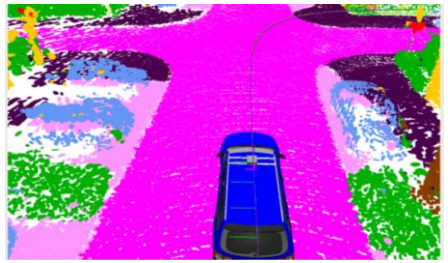
Secure PNT with Sensor Fusion and Machine Learning

Final Presentation (FP)



31.08.2023

Dr. Robert Bensch, Dr. Patrick Henkel, ANavS GmbH
Dr. Jan Wendel, Airbus Defence and Space GmbH

Enabling Technologies for Secure Position-Navigation-Time User Segments (ESA-TRP-TECESN-SOW-015054)

AIRBUS

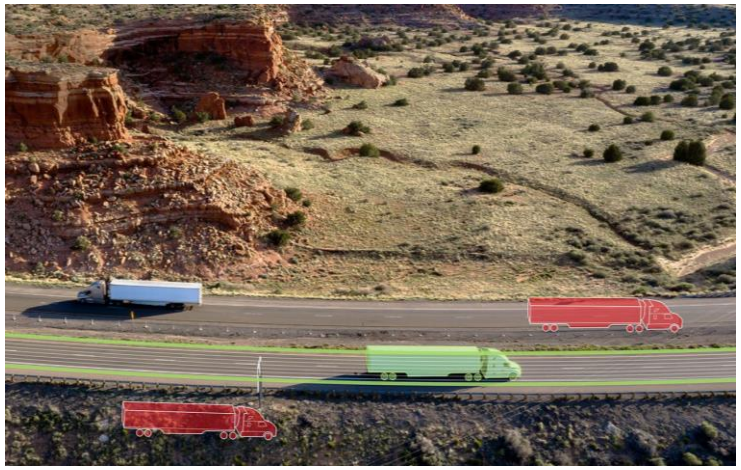
ANAVS
Advanced Navigation Solutions

Outline

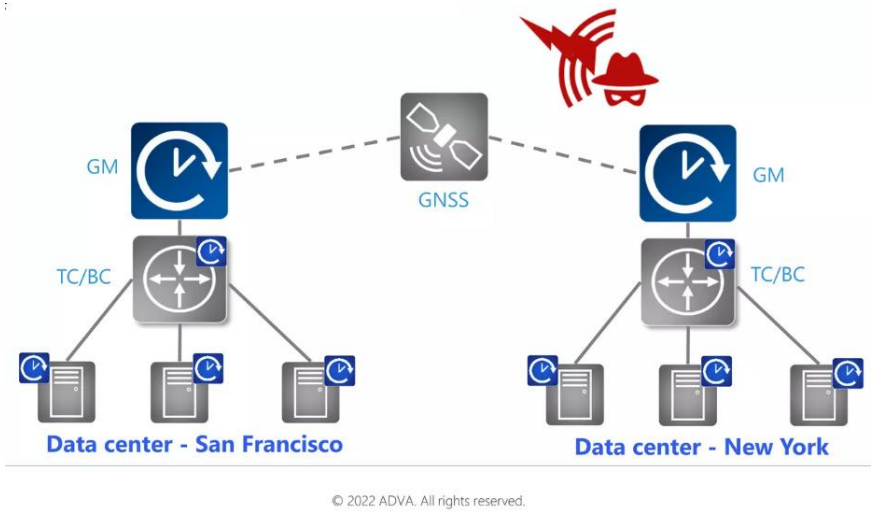
- **Motivation**
- Innovative Anti-Spoofing Testbed with Sensor Fusion and Machine Learning
  - Design
  - Results
  - Software and Hardware
- Summary
- Next Steps

Motivation – GNSS Attacks

Maritime coordinated attack.
Image source [1]



Transport/logistics coordinated attack.
Image source [2]

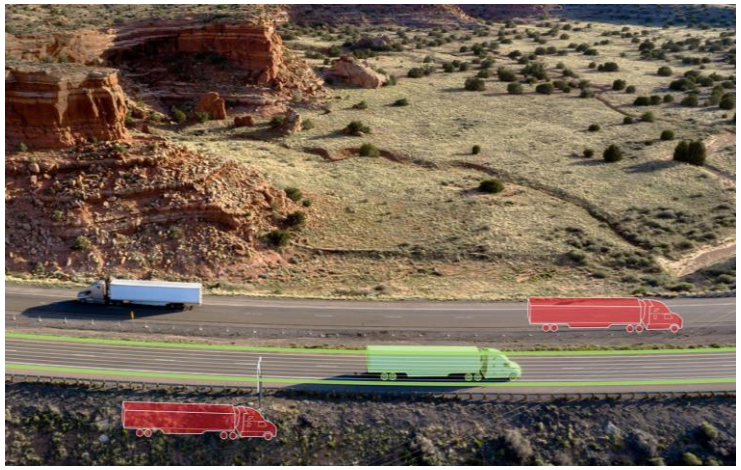


Communication/energy networks timing attack.
Image source [3]

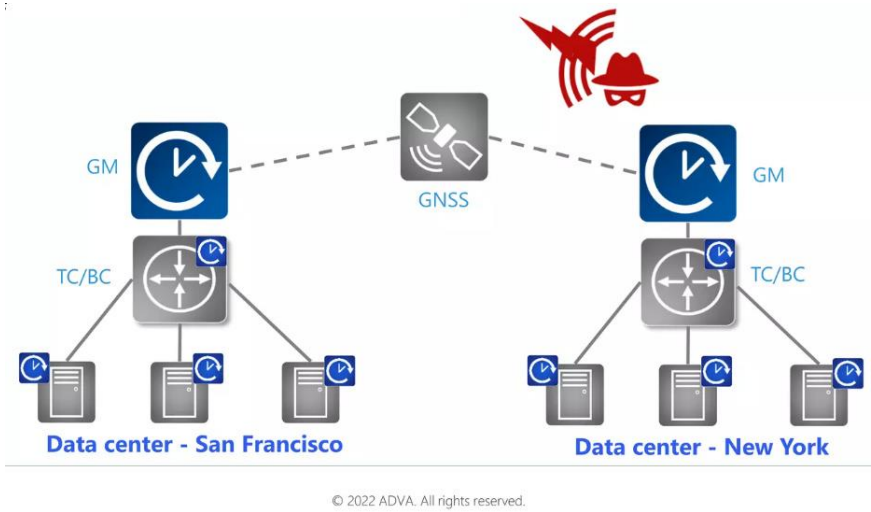
[1] Jamming and Spoofing of Global Navigation Satellite Systems (GNSS), Intertanko, 2019, p. 5, fig. 2
[2] GNSS Spoofing Detection, Identifying GNSS Spoofing, Hexagon, Novatel, 2023
[3] Introducing GNSS/GPS backup as a service (GBaaS), ADVA, 2022, slide 2

Motivation – GNSS Attacks

Maritime coordinated attack.
Image source [1]



Transport/logistics coordinated attack.
Image source [2]



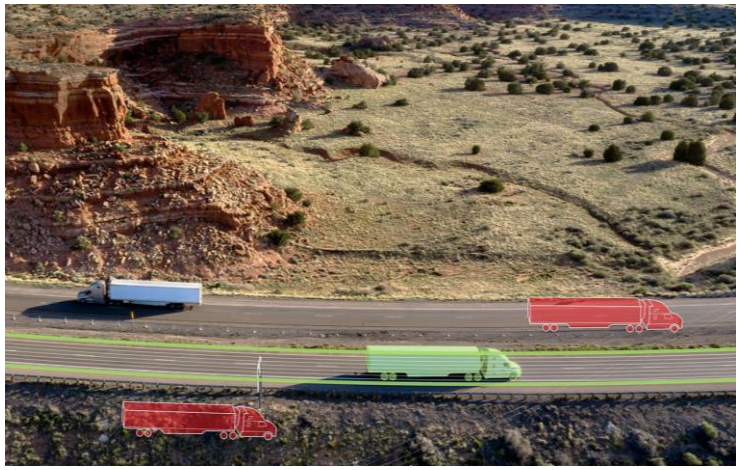
Communication/energy networks timing attack.
Image source [3]

Attacks on GNSS positioning information

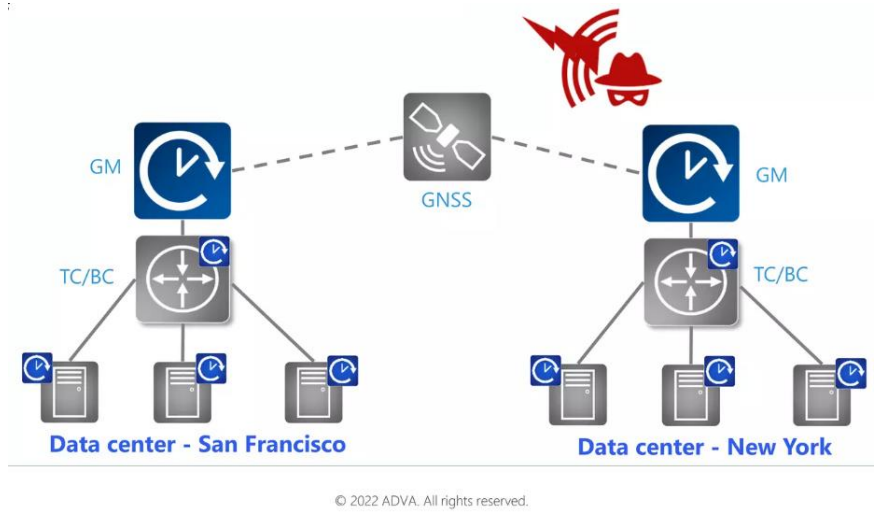
[1] Jamming and Spoofing of Global Navigation Satellite Systems (GNSS), Intertanko, 2019, p. 5, fig. 2
[2] GNSS Spoofing Detection, Identifying GNSS Spoofing, Hexagon, Novatel, 2023
[3] Introducing GNSS/GPS backup as a service (GBaaS), ADVA, 2022, slide 2

Motivation – GNSS Attacks

Maritime coordinated attack.
Image source [1]



Transport/logistics coordinated attack.
Image source [2]



Communication/energy networks timing attack.
Image source [3]

Attacks on GNSS timing information

[1] Jamming and Spoofing of Global Navigation Satellite Systems (GNSS), Intertanko, 2019, p. 5, fig. 2
[2] GNSS Spoofing Detection, Identifying GNSS Spoofing, Hexagon, Novatel, 2023
[3] Introducing GNSS/GPS backup as a service (GBaaS), ADVA, 2022, slide 2

ENABLING TECHNOLOGIES FOR SECURE POSITION-NAVIGATION-TIME USER SEGMENTS

Contractor(s): ANavS (DE), Airbus Defence & Space (DE)			ESA Budget:	600k€
TRP T606-606ES	Contract 4000129660	YoC: 2023	TO: Gianluca Caparra (TEC-ESN)	
TRL	Initial: 2	Achieved: 4	Target TRL: 3 Date: Q4 2022	

Background and justification:

Over the past years the thread of intentional GNSS jamming and spoofing, aiming at falsifying the computed Position, Velocity and Time (PVT), has significantly increased since nowadays virtually anyone is able to perform GNSS attacks with low budget and open source code. Since today many sectors, including critical infrastructure, rely on Global Navigation Satellite Systems (GNSS) the necessity and relevance is given for the development of anti-spoofing techniques that allow to protect against GNSS attacks. This activity aims at developing a flexible testbed architecture and a machine learning (ML) based fusion approach for the detection and mitigation of spoofing attacks at the receiver level that can cope with different sensor configurations.

Objectives:

- Consolidation of the state-of-the-art and emerging technologies that can be used for PVT assurance
- Design and implementation of innovative spoofing detection and mitigation technique based on sensor fusion
- Design and implementation of a flexible testbed capable of emulating/integrating multiple selected technologies, including machine learning for spoofing detection and mitigation
- Performance assessment and benchmark of different solutions

Achievements and status:

- Definition of the system requirements (Scenarios, target techniques and sensors; testbed requirements, test plan; anti-spoofing sensors API; SRR achieved)
- Design of the anti-spoofing testbed and sensor fusion (CDR achieved)
- Anti-spoofing testbed implementation and validation successful (data collection; training of ML techniques; testbed user manual, validation report; TRR achieved)
- Testbed execution successful (all tests of the test plan performed; performance report; promising spoofing detection and mitigation performance; QR achieved)

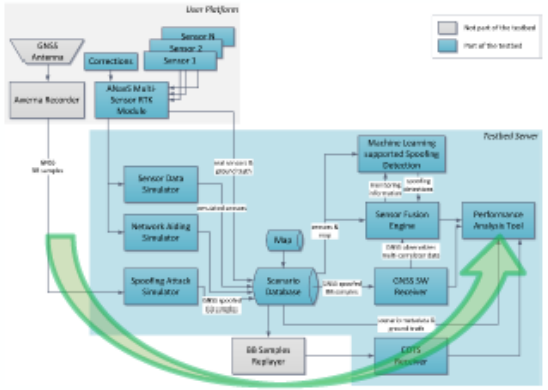
Benefits:

- Flexible testbed architecture and implementation for the evaluation of multi-sensor anti-spoofing sensor fusion techniques including sensor data and spoofing attack simulation
- Machine learning based anti-spoofing techniques proposed and evaluated that show promising detection and mitigation performance

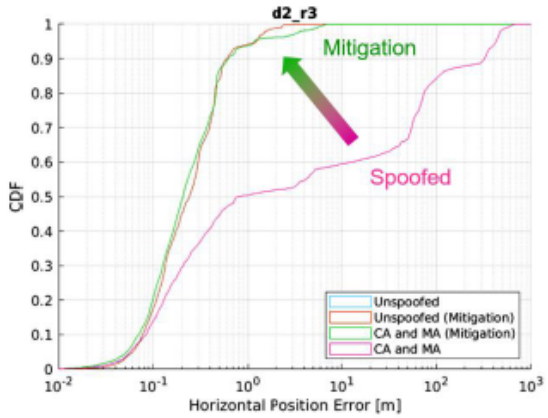
Next steps:

- Secure, robust and accurate positioning enabled by camera-, LiDAR- and/or RADAR-based localization on custom and publicly available maps.
- General purpose flexible machine learning techniques for multi-sensor data anomaly detection.
- Technical Note: „Guidelines for Sensor fusion-based GNSS Anti-Spoofing and Potential System Evolution“ discusses potential system future evolution

