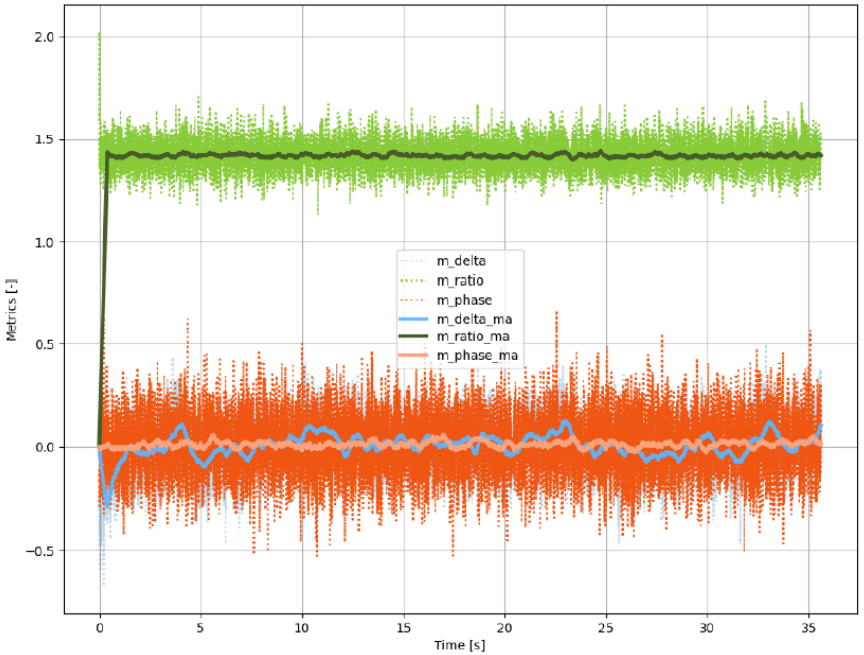
Detail: OAKBAT os10 clean



OAKBAT os10 spoofed



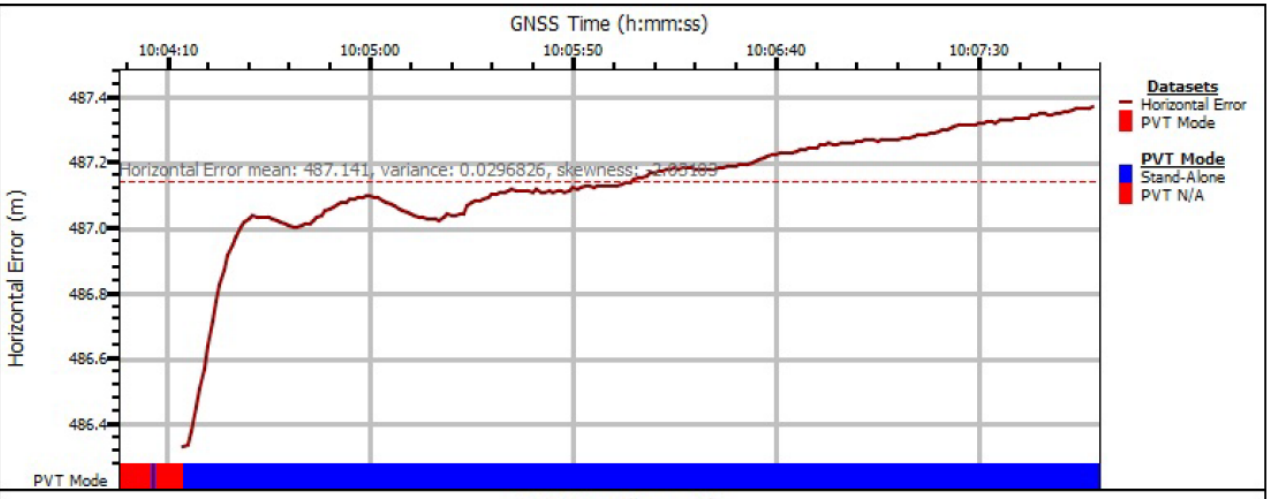


