NEW CONCEPT FOR EVOLUTIVE MITIGATION OF RFI TO GNSS

ANTIFERENCE

FINAL PRESENTATION

15.07.2022

AGENDA

1 Project introduction

2 System concept and technical scope

3 Presentation of Antiference system

4 Presentation of main results

5 Conclusions & way forward

1

PROJECT INTRODUCTION

PROJECT OVERVIEW

FACTS & FIGURES

Programme

- NAVISP – EL1 – 051
- New Concept for Evolutive Mitigation of RFI to GNSS (Antiference)

Duration

- 18 months
- 01/2021 – 06/2022

Project Team

- OHB Digital Solutions GmbH (OHB)
- Science & Technology (S&T)
- IntegriCom (IC)

MOTIVATION

MAIN PROJECT GOALS

PROJECT GOALS

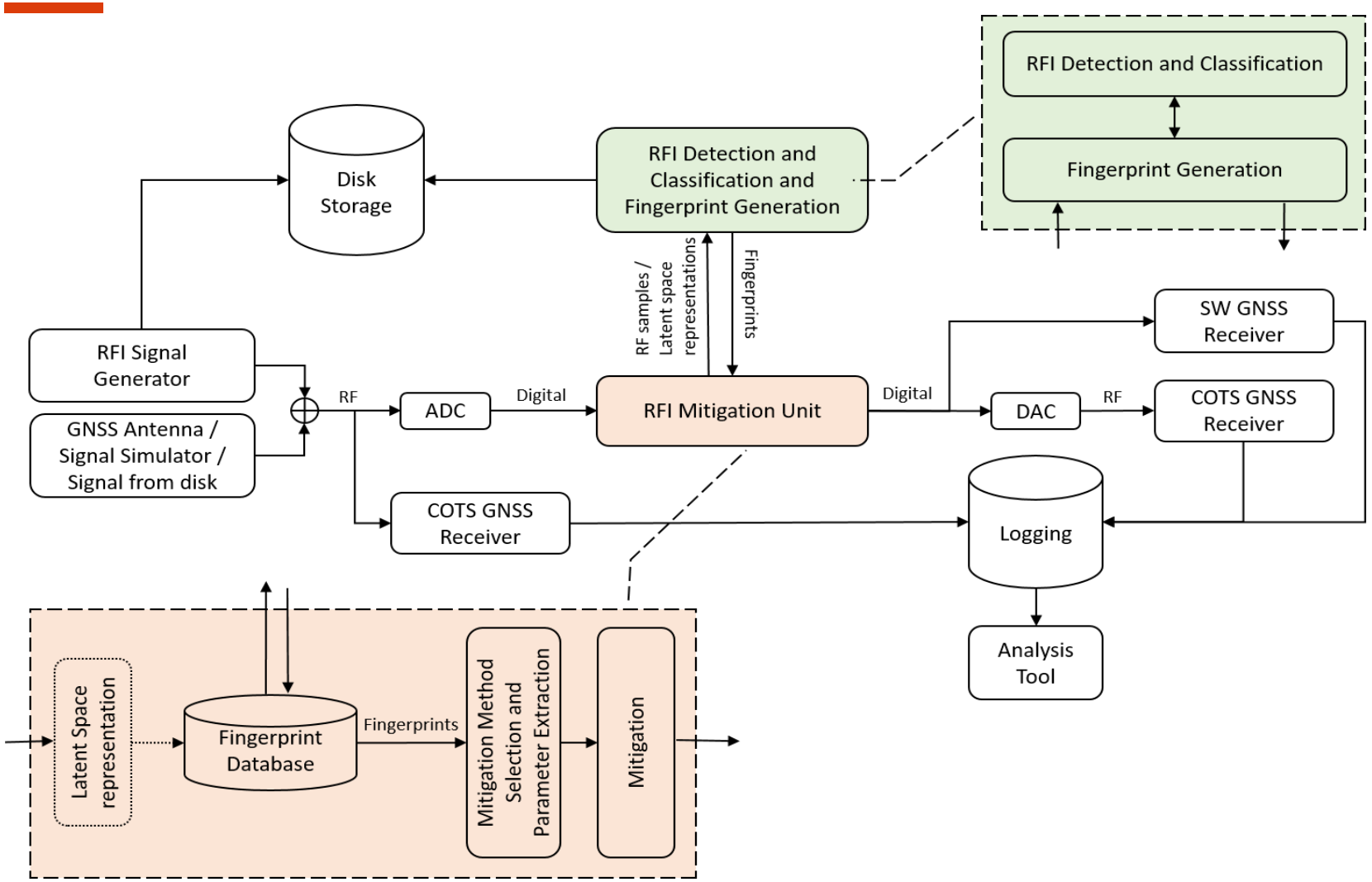
- Investigation of the feasibility of flexible and reconfigurable Digital Signal Processing (DSP) techniques for GNSS interference mitigation using ML-techniques
- Investigation of methods for the identification of new GNSS interference and fingerprint extraction, allowing to reconfigure the DSP to effectively mitigate them
- Validate the proof of concept (PoC) via breadboarding and demonstration

HERITAGE

- GNSS record-replay system (MGSE)
- GNSS simulator including RFI simulation (GIPSIE)
- Recorded real-world test data
- ML environment for development
- SDR-based and COTS receivers for validation

HIGH-LEVEL SYSTEM CONCEPT

BLOCK DIAGRAM OF COMPONENTS

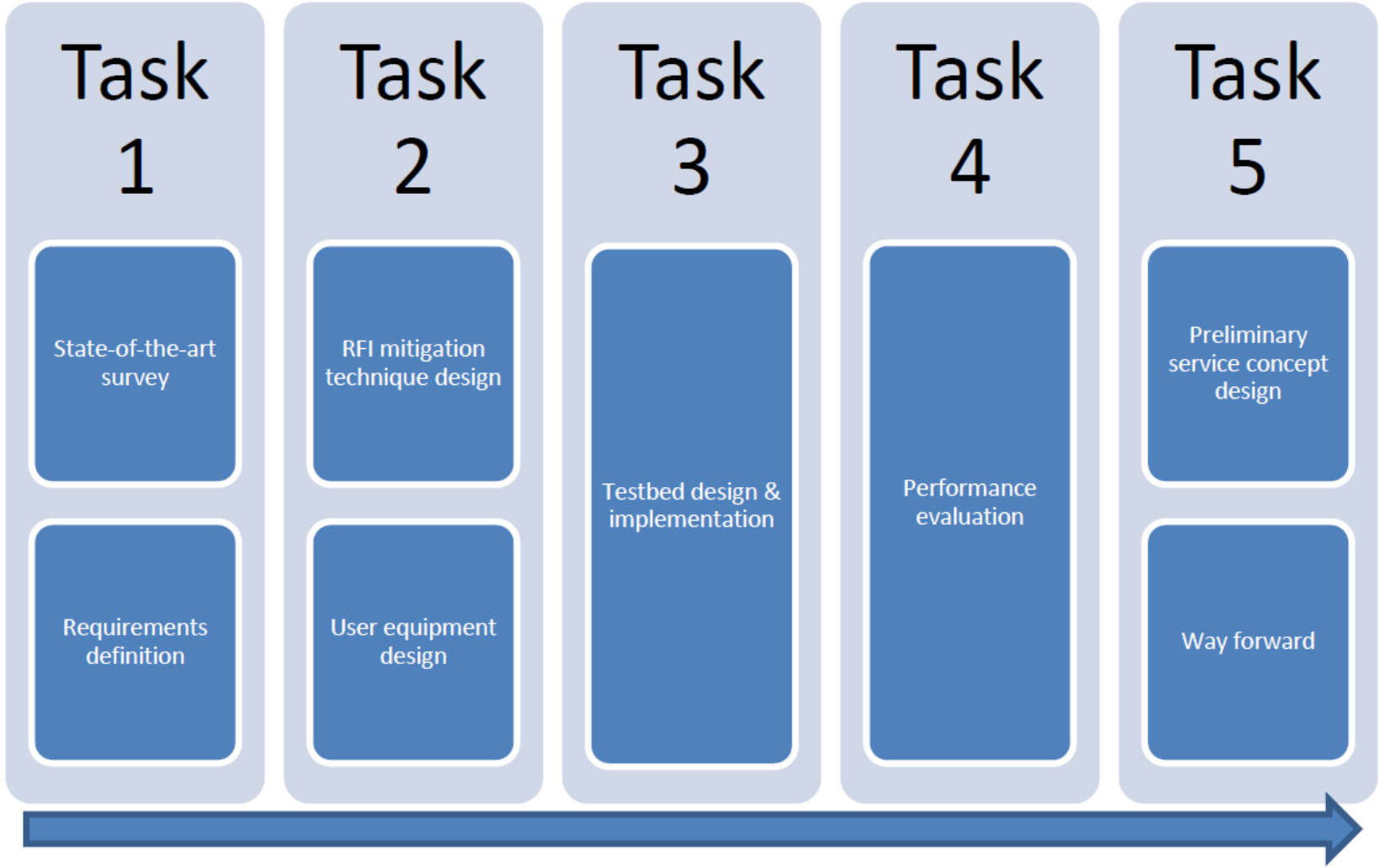


MAIN COMPONENTS

- MGSE record-replay system
- GIPSIE GNSS signal simulator
- Fingerprint database
- RFI detection and classification
- RFI mitigation unit
- SW & COTS GNSS Receiver
- Results analysis tool