Advanced Navigation Solutions



Testbed architecture

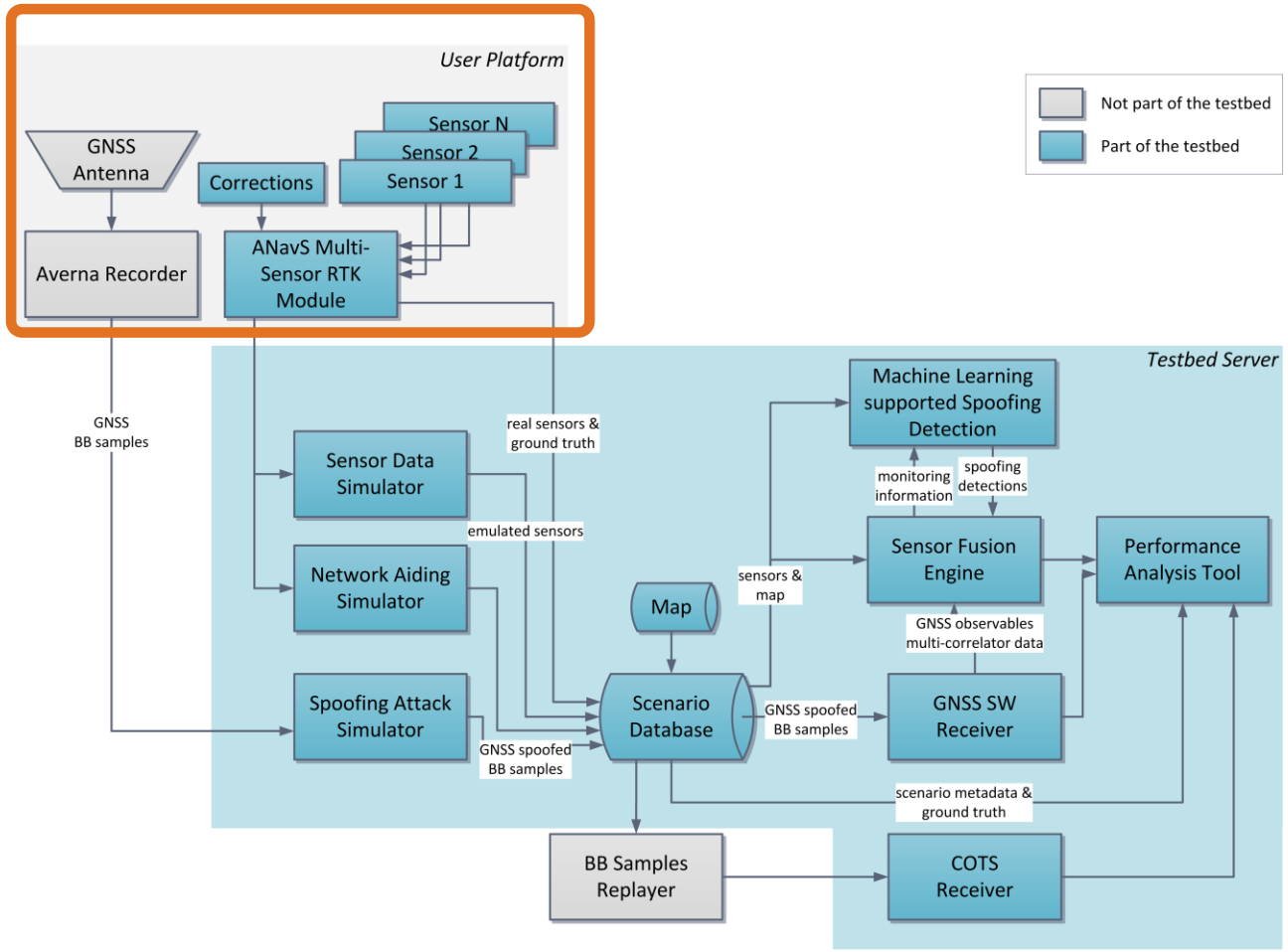


Spoofing mitigation performance

Outline

- Motivation
- **Innovative Anti-Spoofing Testbed with Sensor Fusion and Machine Learning**
  - **Design**
  - Results
  - Software and Hardware
- Summary
- Next Steps