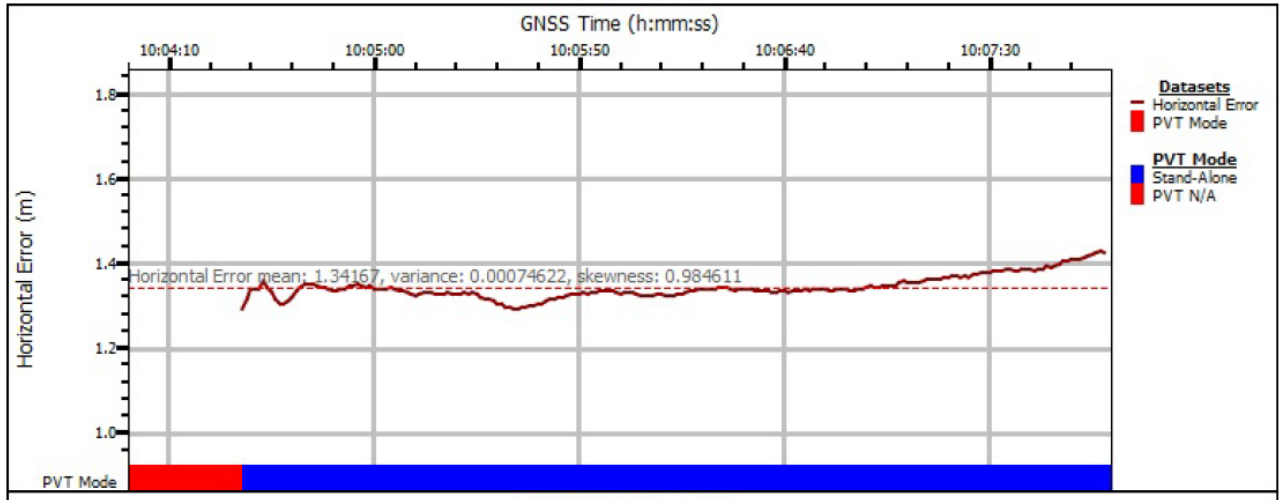


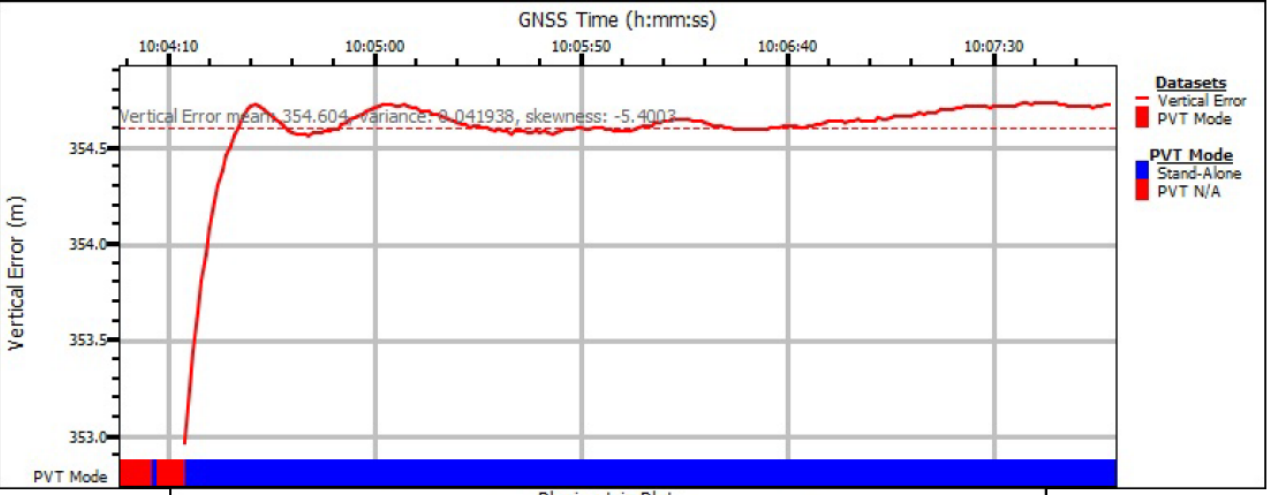
Spoofing detection & mitigation (E2E model)