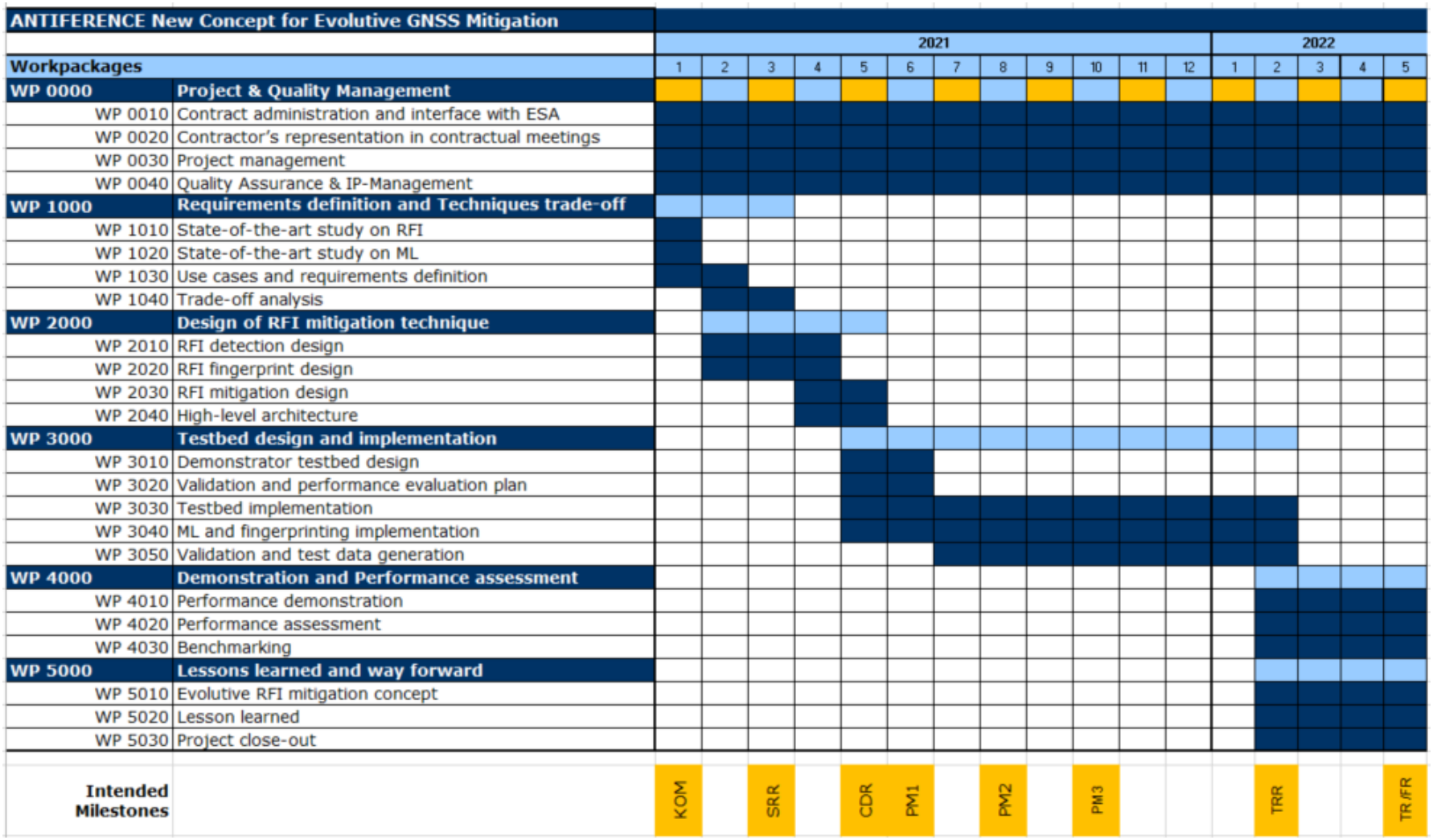
WORK LOGIC

DEVELOPMENT TASKS AS GIVEN IN ESA ITT



GANTT CHART

SCHEDULE & WORK PACKAGES



ANTIFERENCE New Concept for Evolutive GNSS Mitigation		2021												2022				
Workpackages		1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5
WP 0000	Project & Quality Management																	
WP 0010	Contract administration and interface with ESA																	
WP 0020	Contractor's representation in contractual meetings																	
WP 0030	Project management																	
WP 0040	Quality Assurance & IP-Management																	
WP 1000	Requirements definition and Techniques trade-off																	
WP 1010	State-of-the-art study on RFI																	
WP 1020	State-of-the-art study on ML																	
WP 1030	Use cases and requirements definition																	
WP 1040	Trade-off analysis																	
WP 2000	Design of RFI mitigation technique																	
WP 2010	RFI detection design																	
WP 2020	RFI fingerprint design																	
WP 2030	RFI mitigation design																	
WP 2040	High-level architecture																	
WP 3000	Testbed design and implementation																	
WP 3010	Demonstrator testbed design																	
WP 3020	Validation and performance evaluation plan																	
WP 3030	Testbed implementation																	
WP 3040	ML and fingerprinting implementation																	
WP 3050	Validation and test data generation																	
WP 4000	Demonstration and Performance assessment																	
WP 4010	Performance demonstration																	
WP 4020	Performance assessment																	
WP 4030	Benchmarking																	
WP 5000	Lessons learned and way forward																	
WP 5010	Evolutive RFI mitigation concept																	
WP 5020	Lesson learned																	
WP 5030	Project close-out																	
Intended Milestones		KOM		SRR		CDR	PM1		PM2		PM3				TRR			TR/FR

2

SYSTEM CONCEPT AND TECHNICAL SCOPE

USER REQUIREMENTS

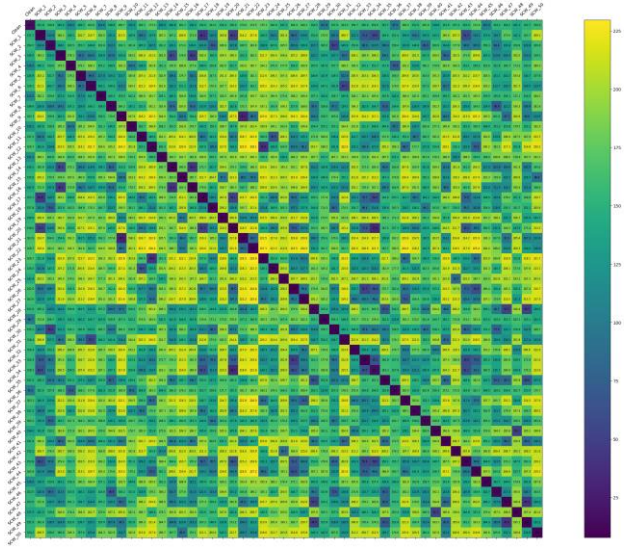
- User requirements were investigated for numerous user communities
  - We selected automotive users as a suitable target community
  - Quantitative and qualitative requirements on interference and spoofing resistance start appearing
- CEN/CENELEC standards
  - PVT Performance metric degradation on 50%,75%,95% percentiles (metrics: accuracy, integrity, continuity,…)
- ETSI standards
  - Robustness based on ‘the maximum tolerable Jamming to GNSS Signal power ratio’
- Conclusion
  - Requirements provide limited guidance and or not (yet) state-of-the-art
    - Explicitly under development (even more so for spoofing)
    - Not really suitable to design RFI detection and mitigation methods against

FINGERPRINT DATABASE

DETECTION/CLASSIFICATION BASED ON FINGERPRINTING

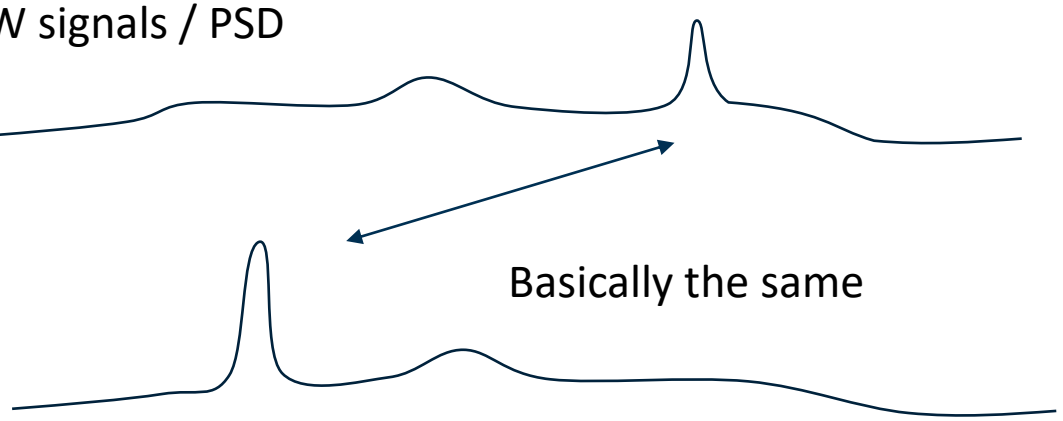
WORKING PRINCIPLE

- Fingerprint is a “summary” of the RF environment, relevant for GNSS
- One main feature included is PSD
- The PSD of two CW jammers are identical, except for irrelevant differences
- We use distance d(fp1, fp2) to distinguish different RF situations
- d(CW1, CW2) should be almost 0 (also true for other types of RFI)



Clean signal / PSD

CW signals / PSD



TESTBED

BLOCK DIAGRAM

Graphical User Interface

RFI Signal Generator

GNSS Antenna

RF

ADC

DAC

Digital

ANTIFERENCE

Digital

DAC

MGSE

COTS GNSS Rx (w. RFI mitigation)

COTS GNSS Rx (wo. RFI mitigation)

RF

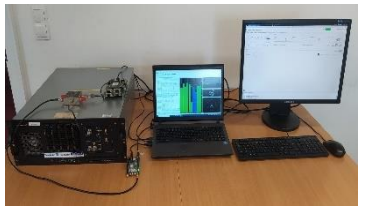
Logging

Analysis Tools

SW GNSS Receiver (SDR)

COTS GNSS Rx (wo. RFI mitigation)

RF

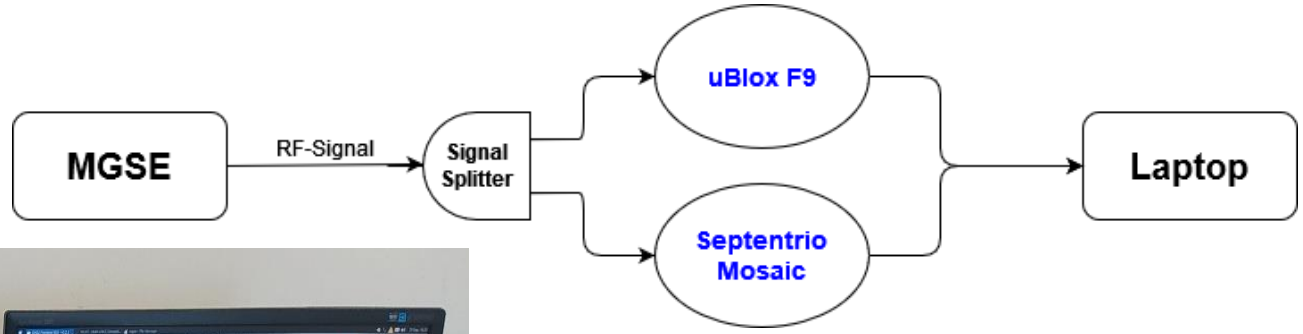


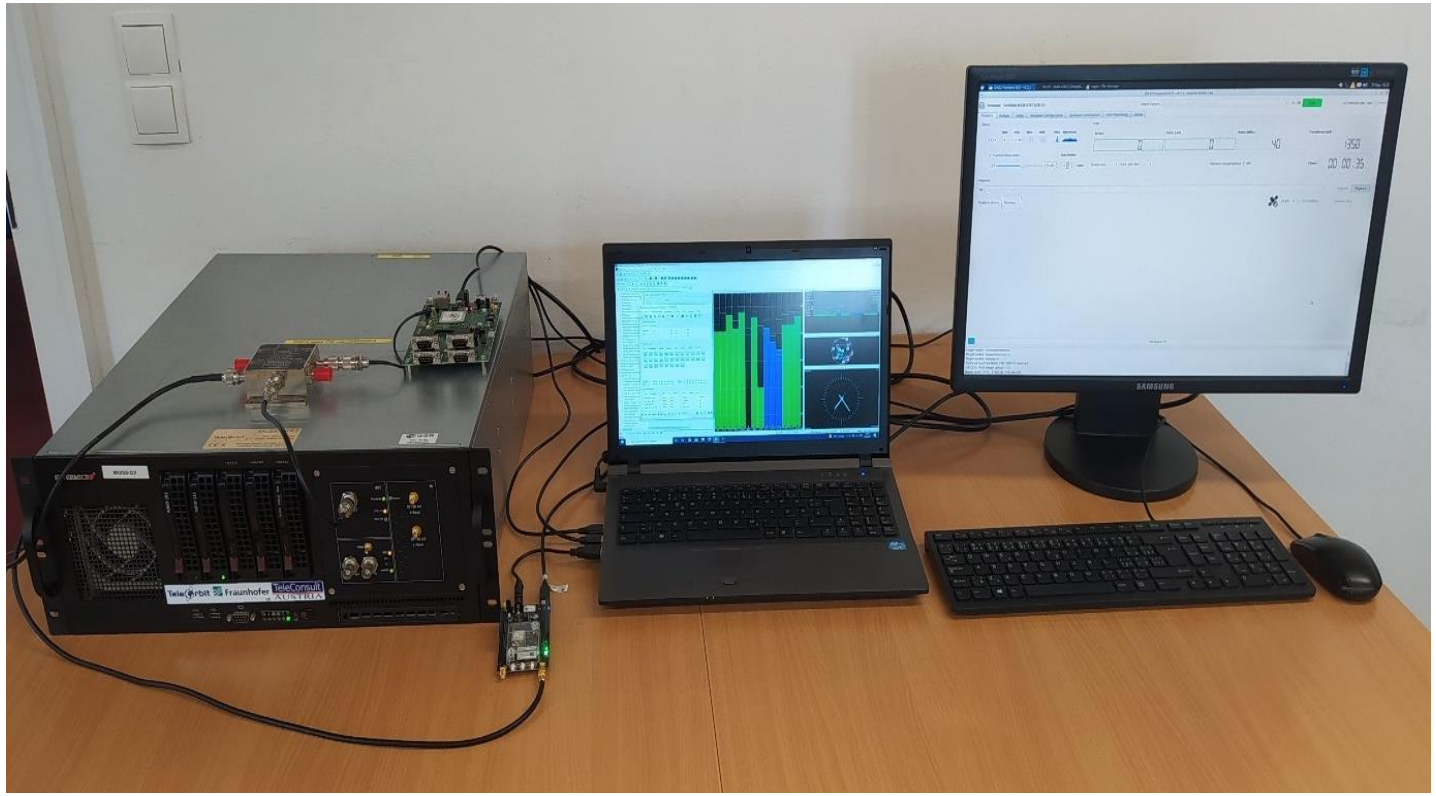
COTS receivers:

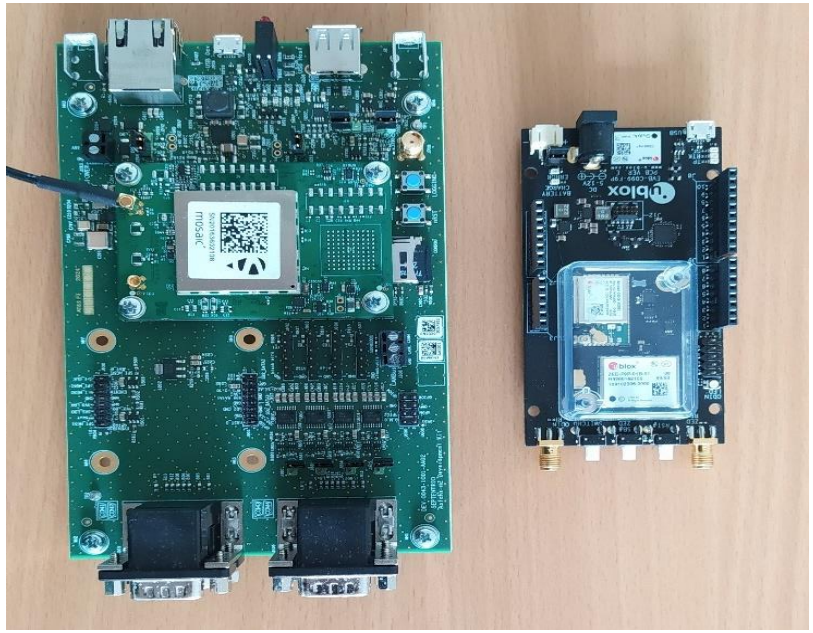
- Ublox ZF9P
- Septentrio Mosaic

SIGNAL REPLAY TO RECEIVERS

SET-UP







3

PRESENTATION OF ANTIFERENCE SYSTEM

MACHINE LEARNING

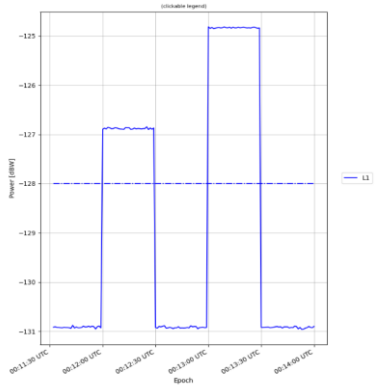
RFI TYPES AND FEATURES USED FOR DETECTION – JAMMING (1)

- Detection module is able to distinguish between 8 jamming environments
- Detection module works on short data slices (<1ms)

- Fairly recognizable using:
  - Statistical test: kurtosis value
  - Power detection

    => Both values are added to ML features

- Limitation: detects jamming but does not recognise its type

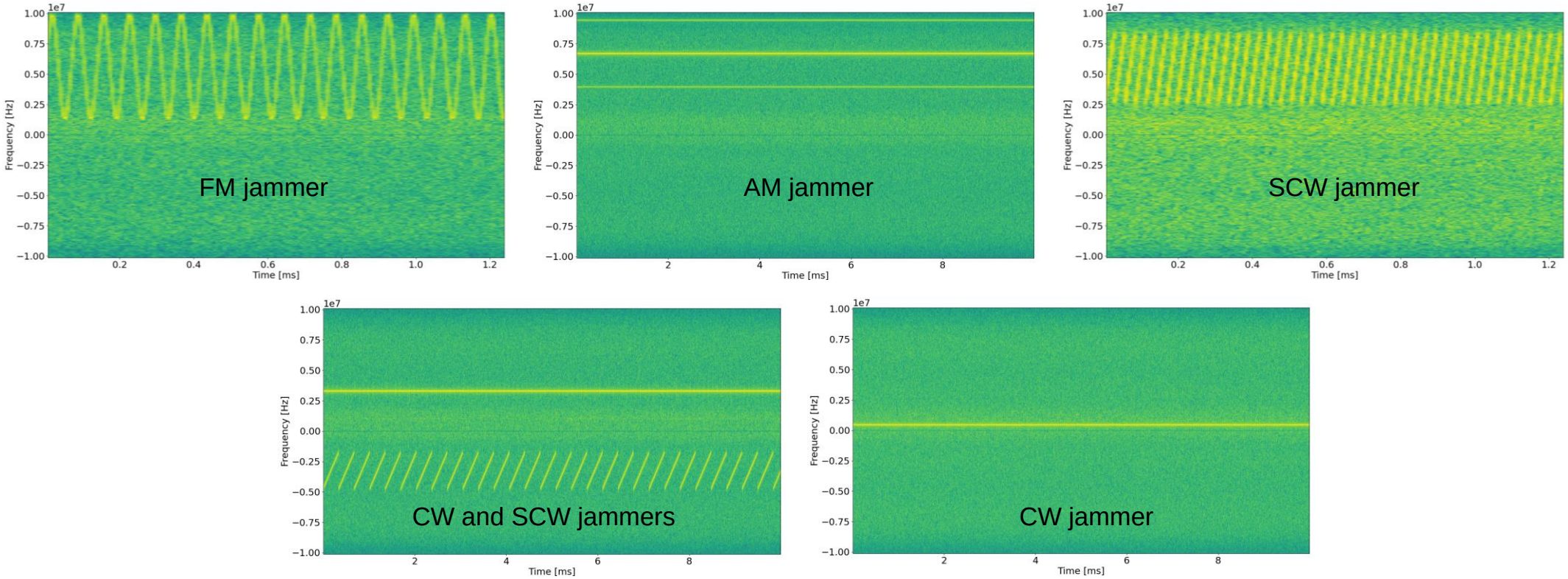


Jamming scenario	Kurtosis value
Clean signal	**2.999**
AM	2.67
CW	2.51
SCW	2.5
FM	2.42
WGN	2.999
Multiple jammers	2.57

MACHINE LEARNING

RFI TYPES AND FEATURES USED FOR DETECTION – JAMMING (2)

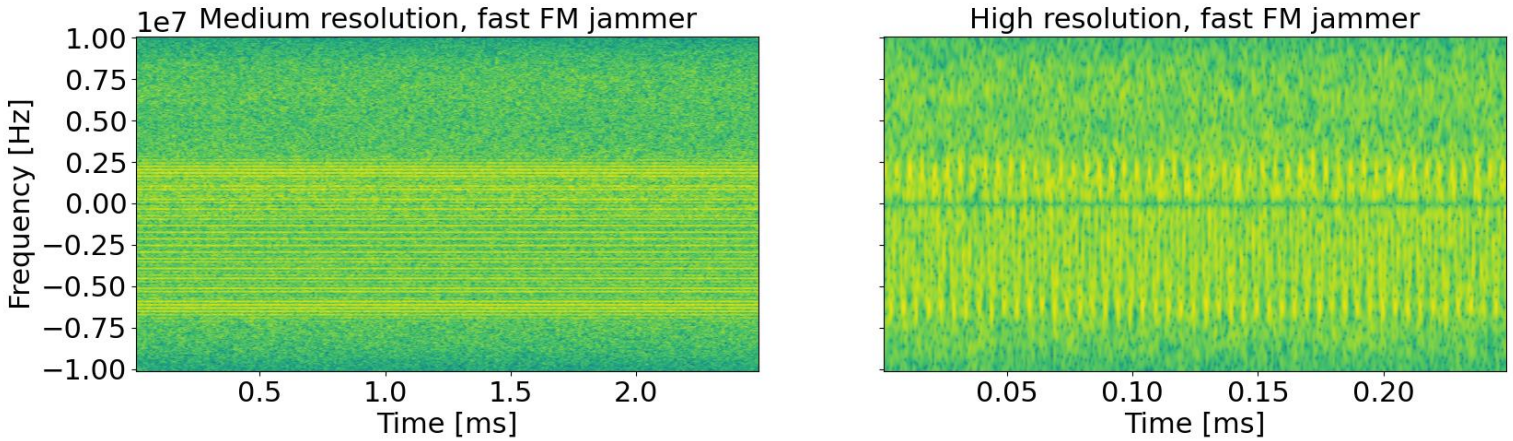
- Type of jamming can be characterized using spectrogram of the signal
- Shows clear, identificable patterns per type of RF content
- Limitation: spectrogram works best when tailored to spectral characteristics
- Modifying preprocessing as function of expected outcome is undesirable
- Would bias ML training



MACHINE LEARNING

RFI TYPES AND FEATURES USED FOR DETECTION – JAMMING (3)

- Compromise solution: add two spectrograms to ML features
  - One of entire data slice, with resolution suitable for jammers with low time variation frequency
  - One of 1/10th of data slice, with higher time resolution suitable for jammers with higher variation frequency