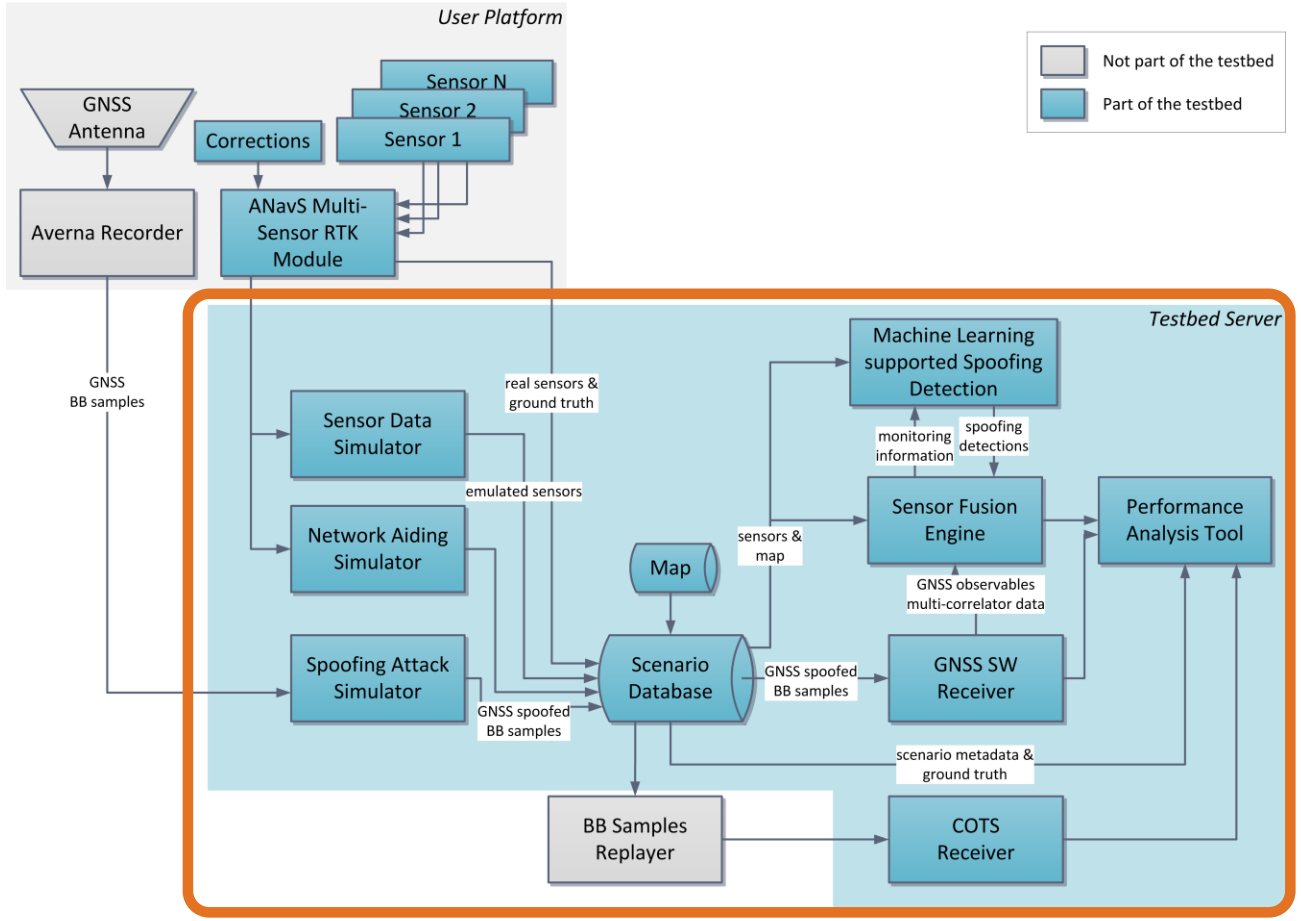
Design: Anti-Spoofing Testbed



High-level testbed architecture

- User Platform

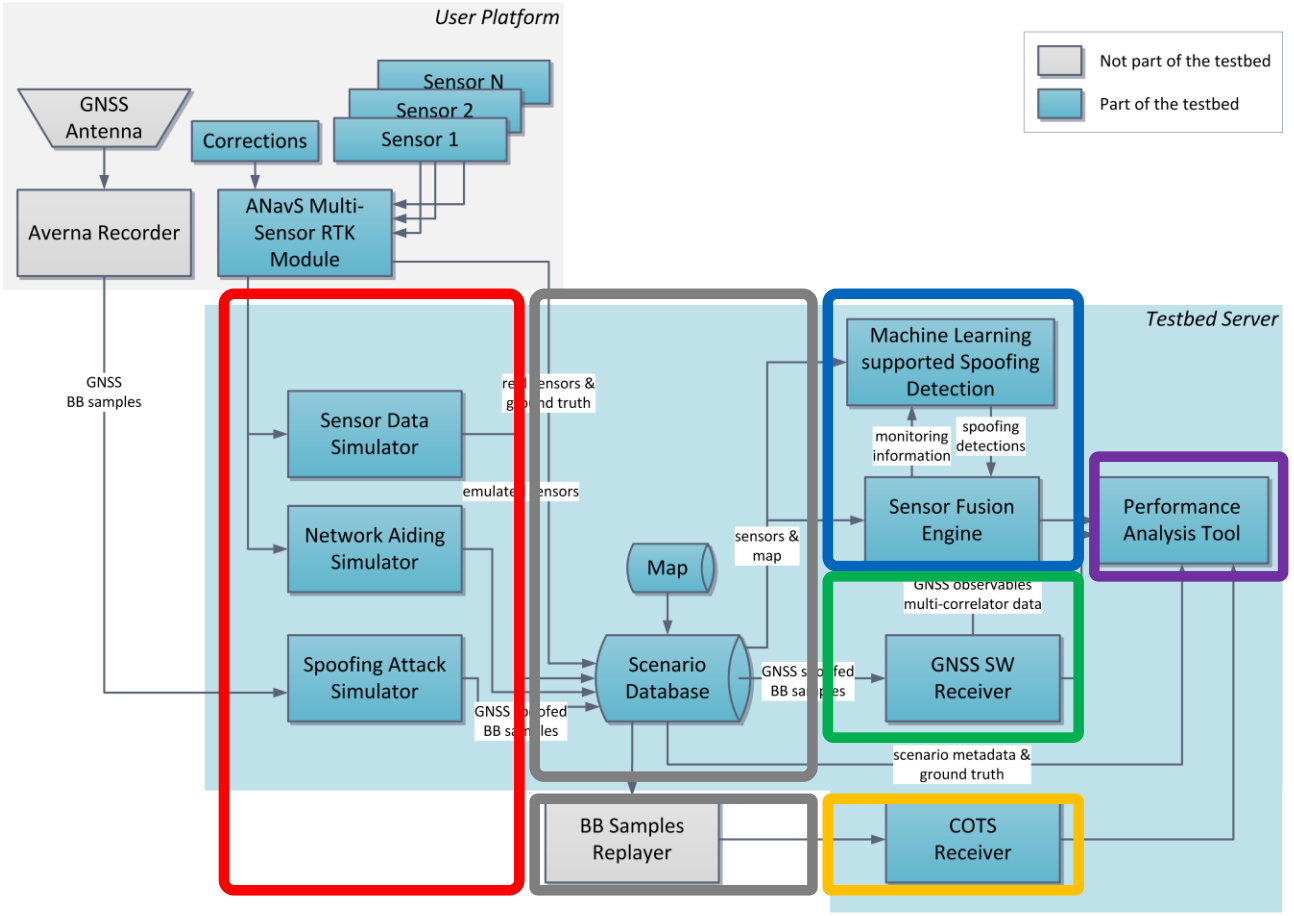
Design: Anti-Spoofing Testbed



High-level testbed architecture

- User Platform
- Testbed Server

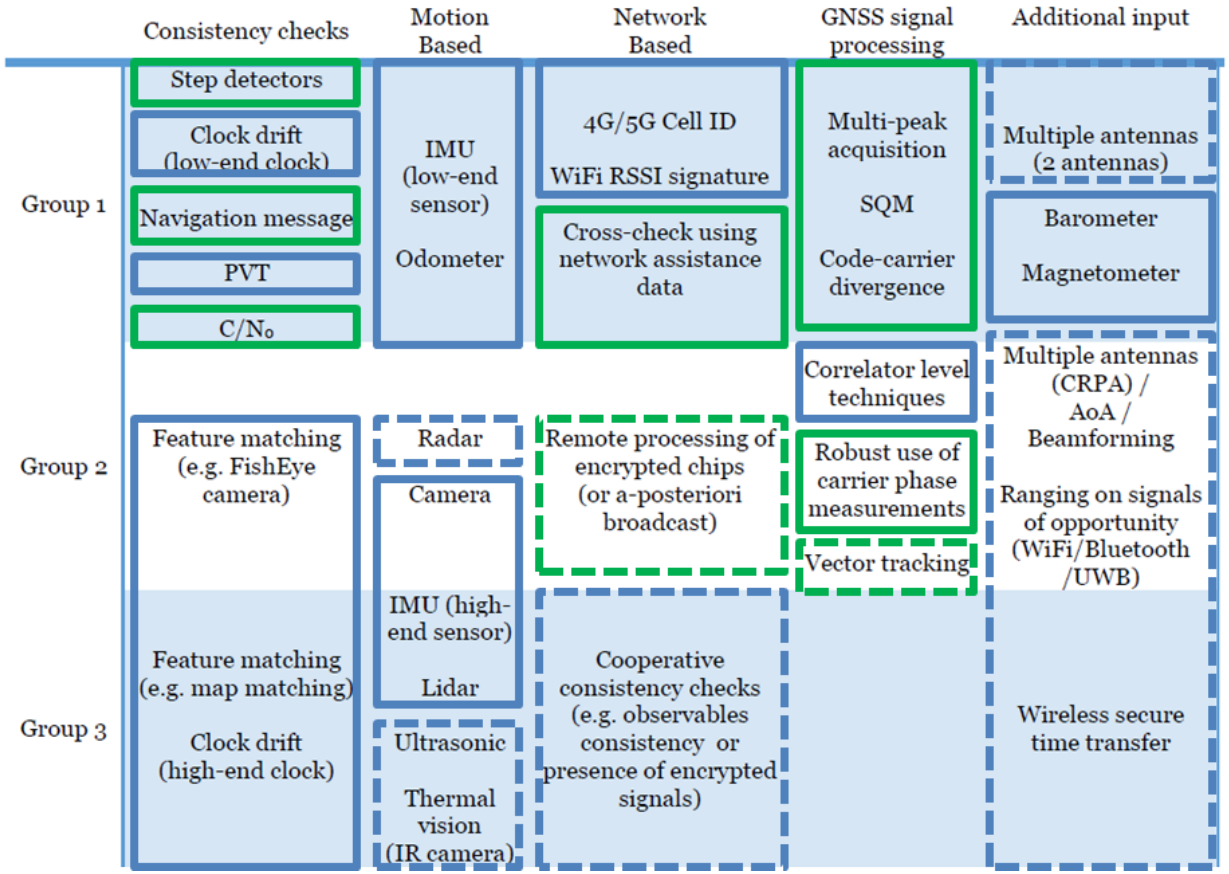
Design: Anti-Spoofing Testbed



High-level testbed architecture

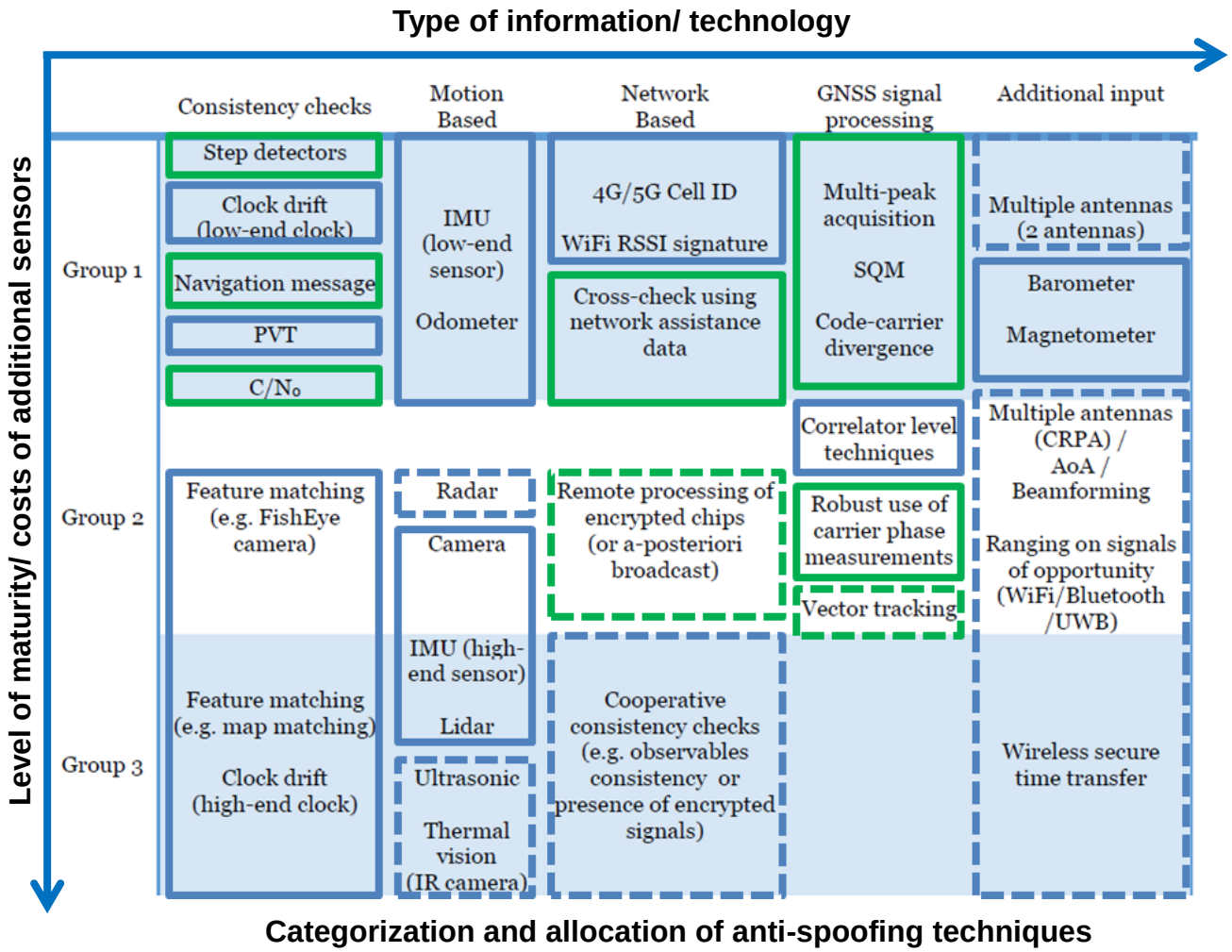
- User Platform
- Testbed Server
  - Sensor data and spoofing attack simulator
  - Scenario database, and BB samples replayer
  - Anti-spoofing sensor fusion based on machine learning
  - GNSS software receiver
  - Commercial-Off-The-Shelf (COTS) receiver
  - Performance analysis tool

Design: Anti-Spoofing Testbed



Categorization and allocation of anti-spoofing techniques

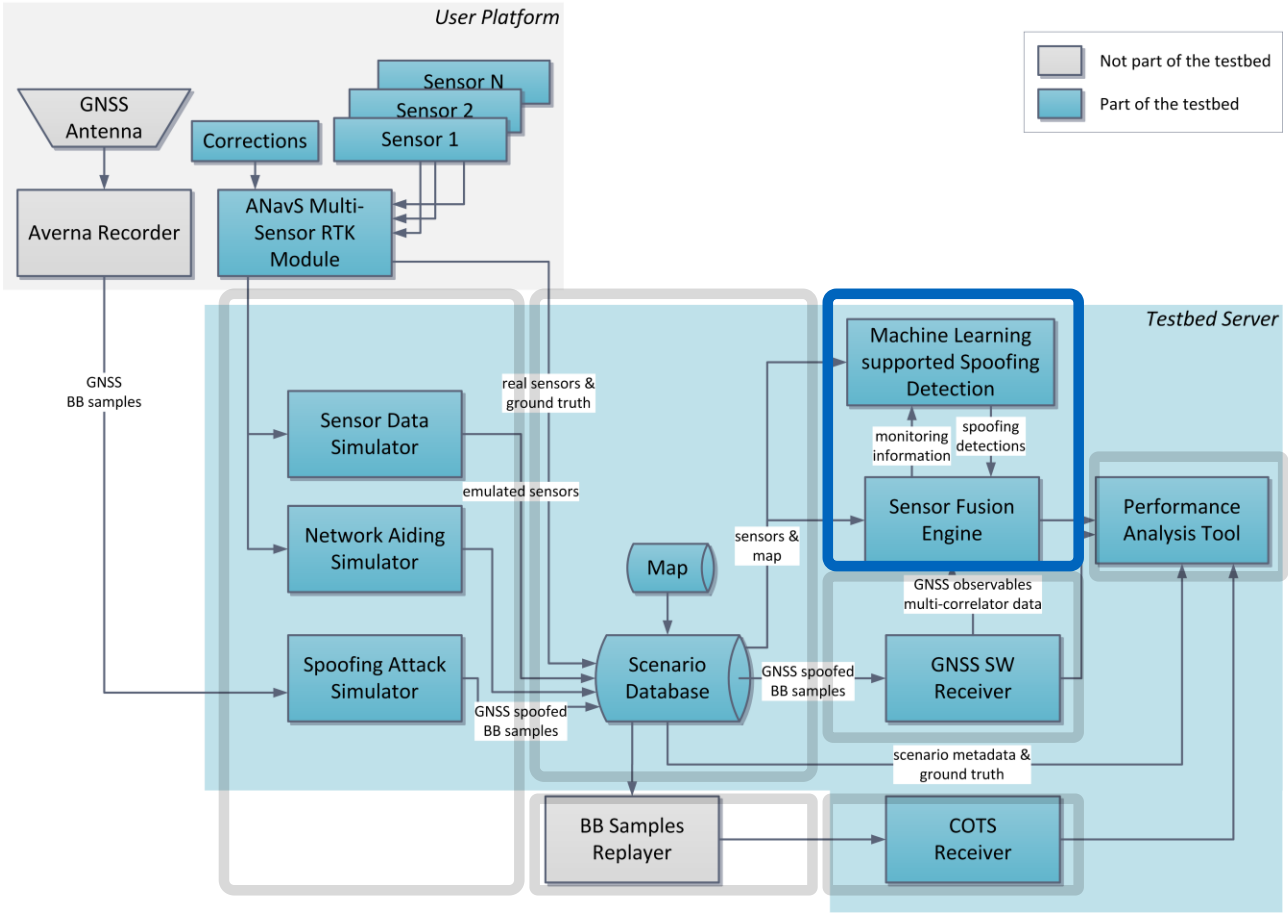
Design: Anti-Spoofing Testbed



GNSS SW Receiver

Anti-Spoofing Sensor Fusion based on Machine Leanring

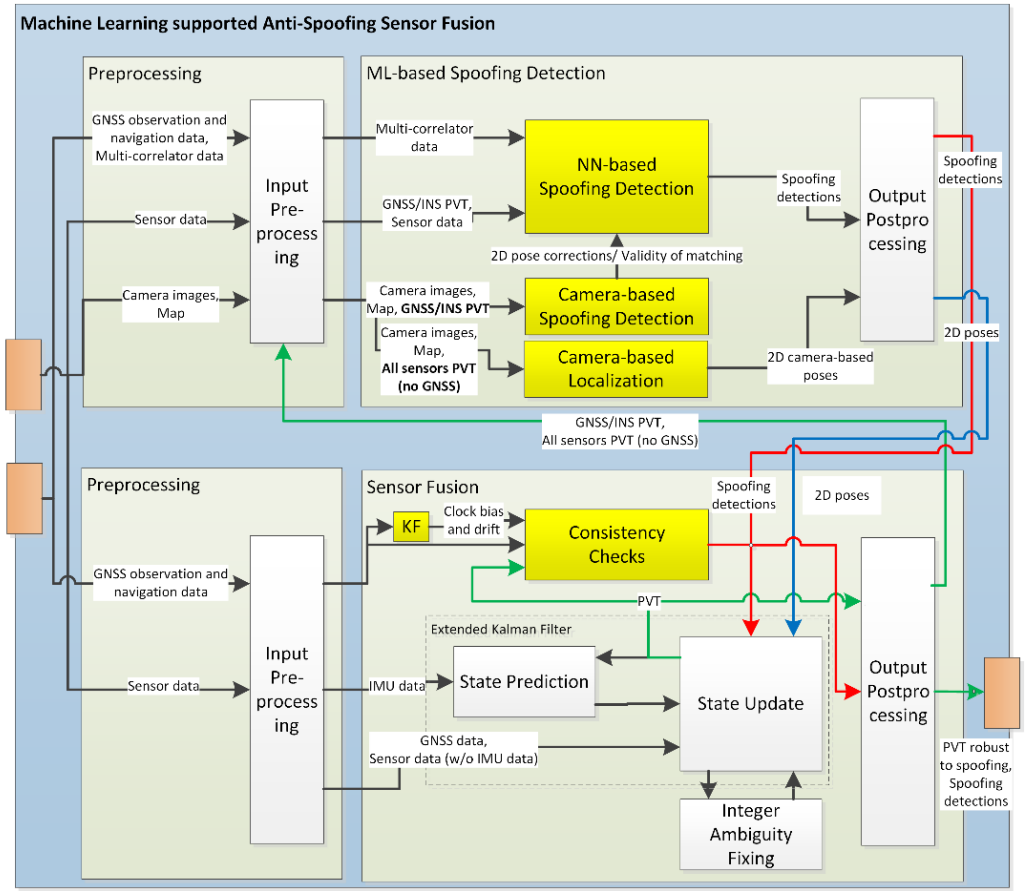
Design: Anti-Spoofing Testbed



High-level testbed architecture

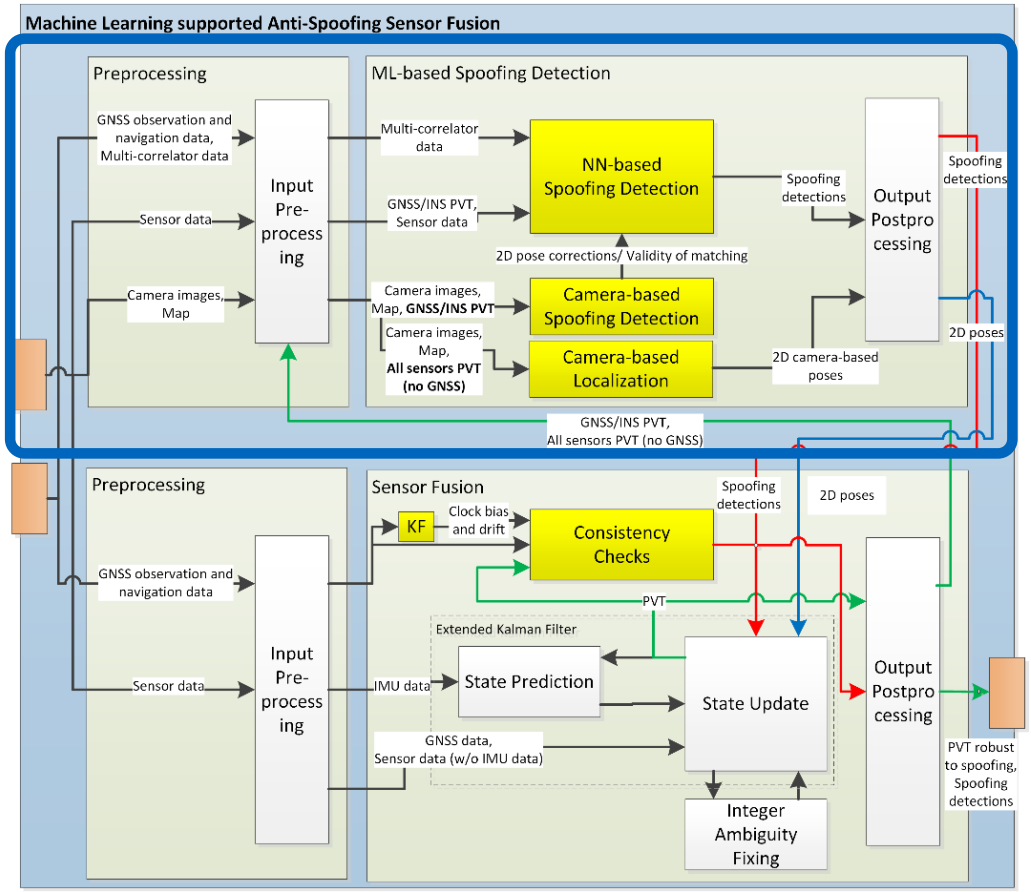
- User Platform
- Testbed Server
  - Sensor data and spoofing attack simulator
  - Scenario database, and BB samples replayer
  - **Anti-spoofing sensor fusion based on machine learning**
  - GNSS software receiver
  - Commercial-Off-The-Shelf (COTS) receiver
  - Performance analysis tool