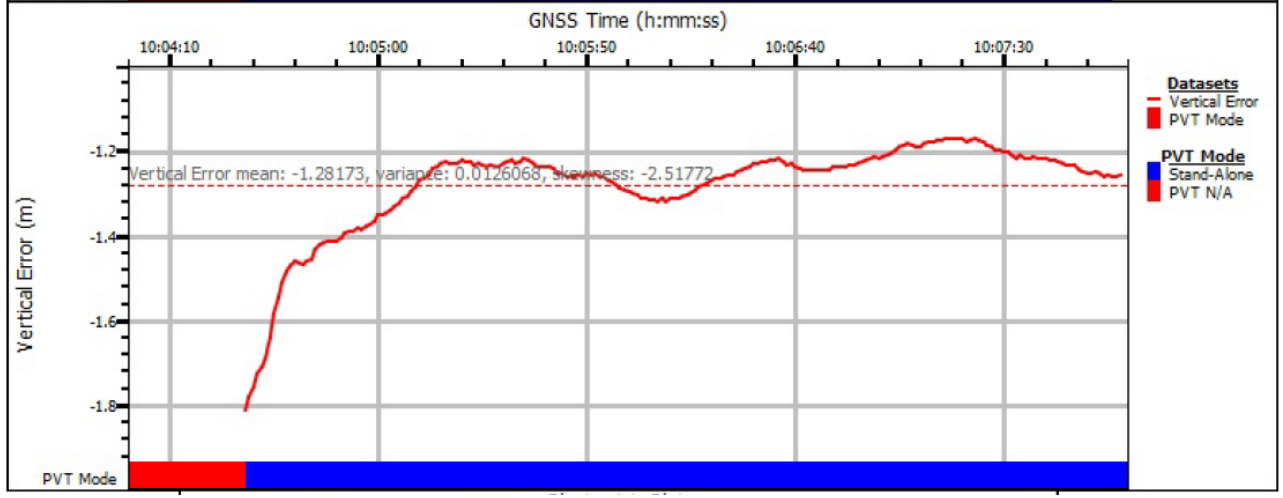
OAKBAT os12

- Static position push 600 m in ECEF Z axis
- Mitigation for 4 satellites (SVID 1, 4, 27, 36)
- Data and pilot spoofing correlation peak wipe-off









Strengths and weaknesses

Strengths

- Robust and powerful HW platform with the real-time processing capability
- Flexible jamming mitigation method effective against various types of jamming
- Record and replay capability
- 2 RF paths – dual antenna readiness

Weaknesses

- Broader real environment data collection and model training needed
- Evaluation of the performance with multipath, signal fading etc.
- Better testing equipment would be beneficial
- Spoofing mitigation only in postprocessing so far

huld

Exploitation proposed in Element 2

Future development plans

- Real-world data collections to improve AI models training
- Implementation of tracking engine and spoofing mitigation to the HW platform
- Experimentation with additional mitigation techniques
- Performance testing with more mature higher-fidelity test setup
- Support to antenna array or dual polarization antennas
- Transformation to the smaller form factor

Navisp element 2 considerations

- Robust record/replay unit for various RF bands (besides GNSS)
- Extension of the server/cloud application capabilities (offloading workload from local units more complex monitoring and threat evaluation)

huld

Benefits working with ESA

- ESA is setting the course for the future technologies and supporting EU industry development
- Connecting relevant businesses and individuals through organizing events and workshops
- Guidance from the top-notch professionals in the field
- Directing the development in the efficient path
- Support with testing HW and facilities
- Support with technical data needed for the successful project execution

Beyond tomorrow