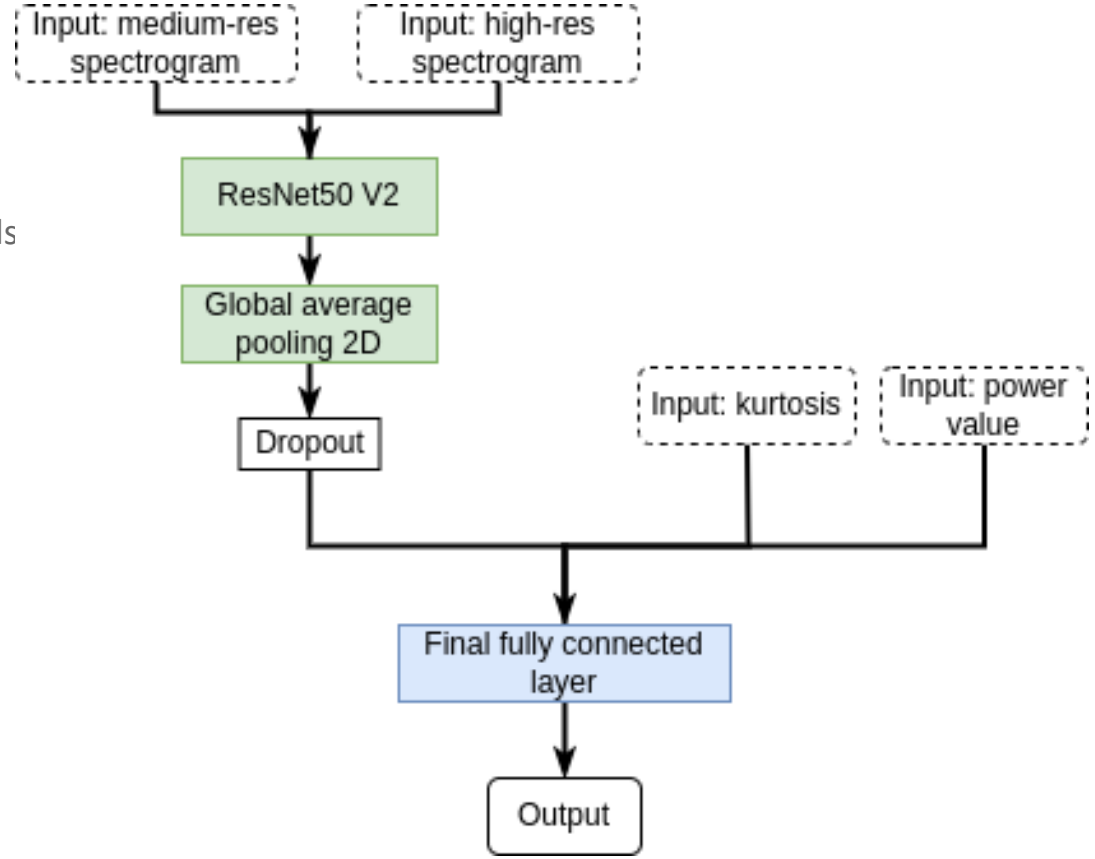


- Detection of spoofing:
  - Detection module works on the same short data slices (<1ms)

ML ARCHITECTURE

JAMMING DETECTION / CLASSIFICATION

- Built using transfer learning from ResNet-50 V2 model
- Two main parts:
  - Feature extraction from spectrograms (green)
  - Combination with additional info into decision layer (blue)
- Architecture and learning params selected using bayesian optimisation methods
- Trained using Adam algorithm



JAMMING DETECTION/CLASSIFICATION

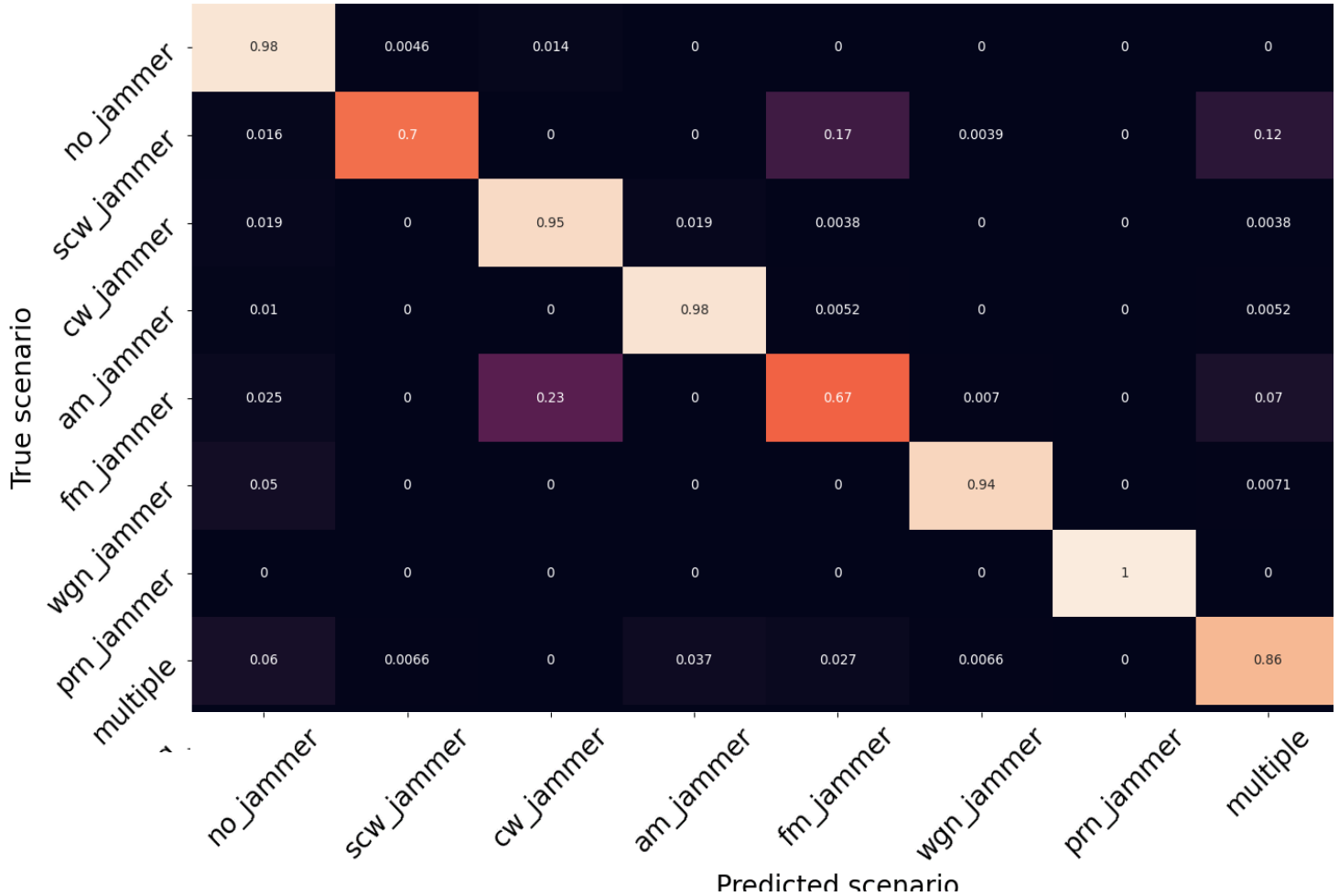
ML-MODEL RESULTS WITH POST-PROCESSING

CONCLUSIONS

- Very promising detection performance (detection rate > 0.94)
- Mostly very good classification performance
  - typical recognition rate > 0.9
  - worst case jamming scenarios: SCW and FM → misclassification due to spectral similarities
- Very low false alarm rate (= 0.02)

FINGERPRINT CONTENT

- PSD of signal, divided by reference clean signal, and normalized
- Kurtosis
- Average power



SPOOFING DETECTION

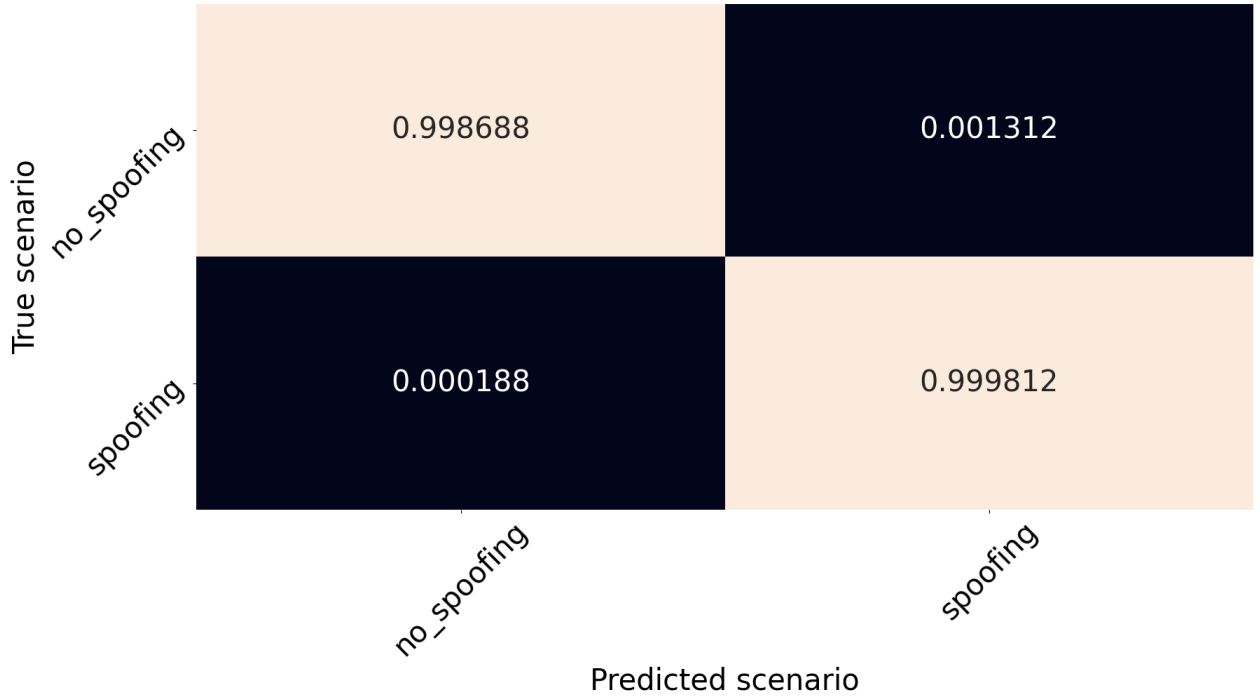
ML-MODEL RESULTS

CONCLUSIONS

- Excellent performance
- Accuracy >99.8%
- ROC AUC > 99.9%
- False alarm rate = 0.13%

FINGERPRINT CONTENT

- SPCA T-statistic
- Kurtosis
- Average power



4

PRESENTATION OF MAIN RESULTS

NUMBER OF SAMPLES

OVERALL AND PER RFI TYPE/ENVIRONMENT

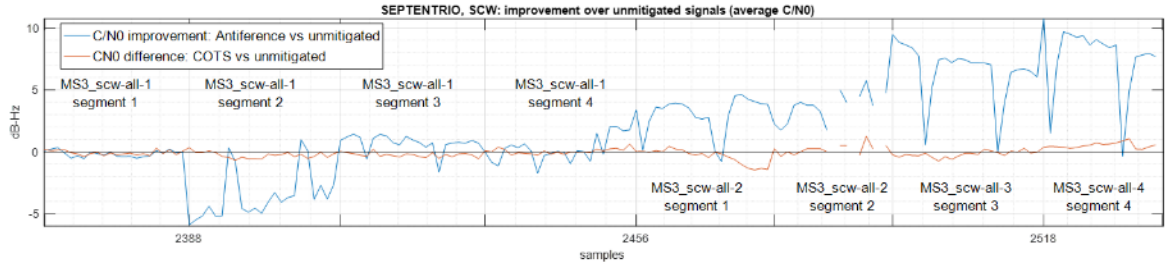
Receiver and Mitigation	Number of samples	Number of segments
Septentrio, no mitigation	37066	156
ublox, no mitigation	-	-
Septentrio, COTS mitigation	39703	158
ublox, COTS mitigation	33380	147
All receivers, all mitigations	110149	461

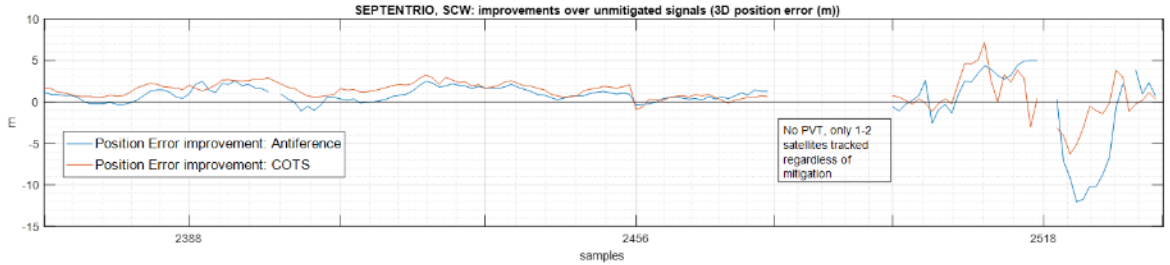
RFI	Any Environment	Open Sky	Urban Short	Urban Tall	Wooded	Remarks
Clean	72372	59208	3009	5894	3715	Includes receiver initialization segments
AM	1609	786	466	246	99	
CW	1417	812	155	246	192	
FM	1488	917	311	104	156	
PRN	2321	2321	-	-	-	
SCW	8321	8321	-	-	-	
SPOOFING	5562	5562	-	-	-	
SYSTEMATIC	1456	1456	-	-	-	
WGN	1537	1117	-	107	312	
DUAL	2301	764	468	541	504	