Design: Anti-Spoofing Sensor Fusion and Machine Learning



Machine learning supported anti-spoofing sensor fusion

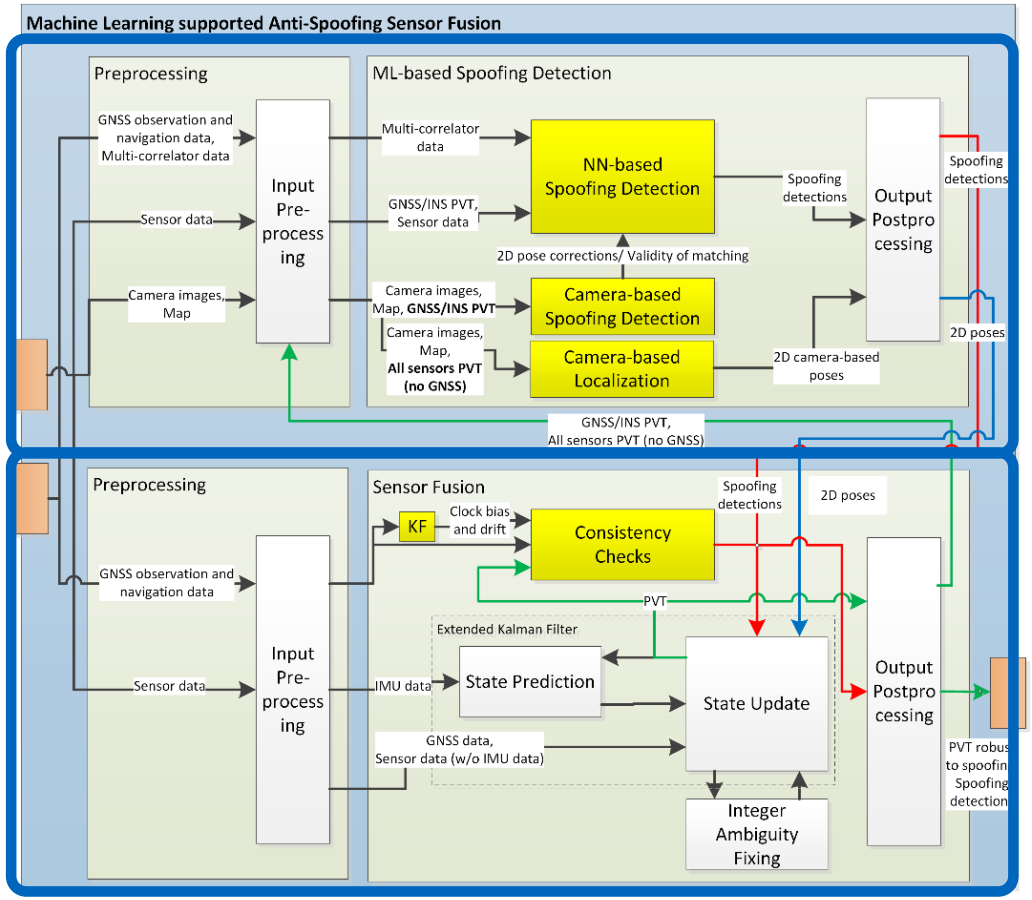
Design: Anti-Spoofing Sensor Fusion and Machine Learning



Machine learning supported anti-spoofing sensor fusion

- Machine Learning based Spoofing Detection

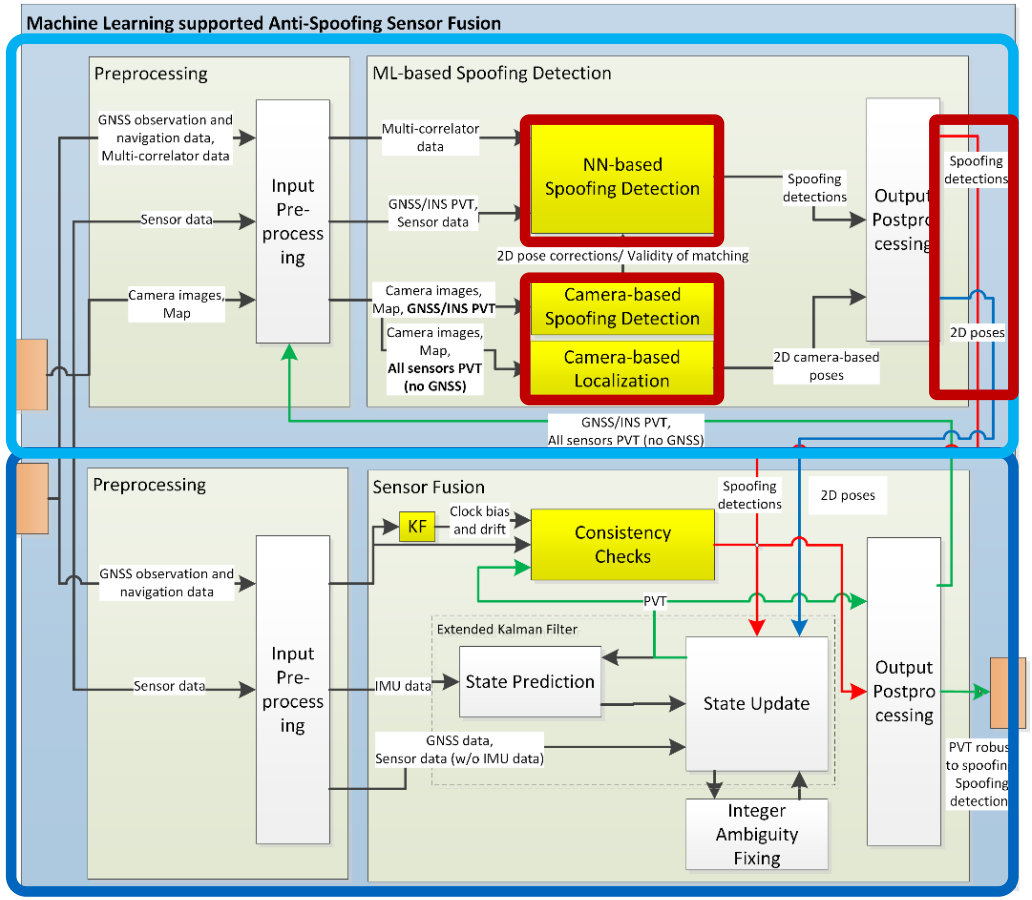
Design: Anti-Spoofing Sensor Fusion and Machine Learning



Machine learning supported anti-spoofing sensor fusion

- Machine Learning based Spoofing Detection
- Anti-Spoofing Sensor Fusion

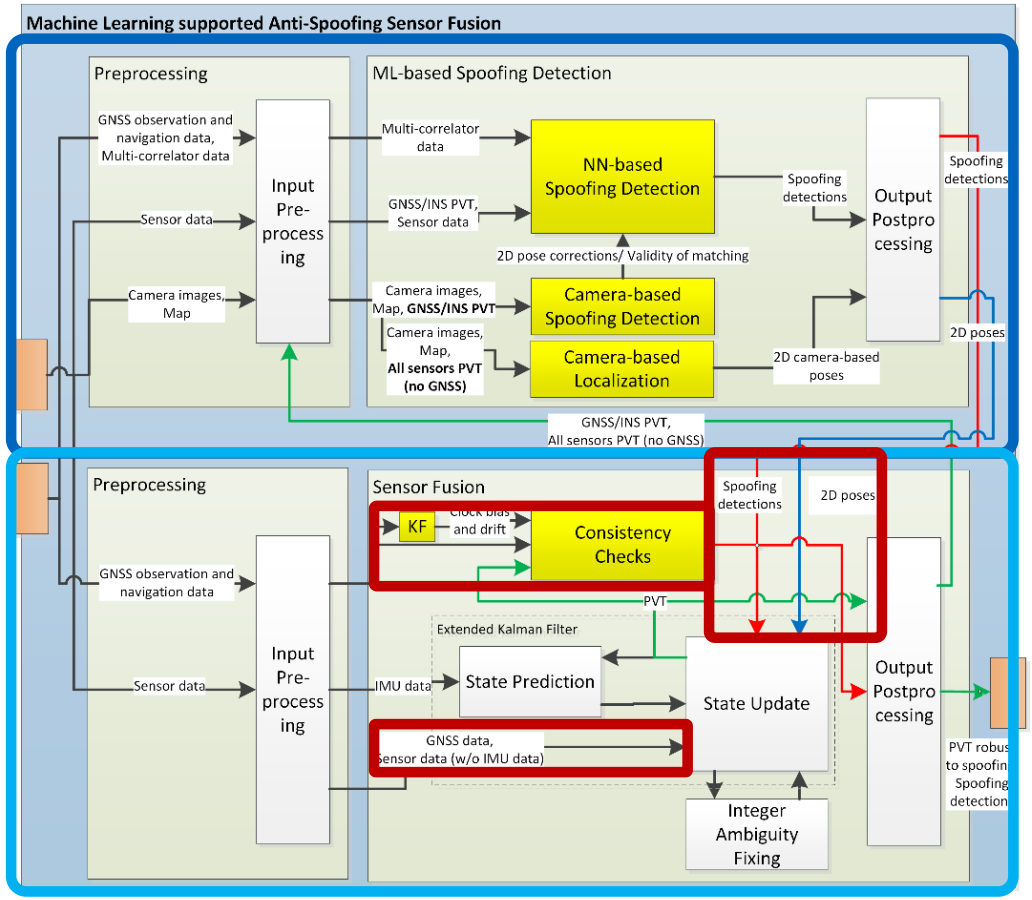
Design: Anti-Spoofing Sensor Fusion and Machine Learning



Machine learning supported anti-spoofing sensor fusion

- Machine Learning based Spoofing Detection
  - **1. NN-based spoofing detection** (Recurrent autoencoder (RAE) and DNN classifier, multi dimensional time-series data)
    - **a)** GNSS multi-correlator data
    - **b)** Cooperative consistency check of compatible sensor and GNSS-derived measurements
  - **2. Camera-based localization** on georeferenced road maps
    - **a)** Spoofing detection (verification of GNSS-based pose)
    - **b)** Spoofing mitigation (provision of camera-based pose)
- Anti-Spoofing Sensor Fusion

Design: Anti-Spoofing Sensor Fusion and Machine Learning



Machine learning supported anti-spoofing sensor fusion

- Machine Learning based Spoofing Detection
- Anti-Spoofing Sensor Fusion
  - **Extended Kalman Filter** based sensor fusion (EKF)
  - **State prediction:** IMU measurements
  - **State update:** GNSS measurements, additional sensors:
    - **Real and Simulated Sensors**
  - GNSS RTK, Integer Ambiguity Fixing
  - **Classical consistency checks module**
  - **Inputs from ML module:**
    - **Spoofing detections and camera-based poses**

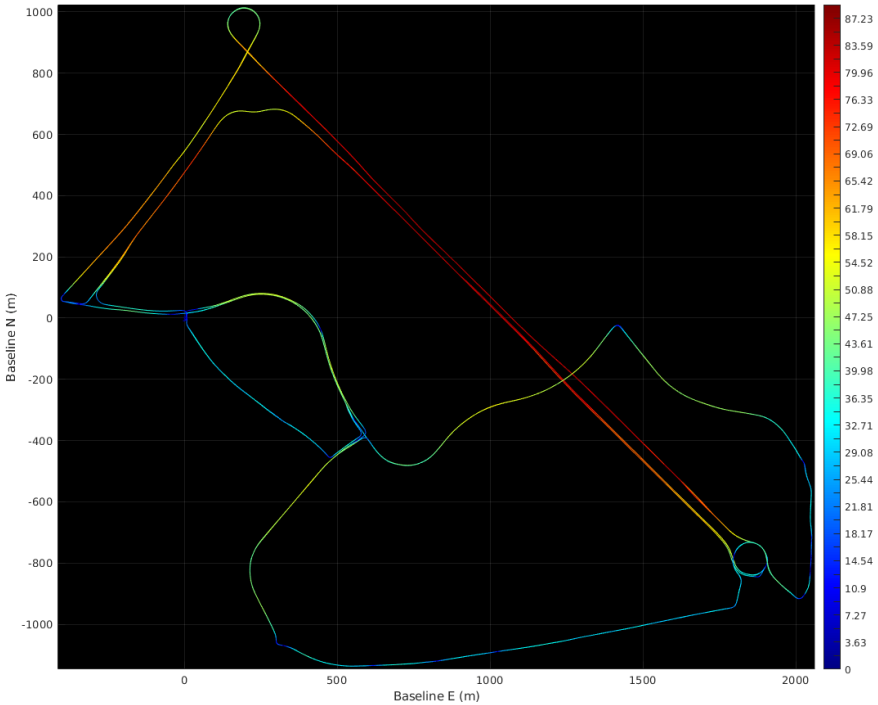
Outline

- Motivation
- **Innovative Anti-Spoofing Testbed with Sensor Fusion and Machine Learning**
  - Design
  - **Results**
  - Software and Hardware
- Summary
- Next Steps

Results: Overview

- **Data Collection and Data Generation**
- Anti-Spoofing Techniques Results

Results: Data Collection and Reference Trajectory



Use Case	Datasets	Duration (min:sec)	Simulated Spoofing Attacks
Static	s1, s2, s3	10:35, 10:46, 09:49	Timing attack (TA)
Low dynamic	d1, d3	10:38, 36:31	Meaconing (MA) and Coordinated attack (CA)
High dynamic	d2	24:50	Meaconing (MA) and Coordinated attack (CA)

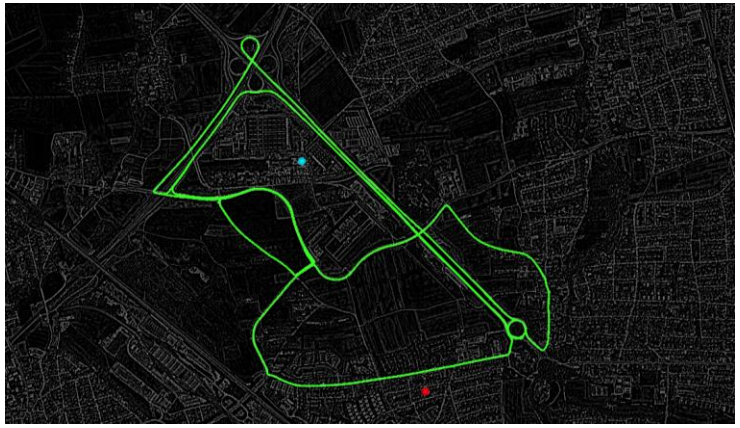
Overview of data collection location, trajectories and simulated attacks.

Reference trajectory computed using ANavS Integrated Sensor Platform (ISP) and ANavS Multi-GNSS RTK Sensor Fusion.

Results: Simulated and Real Sensor Data

Simulated Data	Real Sensor Data
Sensor Data Simulation • Barometer • High-end IMU **Network Aiding Simulation** • Simulated LTE 4G-5G network positioning at ranging level **Spoofing Attack Simulation / Spoofed BB-samples** • Timing Attack • Meaconing Attack • Coordinated Attack	**Real Sensor Data** recorded with the Integrated Sensor Platform (ISP) and the Averna BB-Sample Recorder (Averna RP-6120) • GNSS Baseband Samples (GPS and Galileo, samples rate 12.5 MHz) • Low-cost IMU • Wheel odometry • Camera • LiDAR

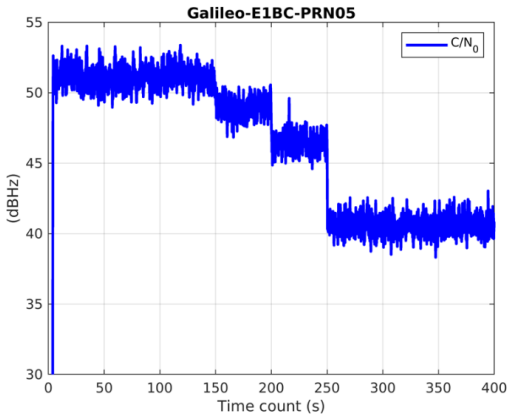
Overview of simulated and recorded real sensor data.



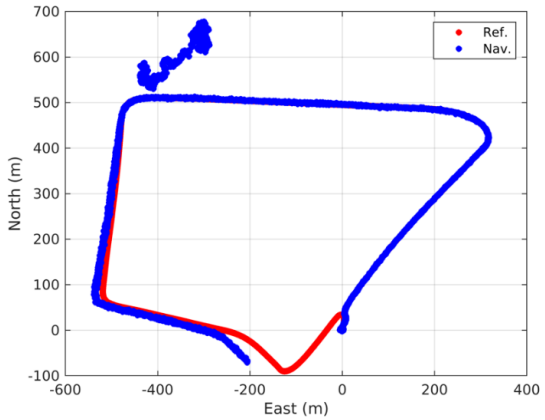
Anchors for network aiding simulation

Camera images

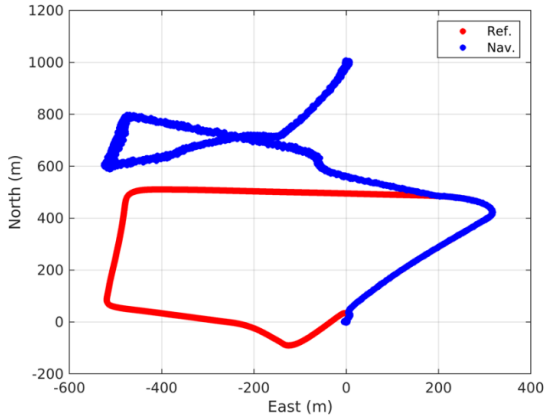
Results: Spoofing Attack Simulation



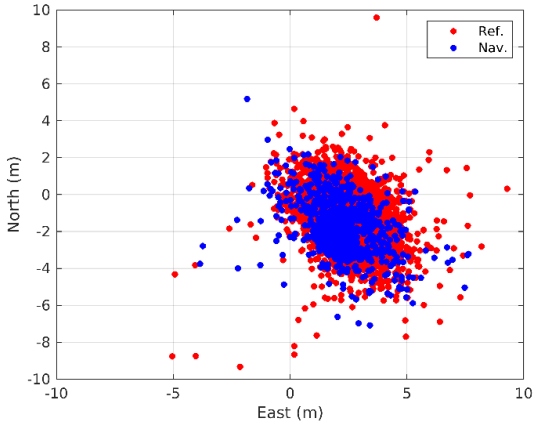
Nulling emulation validation



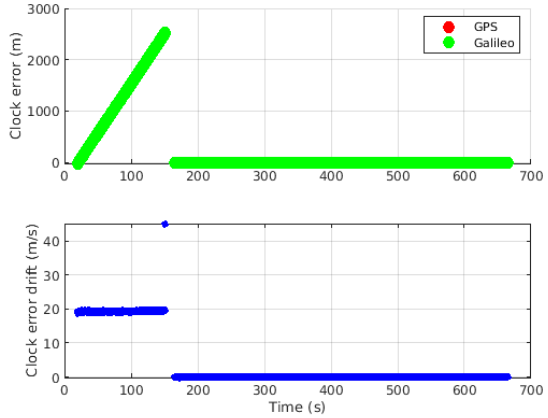
Uncoordinated attack simulation



Coordinated attack simulation



Timing attack simulation position



Timing attack simulation clock error and clock error drift

Results: Overview

- Data Collection and Data Generation
- **Anti-Spoofing Techniques Results**

Results: Overview

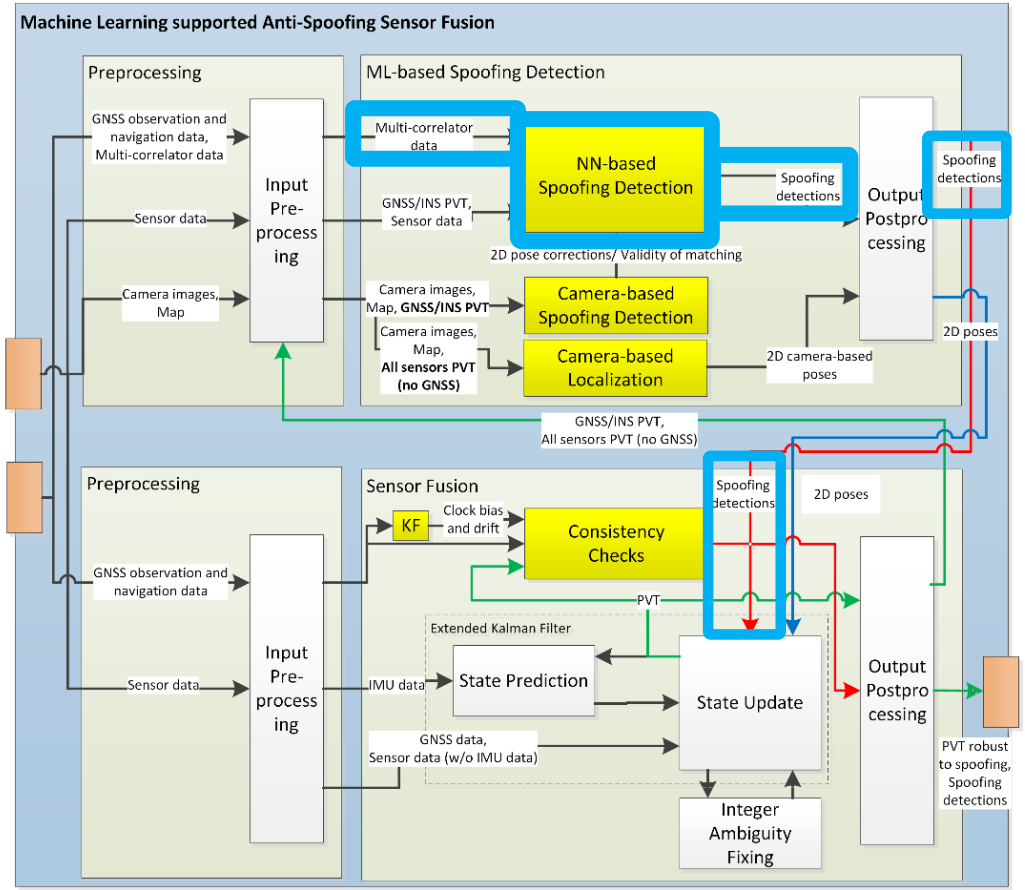
- Data Collection and Data Generation
- **Anti-Spoofing Techniques Results**
  - **Anti-Spoofing Sensor Fusion based on Machine Learning**
    - **Individual techniques results**
    - Overall results
  - GNSS SW Receiver (Airbus SDR) vs. COTS Receiver

Results: NN-based spoofing detection – Multi-correlator data

Advanced Navigation Solutions

Dataset	Total			Accuracy		
	Accuracy	Precision	Recall	CA	MA	TA
Galileo	0.990	0.929	0.976	0.98	0.984	0.99
GPS	0.989	0.844	0.985	0.991	0.994	0.995

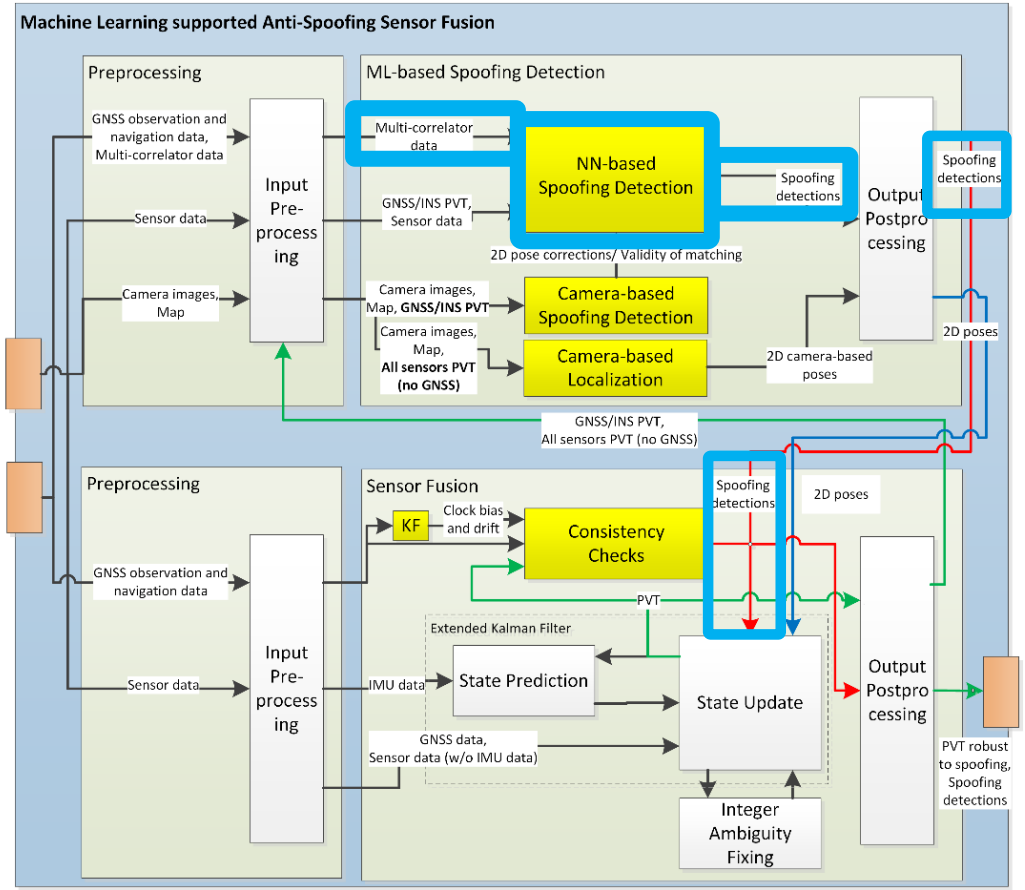
Mutli-correlator data based spoofing detection results for a model trained and tested on Galileo and GPS signals, respectively. Individual and total results for coordinated (CA), meaconing (MA) and timing attacks (TA).



Results: NN-based spoofing detection – Multi-correlator data

Advanced Navigation Solutions

Spoofing detections across time for individual GPS and Galileo signals. Timing attack (dataset: s1_2 TA)

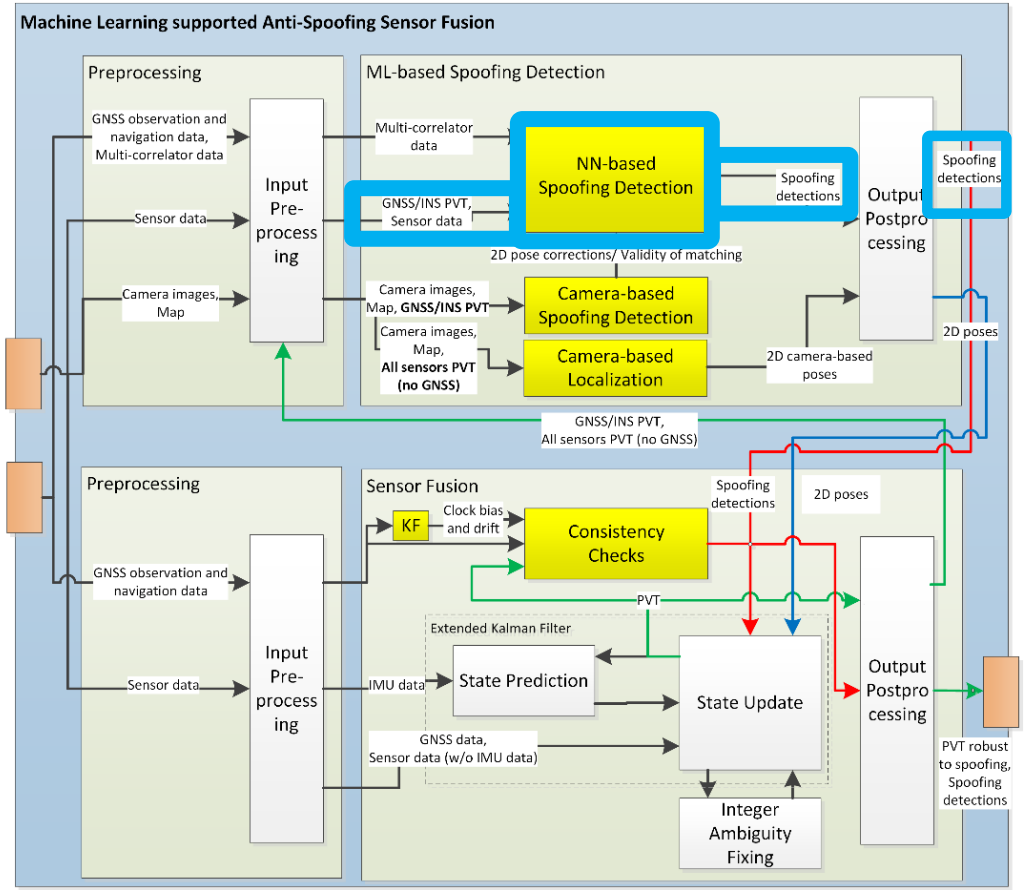


Results: NN-based spoofing detection – Sensor vs. GNSS-derived measurements

Advanced Navigation Solutions

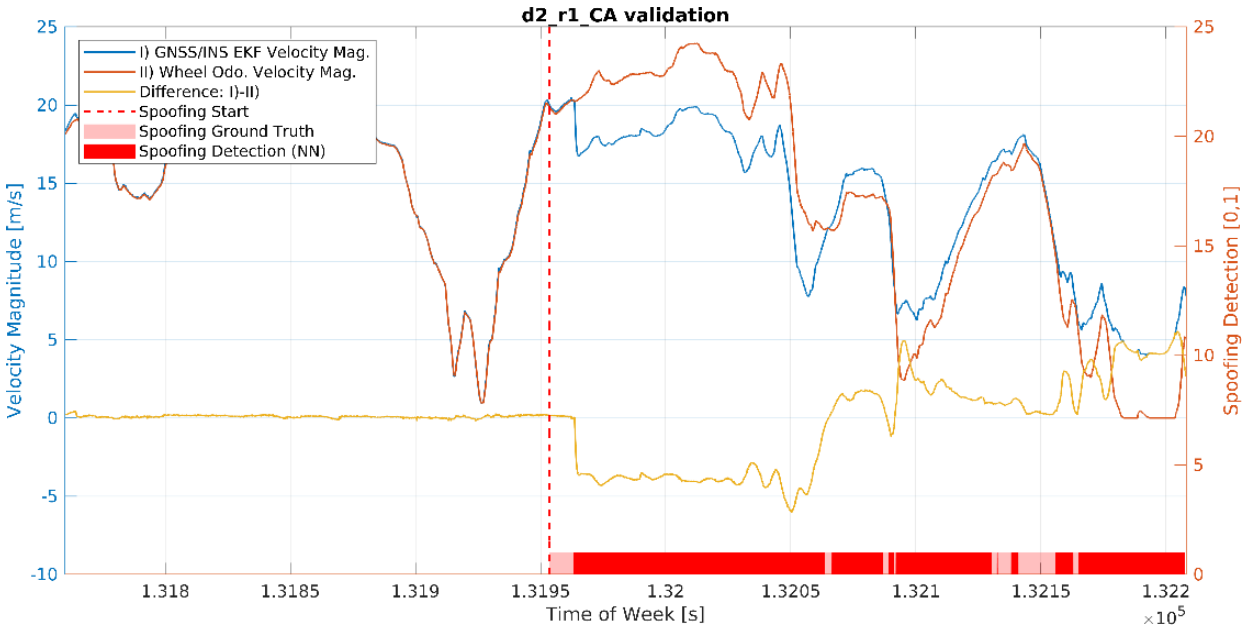
Dataset	Accuracy		
	No Spoofing	CA	MA
d1 (round 2)	0.996	0.902	0.991
d2 (round 1)	0.981	0.912	0.931
d3 (round 2)	0.975	0.796	0.823

Sensor data based spoofing detection results for dynamic scenarios. The detection accurarcy is given for the nominal case and for coordinated (CA) and meaconing attacks (MA).