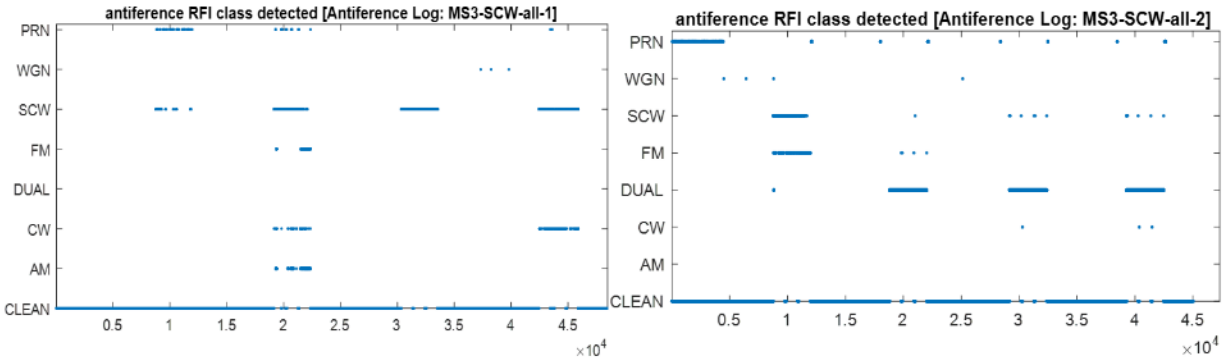
PERFORMANCE ANALYSIS

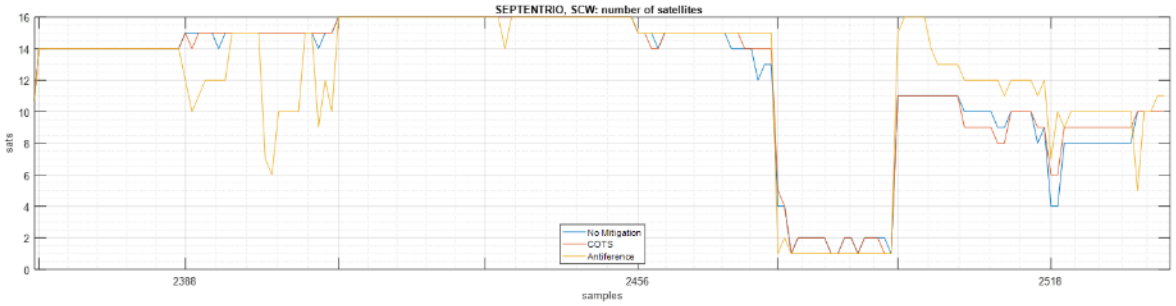
SCW MITIGATION

- Every attack contains regularly spaced ‘CLEAN’ segments
  - NOT missed detection, but artifact of restarting the jammers every 30 seconds (Seetaler 2021 data)
  - Also seen for other types of jammers
- Antiference gives, worse C/N0 for some sections, much improved C/N0 for others, while COTS mitigation does very little
- Explanation:
  - Mitigation of low power SCW removes more signal than RFI (SCW-ALL-1 segment 2), so Antiference should be made less sensitive
  - SCW-ALL-2 has higher power and Antiference improves C/N0 much better than COTS mitigation