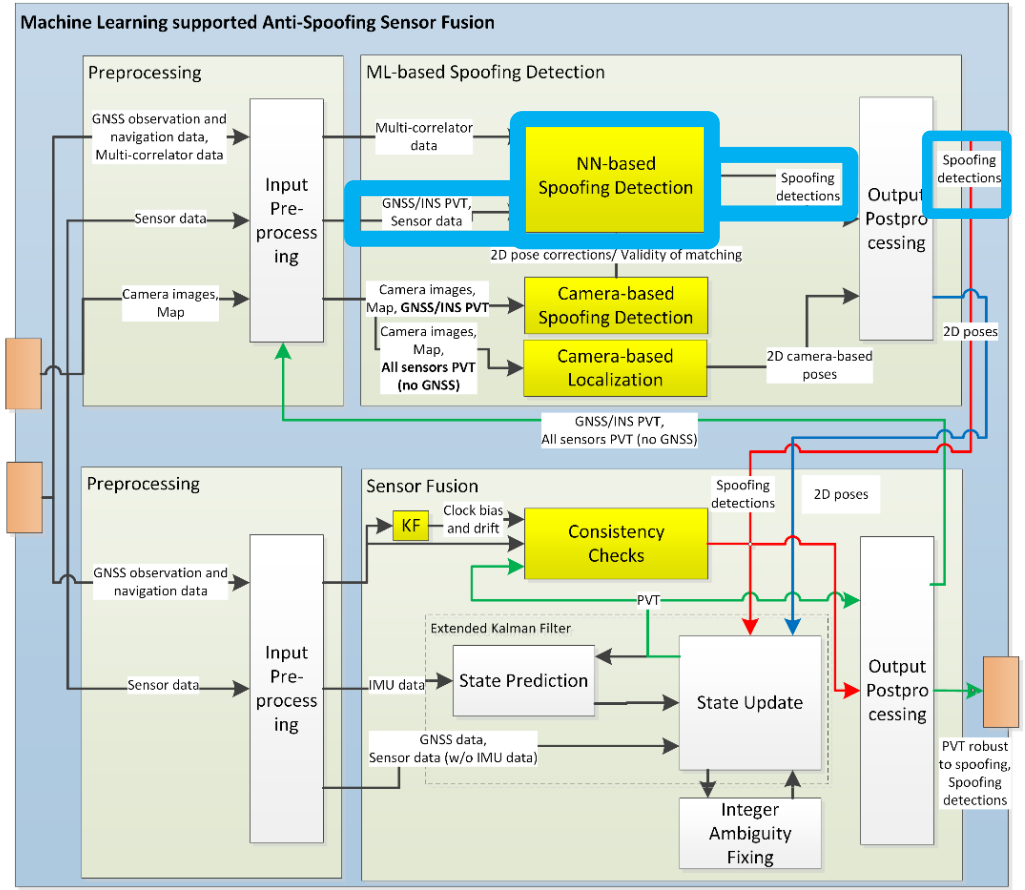


Results: NN-based spoofing detection – Sensor vs. GNSS-derived measurements

Advanced Navigation Solutions

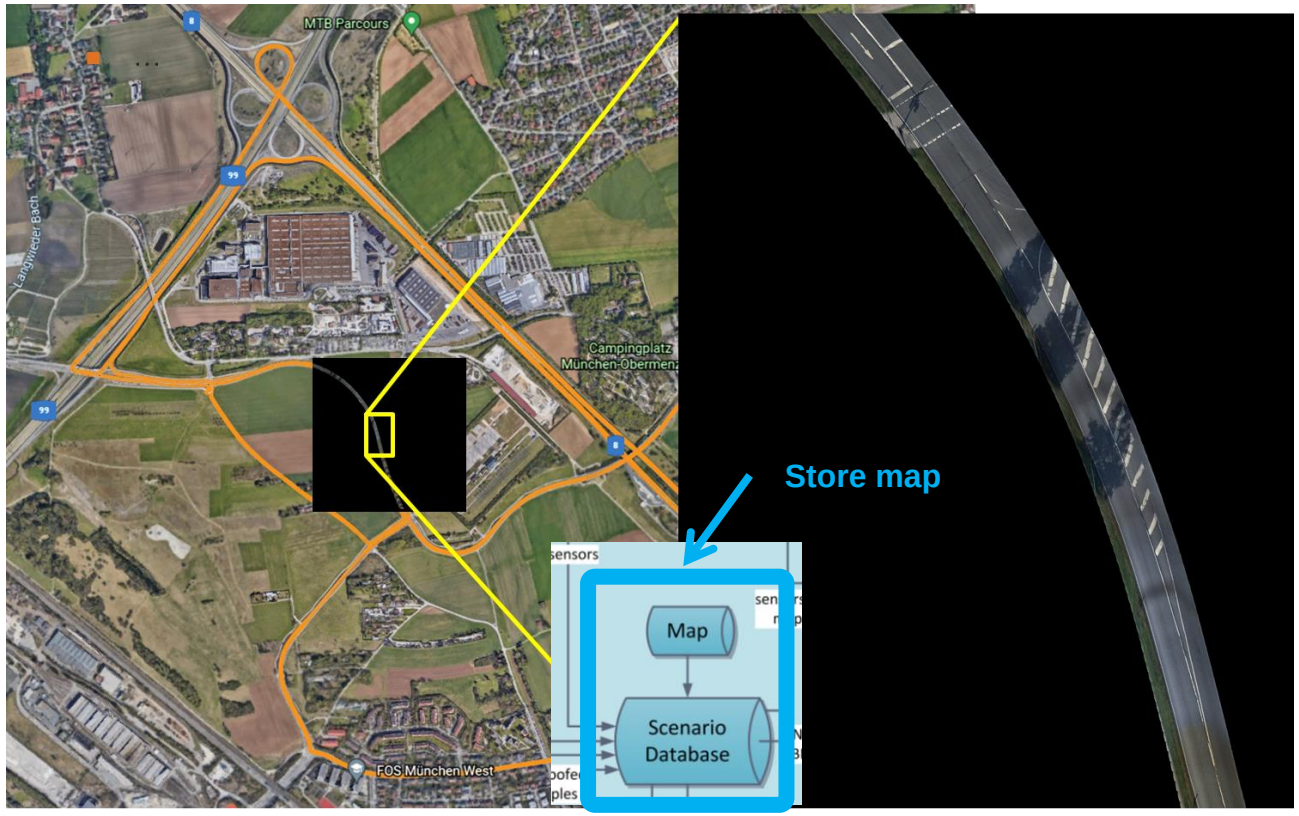


Spoofing detection across time (marked red) for a simulated coordinated attack (attack start marked with red dashed line). Consistency check of wheel odometry velocity (orange) and GNSS/IMU EKF derived velocity (blue). Signal difference in yellow.

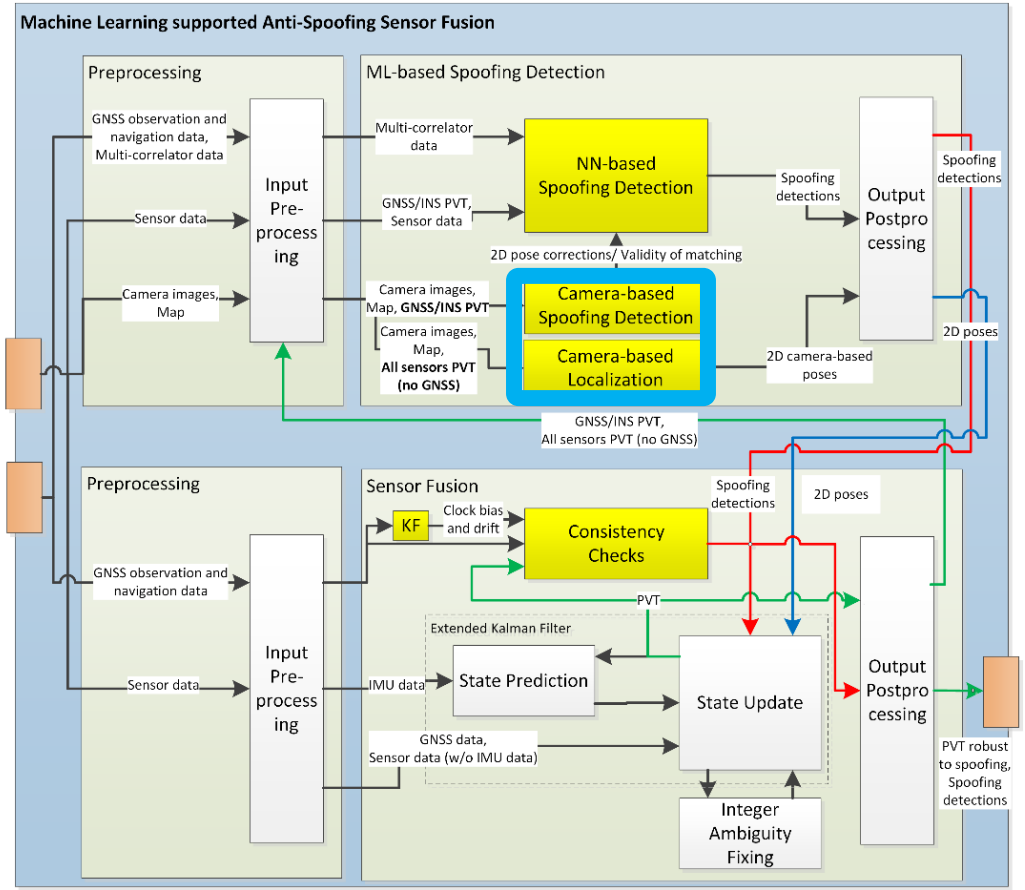


Results: Camera-based localization – Road map generation

Advanced Navigation Solutions

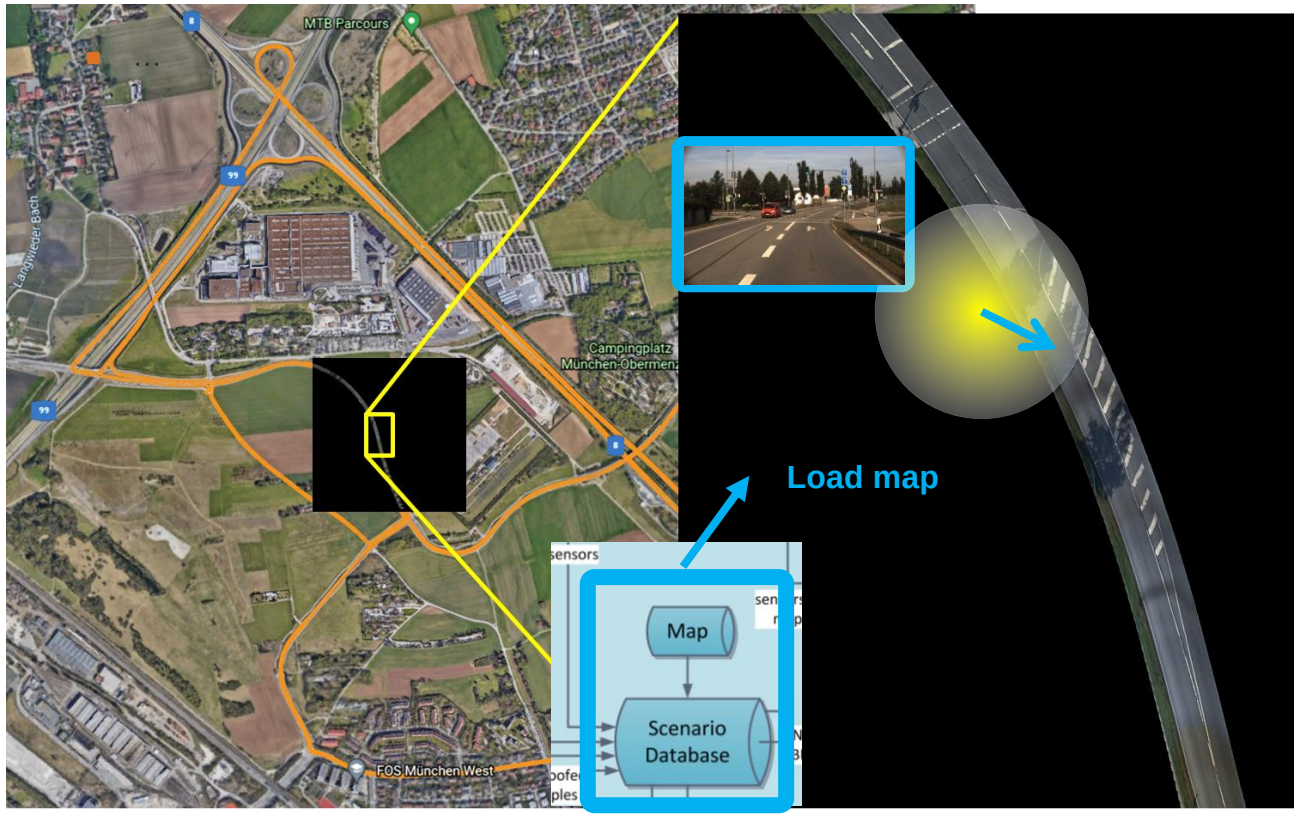


Road map generation from bird's eye projected camera images.