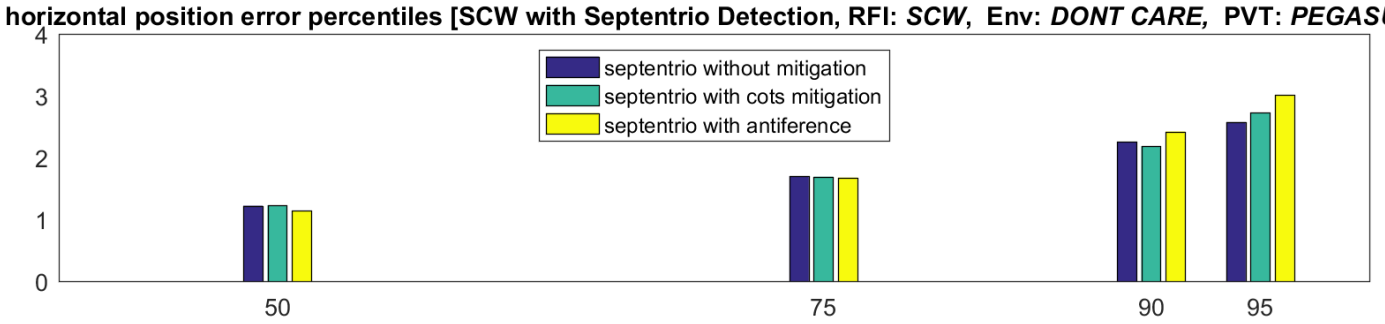


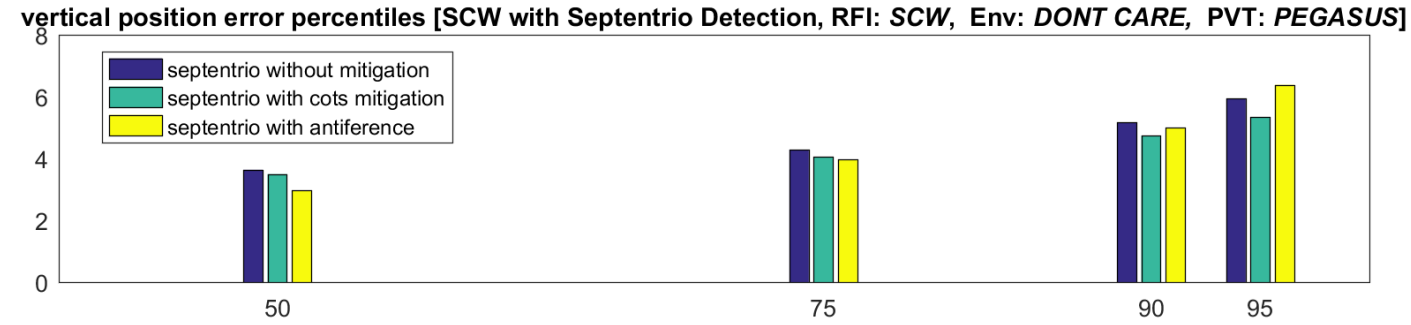


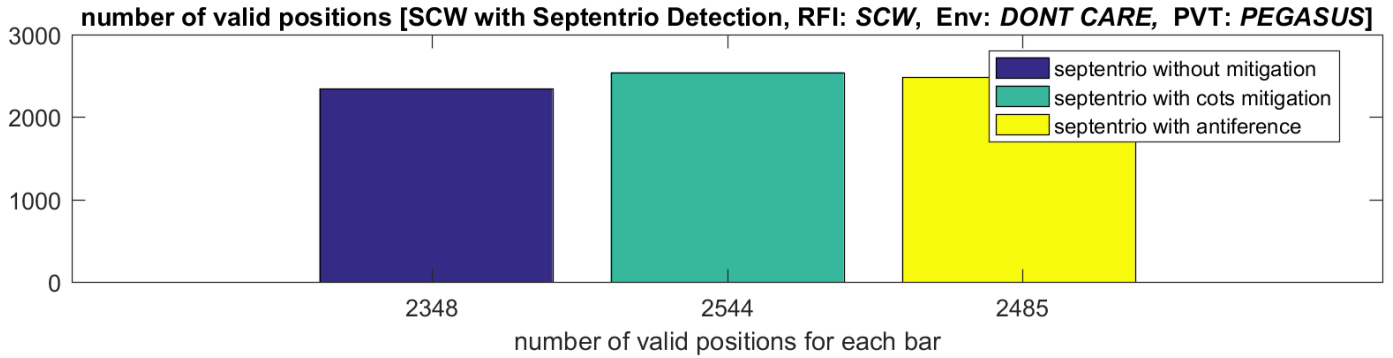


PERFORMANCE ANALYSIS: OVERALL OF ANTIFERENCE VS COTS

STATIC SCENARIOS: SCW



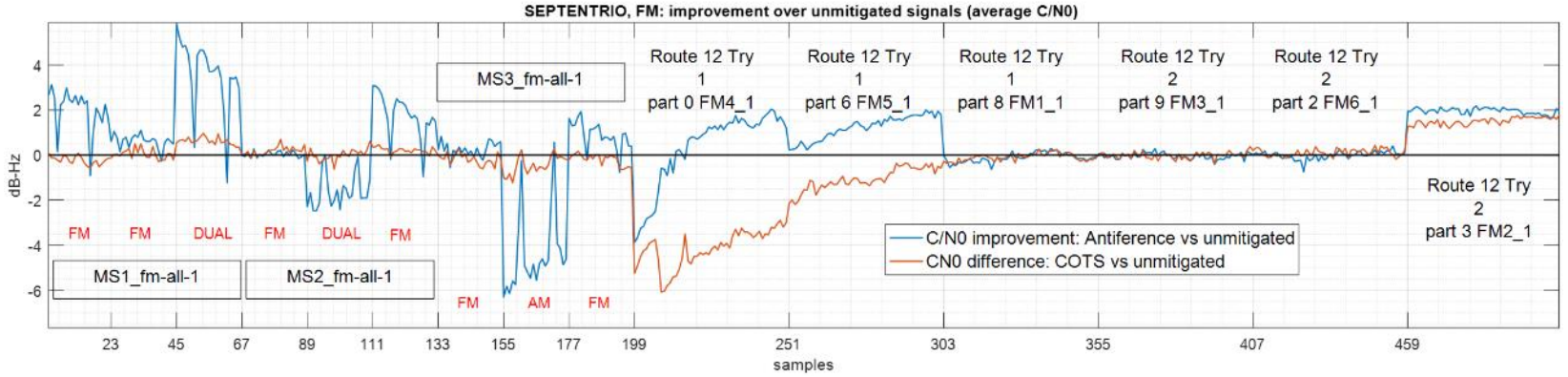


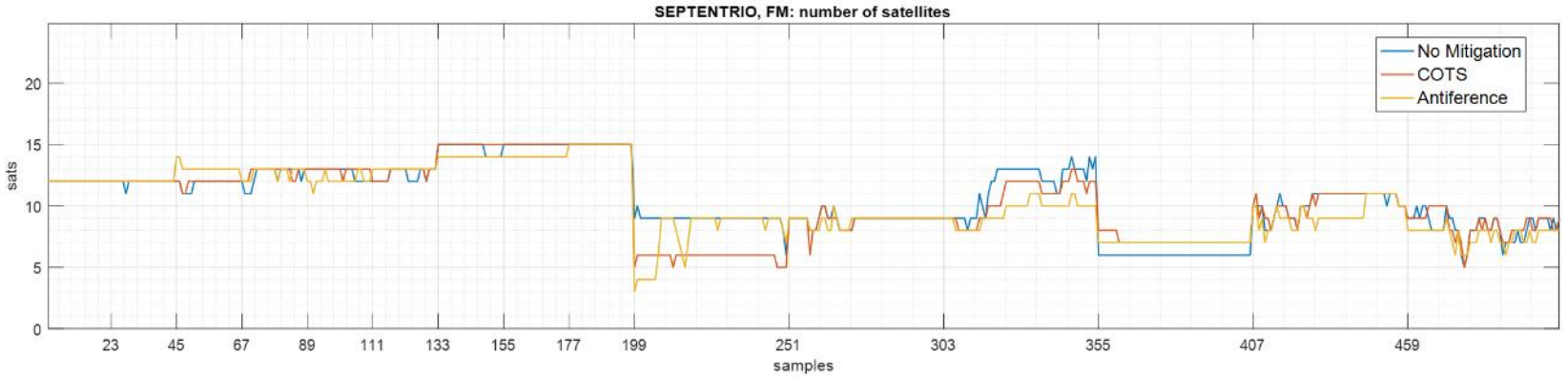


PERFORMANCE ANALYSIS

FM MITIGATION

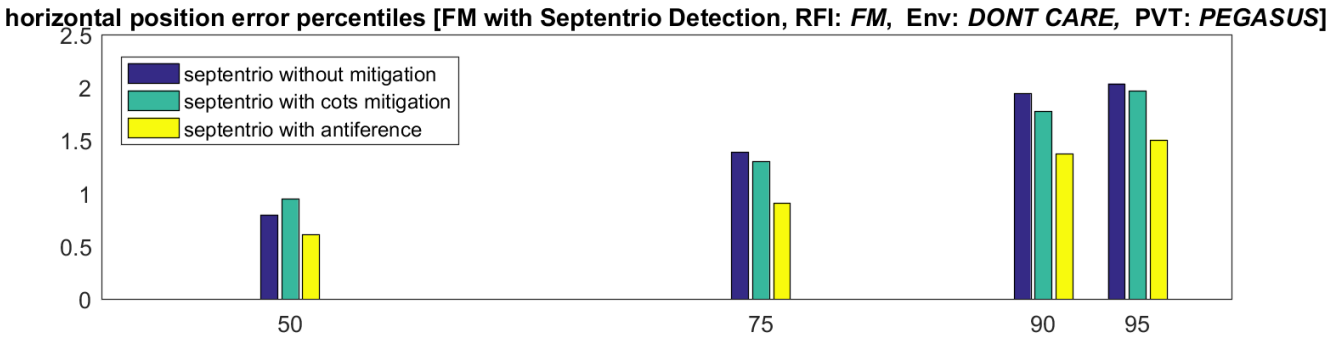
- Overall picture: Antiference works better than COTS
  - C/N0 improvement drops to zero due to 1s interruption of the jamming
- MS2-FM-ALL2, MS3-FM-ALL-1 are the exception with lower C/N0
  - Coincides with missed classifications and suboptimal mitigation
  - Low-power jamming, MS2 and MS3 receivers at larger distance than MS1
- Route 12 Try 2 Part 2 (FM6_1) is exception with bad PVT
  - Weak FM, often classified as WGN and not mitigated (but C/N0 is mostly flat)
  - Less satellites with Antiference

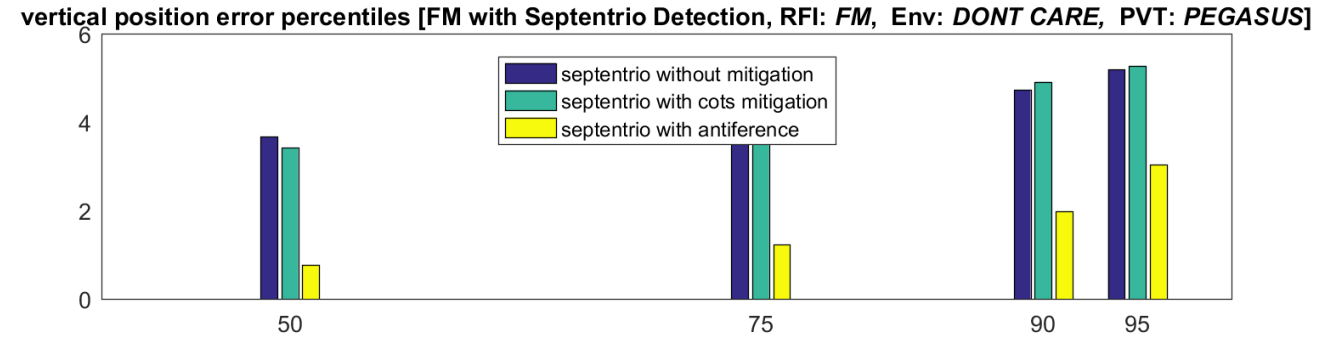


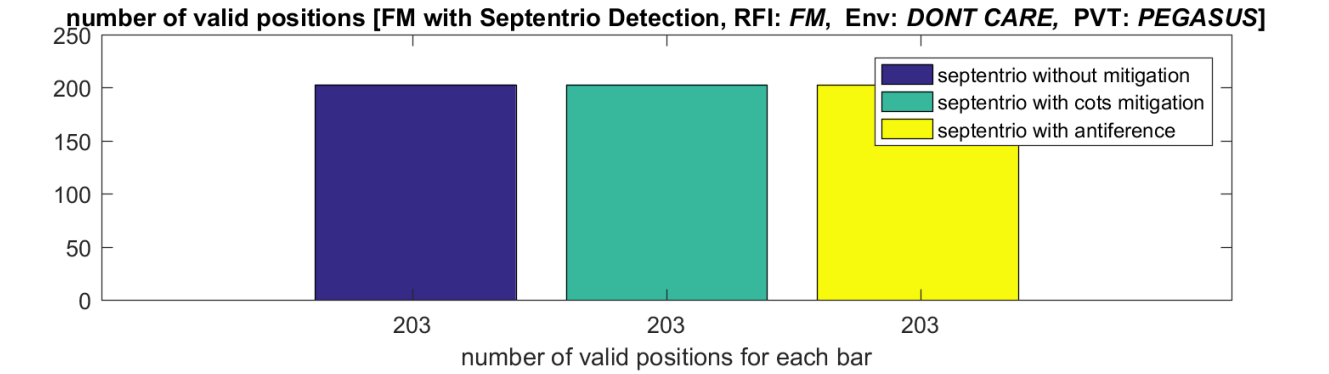


PERFORMANCE ANALYSIS: OVERALL OF ANTIFERENCE VS COTS

STATIC SCENARIOS:FM



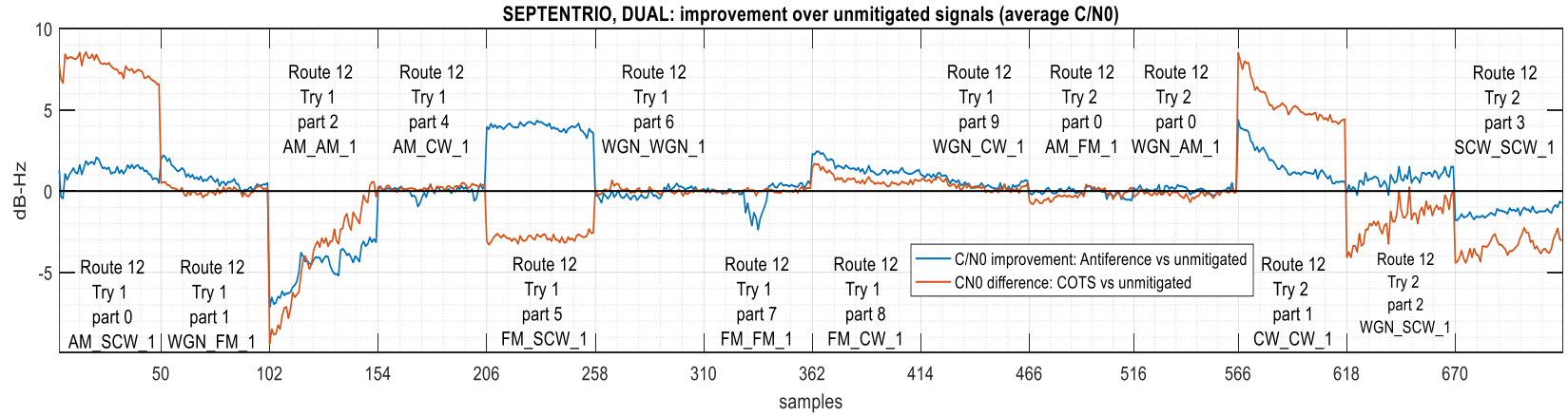


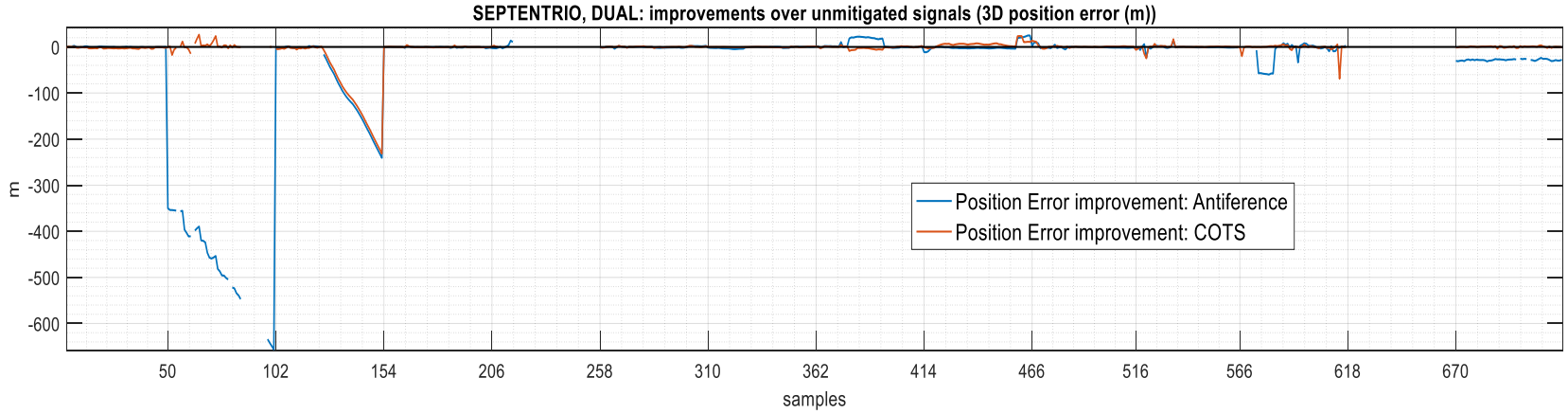


PERFORMANCE ANALYSIS

DUAL MITIGATION

- Overall picture Antiference has better C/N0 than COTS
  - Try 1 part 1 (WGN+FM)
  - Try 1 part 5 (FM+SCW),
  - Try 1 part 8 (FM+CW),
  - Try 2 part 2 (WGN+SCW),
  - Try 2 part 3 (SCW+SCW),
- while COTS performs better for:
  - Try 1, part 0 (AM+SCW),
  - Try 2, part 1 (CW+CW).
- Route 12 Try 1 Part 1 WGN+FM, Part 2 AM+AM have bad PVT with linear drift
  - Unstable clock, bad pseudoranges
  - Receiver tracking loop related





LIMITATION WORKING WITH DIGITIZED SIGNALS

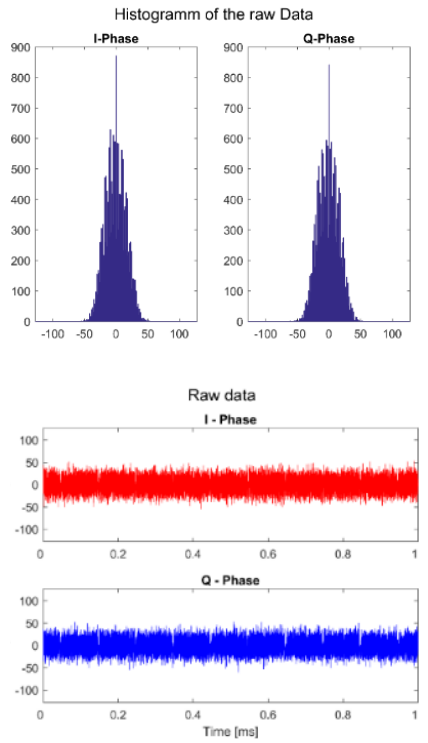
ANF FOR MITIGATION VS. JAMMING/RFI POWER

EXPERIENCED MITIGATION LIMITATION

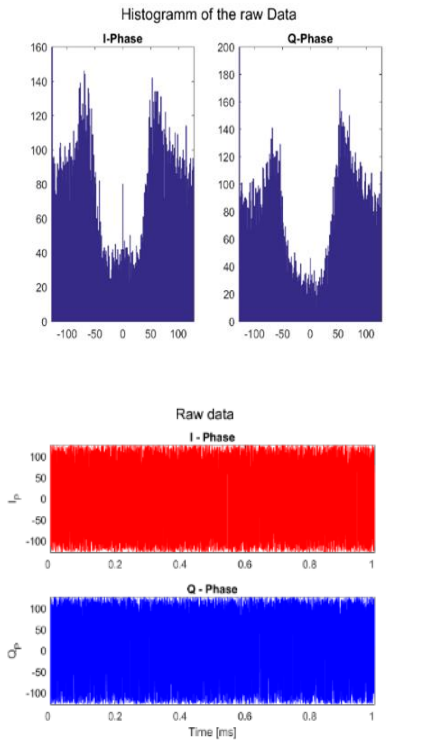
- Results show that the applied mitigation (ANF) can sometimes worsen the results
- This is due to the jamming power and digitized signals being used
- Detailed analysis performed to showcase the limitations:
  - Too low jamming power
  - Too high jamming power

Post-ADC ANF can only work in a certain range, depending on dynamic range in quantization

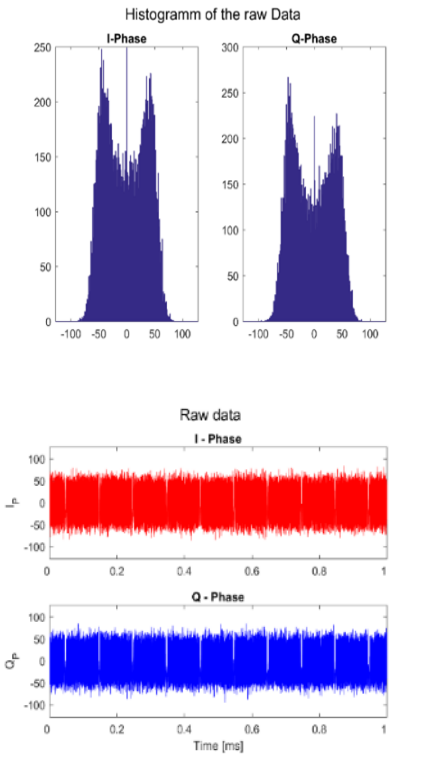
Scenario 1: Low-Power Jammer



Scenario 2: High-power Jammer

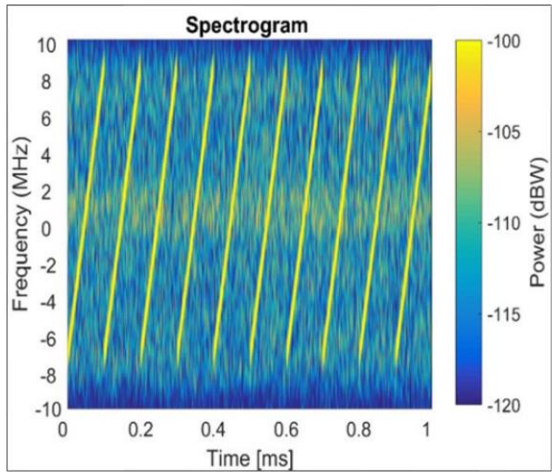
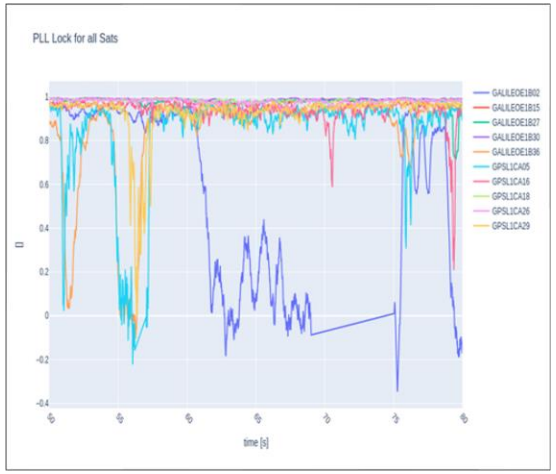
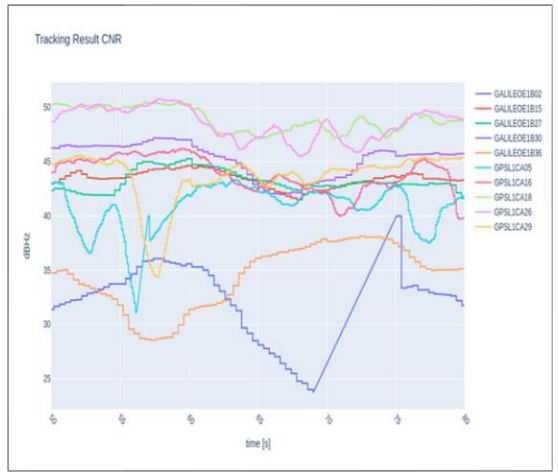
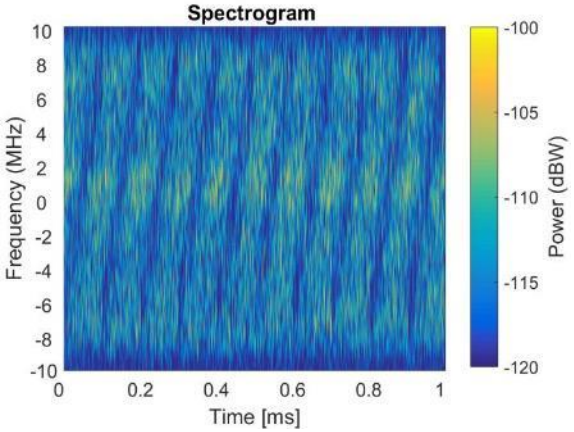
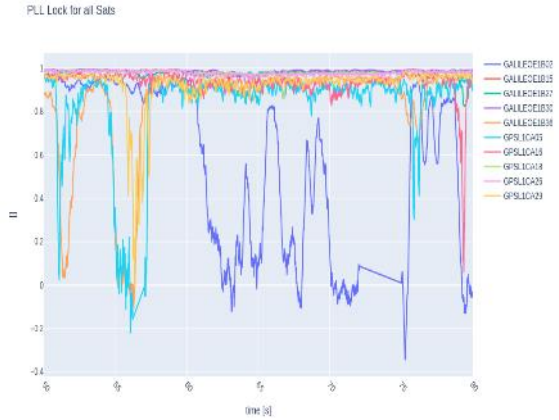
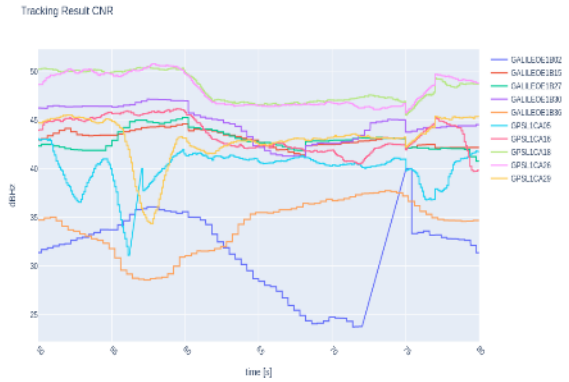


Scenario 3: Middle-power Jammer



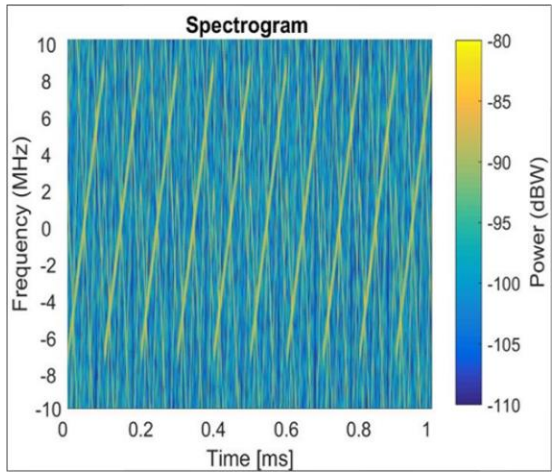
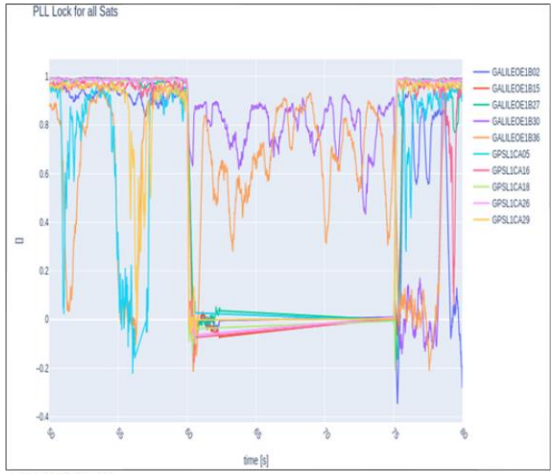
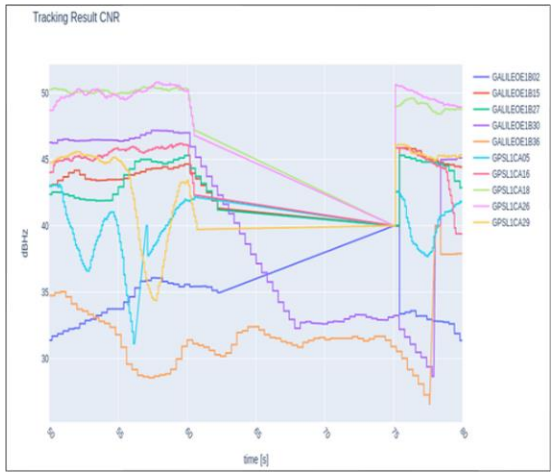
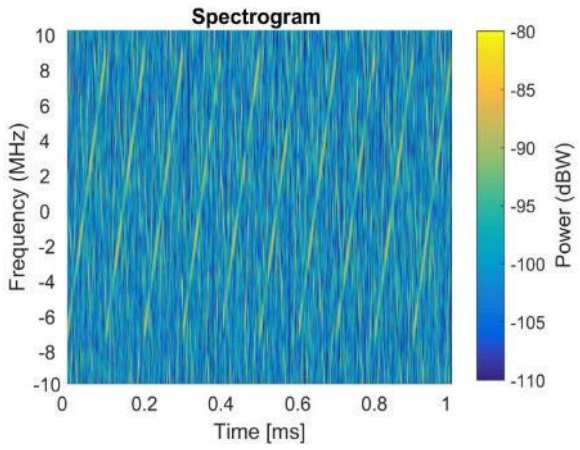
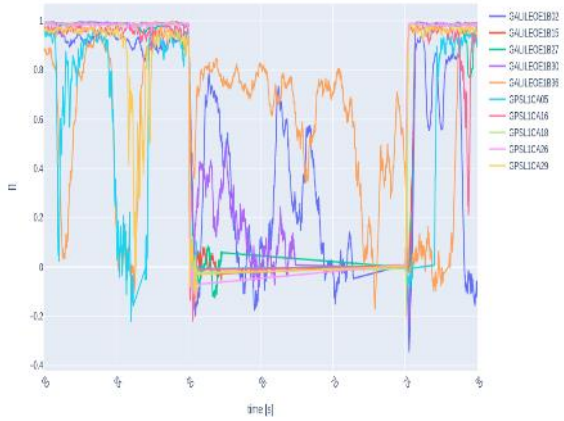
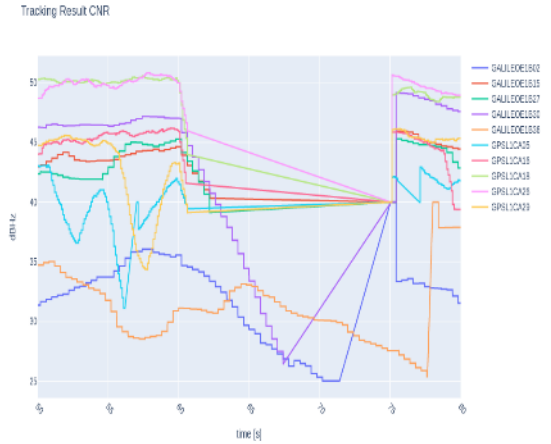
ANF VS. JAMMING POWER