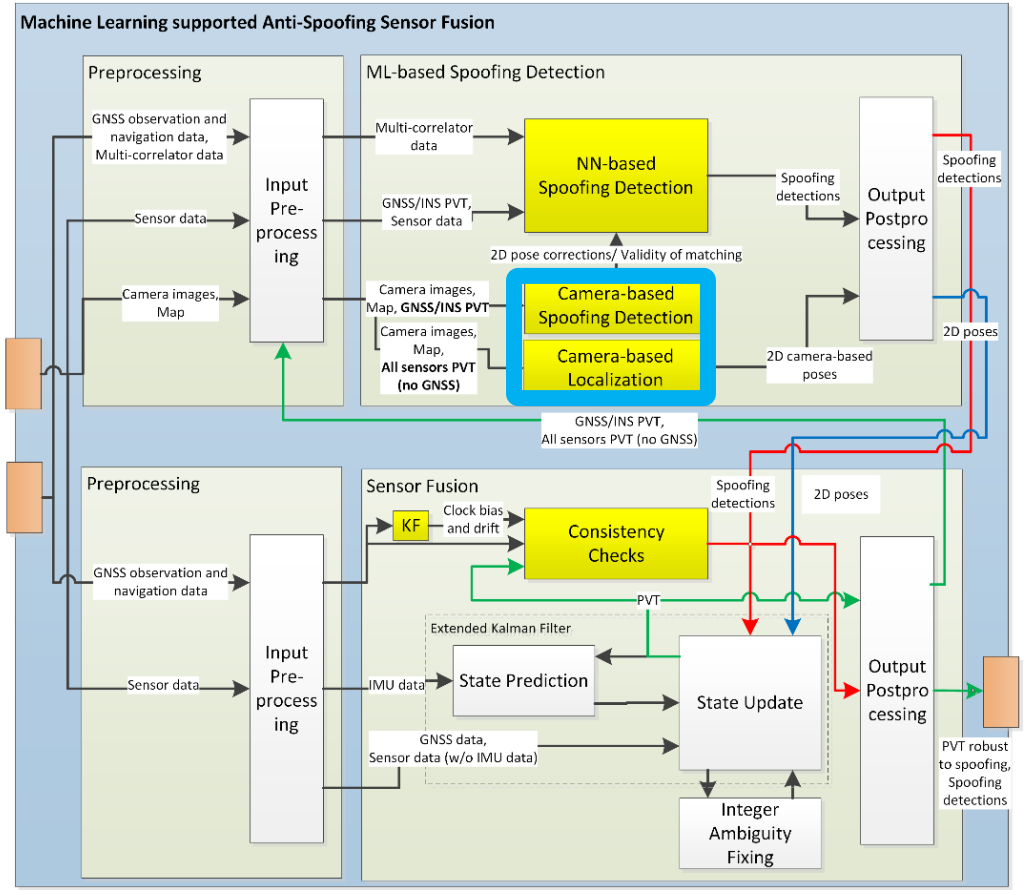


AIRBUS ANAVS

Results: Camera-based localization – Two applications

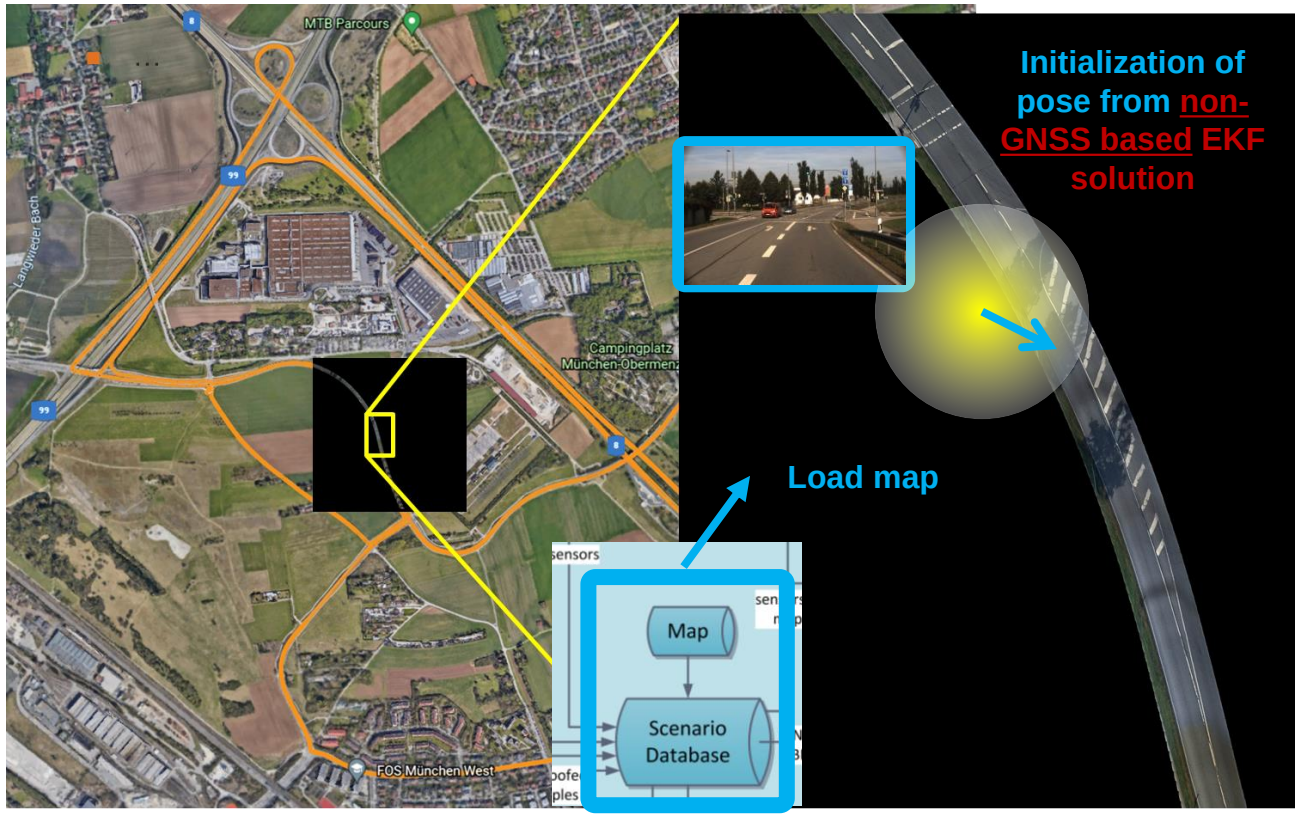


Road map generation from bird's eye projected camera images.

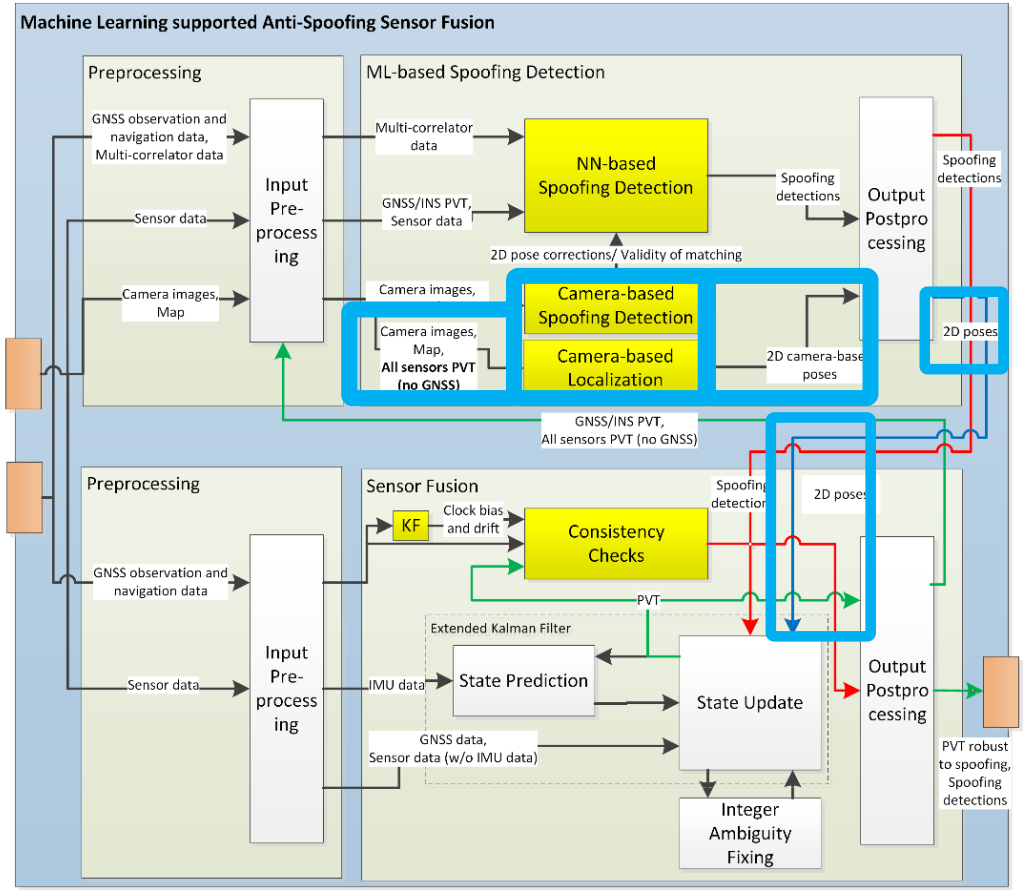


Results: Camera-based localization – Spoofing mitigation using camera-based pose from camera-image-to-map matching

Advanced Navigation Solutions

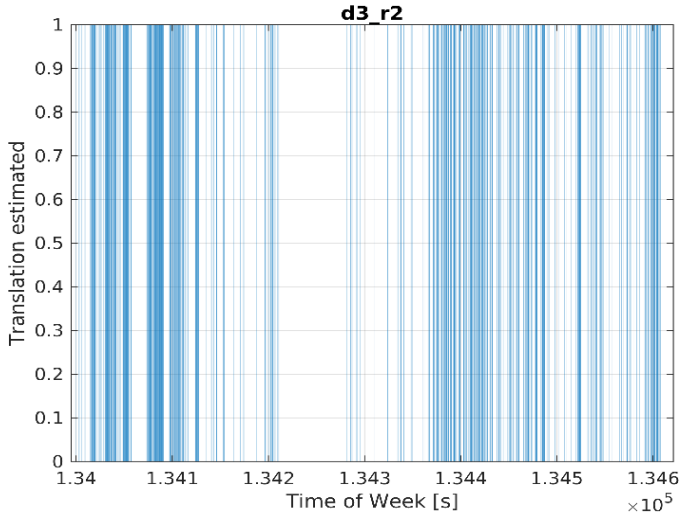


Road map generation from bird's eye projected camera images.

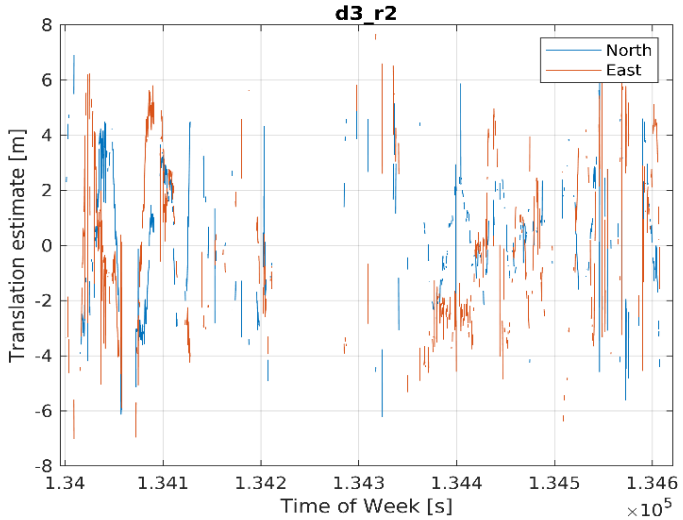


Results: Camera-based localization – Spoofing mitigation using camera-based pose from camera-image-to-map matching

Advanced Navigation Solutions



Valid camera-image-to-map matches

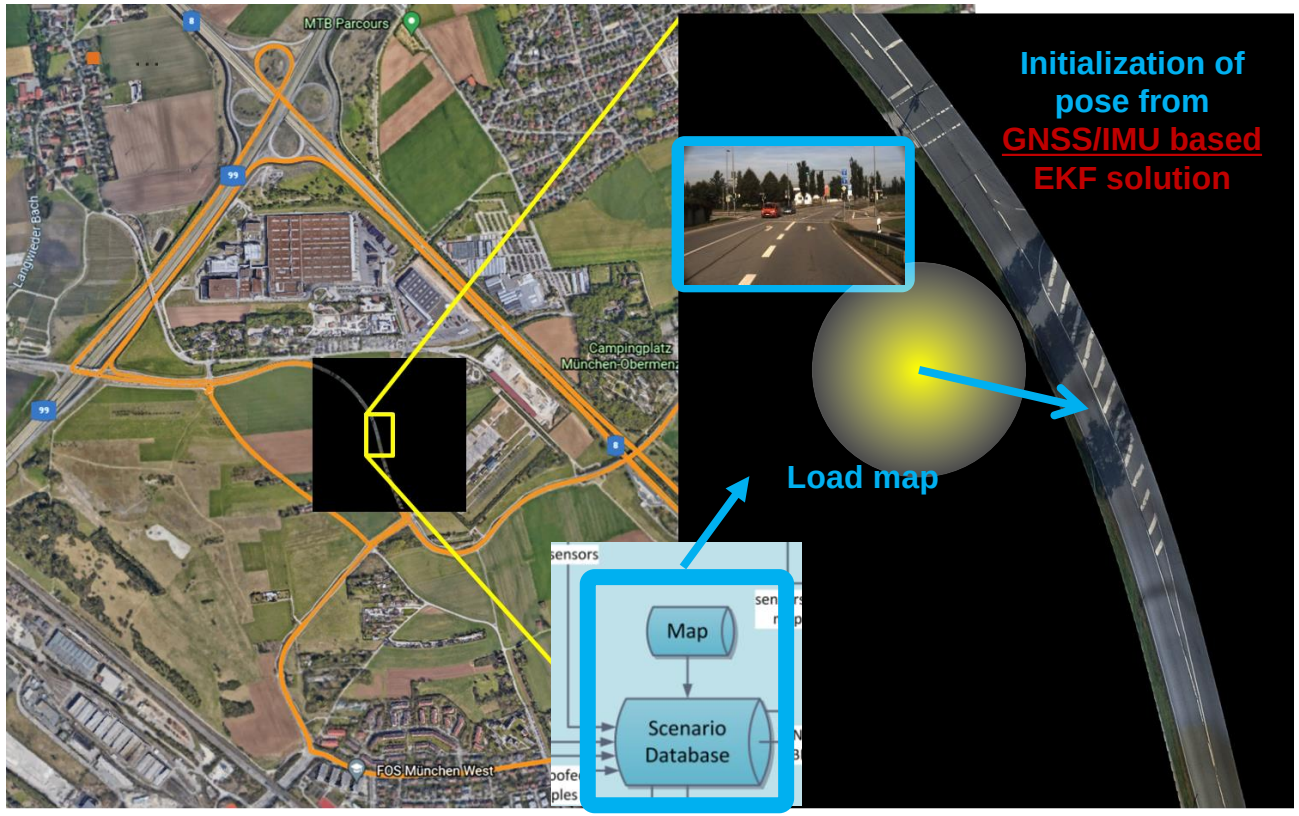


Estimated pose errors (North and East)