SCENARIO 1: LOW POWER JAMMER

	Spectrogram	PLL	CNR
During Jamming Attack			
After Mitigation			

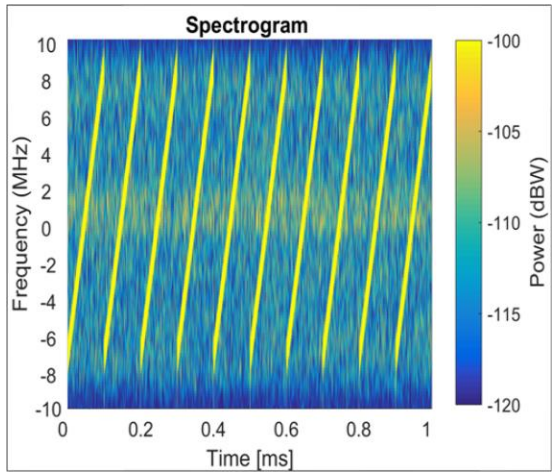
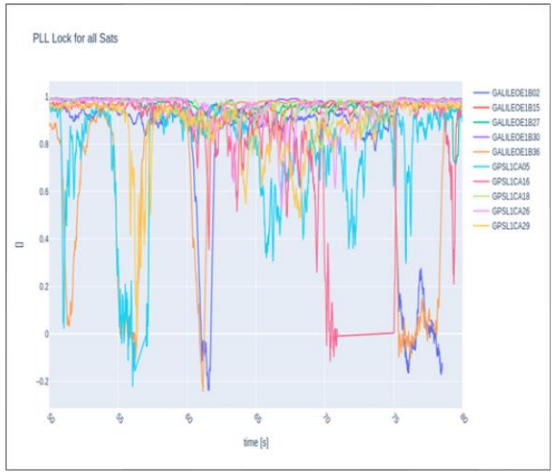
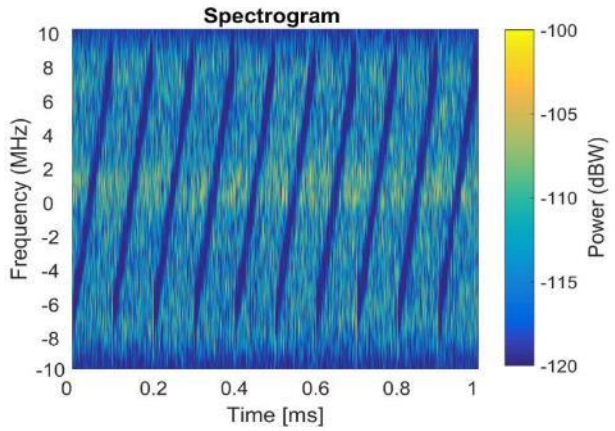
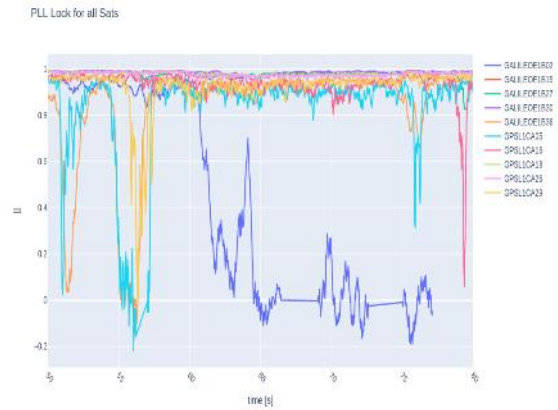
ANF VS. JAMMING POWER

SCENARIO 2: HIGH POWER JAMMER

	Spectrogram	PLL	CNR
During Jamming Attack			
After Mitigation			

ANF VS. JAMMING POWER

SCENARIO 3: MIDDLE POWER JAMMER

	Spectrogram	PLL	CNR
During Jamming Attack			
After Mitigation			

5

CONCLUSIONS & WAY FORWARD

LESSONS LEARNED

CAVEATS AND FUTURE IMPROVEMENTS

ML AND DATASETS

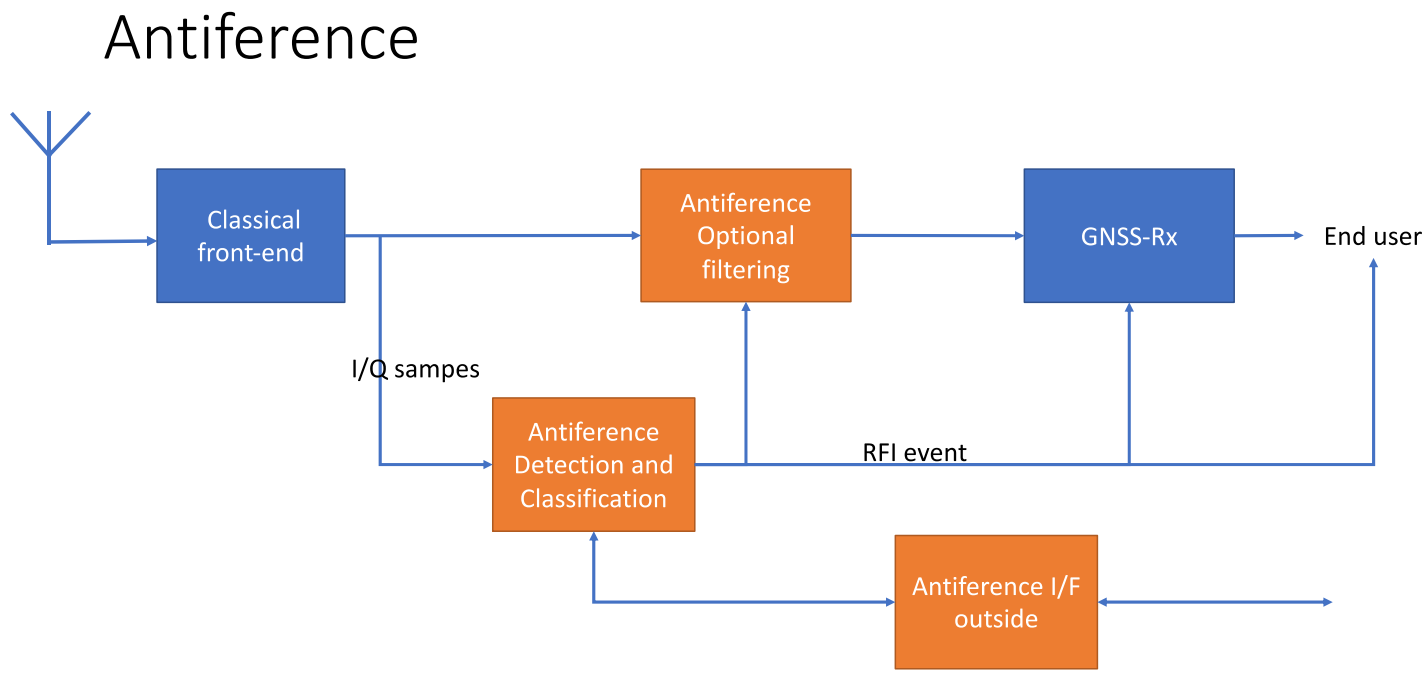
- The FP matching function should be better capable of handling the (especially noisy) non-jammed / clean samples. Now the database grows too large of a size, and during operations too many false alarms are being generated.
- For the signal mitigation, the presence of misclassification could be better integrated in the filtering approach.
- For inclusion of mitigation methods into the ML-model, the following criteria needs to be met:
  - Availability of a much larger amount of data or a reliable method to augment the existing ones
  - Real-time analog mitigation and filtering of the signals to avoid clipping

PERFORMANCE ANALYSIS

- Detection is highly sensitive and picks up low-level RFI quite well. But: performance could be further improved when detection would be desensitised
- Trade-off between chunk size and decision windows can be optimized
- It has proven hard to use user-level KPIs in optimising Antiference algorithms
  - Generally hard to link PVT to range-level errors
  - ML (big-data) optimization based on range-level errors hard: workable proxies to impact of RFI on tracking are needed

FUTURE SERVICE ARCHITECTURE

- The ANTIFERENCE use-case is the front-end “RFI add-on”
- Besides, ANTIFERENCE (detection and classification) can be used for RFI monitoring / detection systems



FUTURE SERVICE ARCHITECTURE

CENTRALIZED VS. DECENTRALIZED

- Interface between ANTIFERENCE and outside world:
  - Update of the knowledge (FP database or the NN model) to be exploited by the system
  - Transferring information about jamming and spoofing events, possibly augmented with time and position information

Centralized Approach

- The main detection modules (NN model and/or FP database) are located on Cloud
- Data from all instances are collected in a central area
- Updates are distributed to the instances
- Especially beneficial for applications such as automotive domain,
  with good access to internet and reliant on latest updates

Decentralized Approach

- The main detection modules (NN model and/or FP database) are located in each ANTIFERENCE device/instance
- Updates are provides in a decentralised approach (and with time delay)
- Beneficial for applications and use-cases with limited access to network

CONCLUSIONS

ML EXPERIMENTS

- Results are very promising, in lab environment
- Jamming classification needs more investigation in features used, but already shows good performance when in operational range of current features
- Spoofing detection performs very well on simulated data. More experiments needed on real data.

MAIN ACHIEVEMENTS

- Investigation of feasibility of ML-based models in detection, classification and mitigation of major sources of intentional interference to GNSS
- Implementation of a concept demonstrator, showing the high potential of the application of ML methods to RFI detection and classification
- Demonstration of feasibility of a fingerprinting database based on signal fingerprints and benefit of documenting the history of RFI
- Conception of a decentralized future service model to expand the concept demonstrator to a cloud-based approach

NEXT STEPS

- Further development of the concept demonstrator to enable demonstration of the capabilities within an integrated receiver concept using standard FPGA/CPU/GPU-based system
- Further evaluation of potentially interesting market segments along with specific requirements for adoption of the concept

Thank you!

OHB Digital Solutions GmbH

S&T

IntegriCom