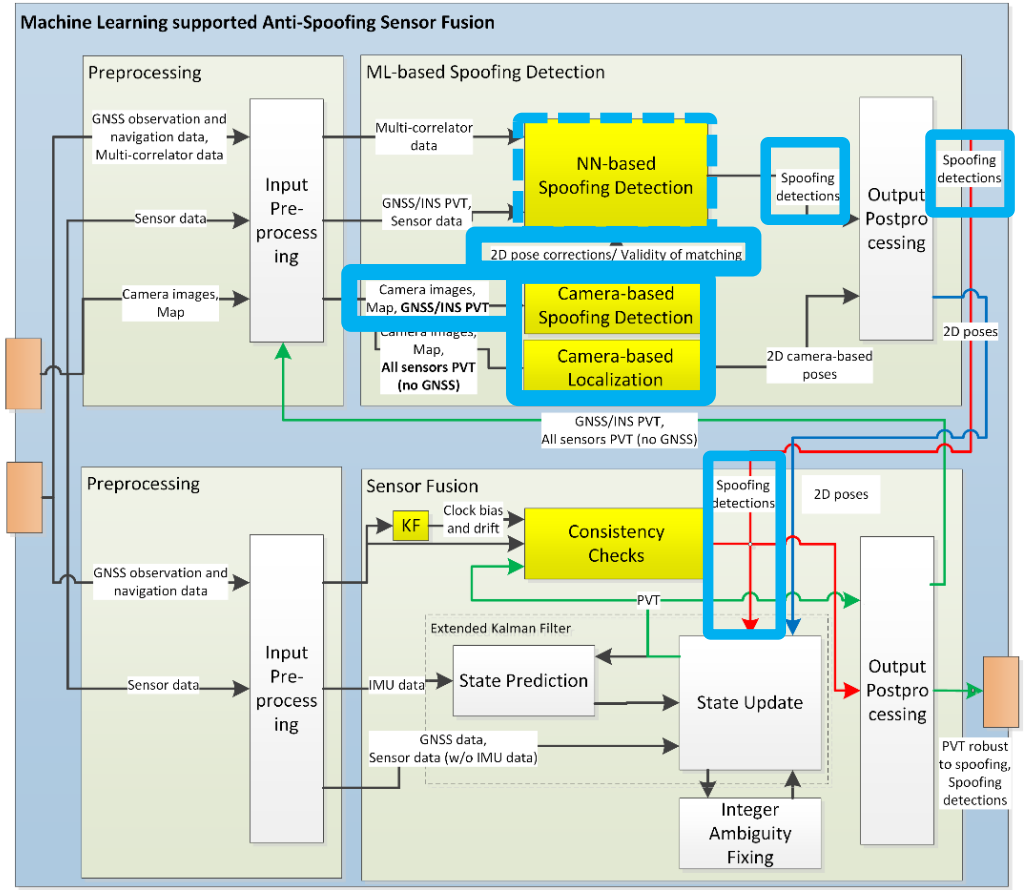
→ Camera-based absolute poses for sensor fusion

Results: Camera-based localization – Spoofing detection by camera-image-to-map matching

Advanced Navigation Solutions



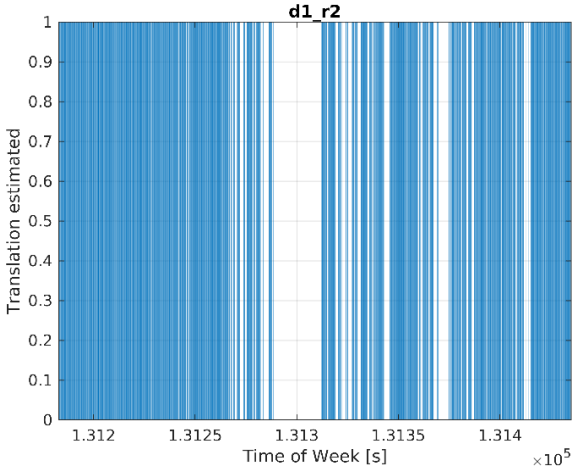
Road map generation from bird's eye projected camera images.



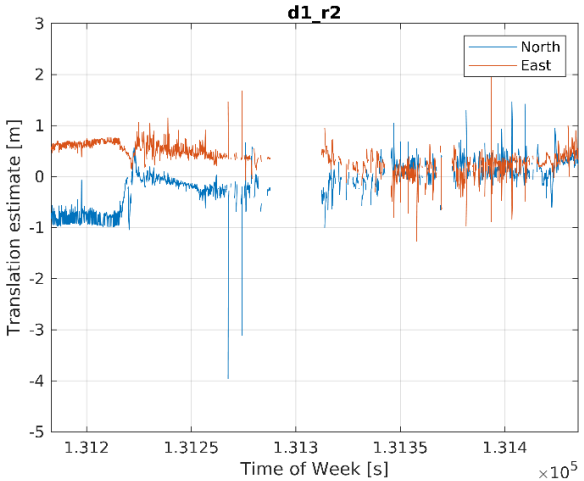
AIRBUS ANAVS

Results: Camera-based localization – Spoofing detection by camera-image-to-map matching

Advanced Navigation Solutions

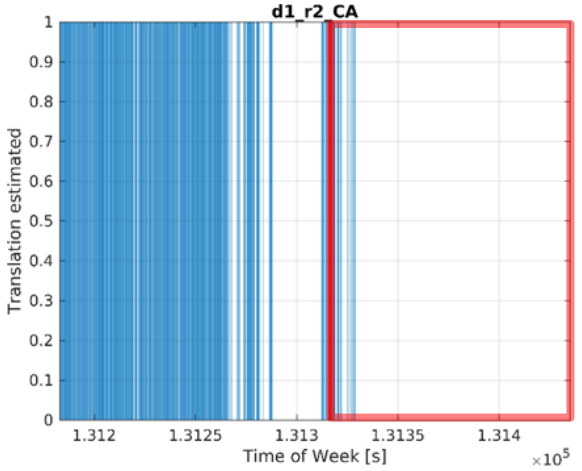


Valid camera-image-to-map matches

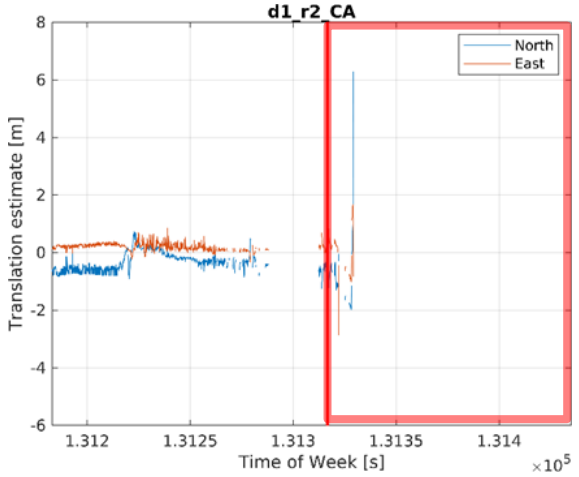


Estimated pose errors (North and East)

Camera-image-to-map matching in Nominal scenario / No Spoofing



Valid camera-image-to-map matches



Estimated pose errors (North and East)

Camera-image-to-map matching in Faulty scenario / Coordinated attack

AIRBUS ANAVS

Results: Overview

- Data Collection and Data Generation
- **Anti-Spoofing Techniques Results**
  - **Anti-Spoofing Sensor Fusion based on Machine Learning**
    - Individual techniques results
    - **Overall results**
  - GNSS SW Receiver (Airbus SDR) vs. COTS Receiver

Results: Anti-Spoofing Sensor Fusion based on Machine Learning.
Sensor fusion performance without spoofing mitigation.

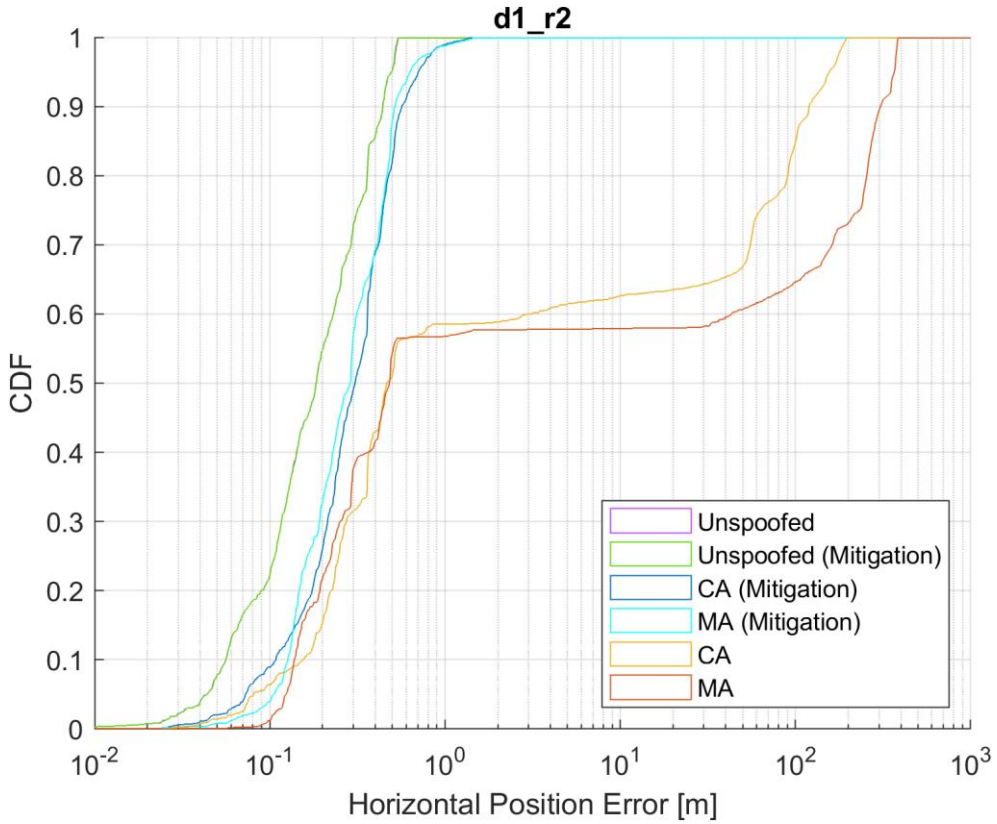
Advanced Navigation Solutions

Unspoofed,
Trajectory of low-dynamic scenario

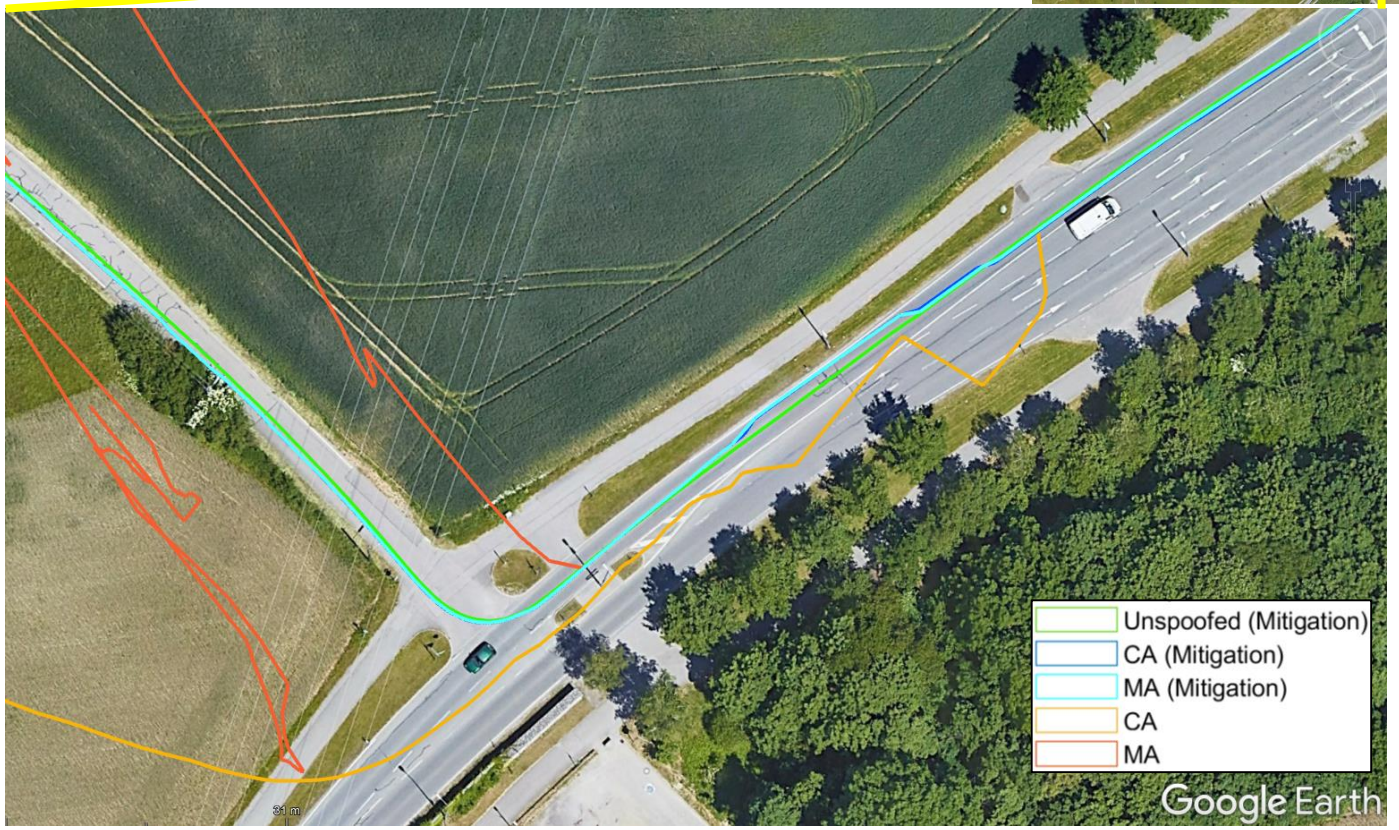
Coordinated attack,
Trajectory of low-dynamic scenario

Meaconing attack,
Trajectory of low-dynamic scenario

Results: Anti-Spoofing Sensor Fusion based on Machine Learning.
Sensor fusion performance with spoofing mitigation.



Performance of spoofing mitigation. Cumulative distribution function (CDF) of horizontal position error.



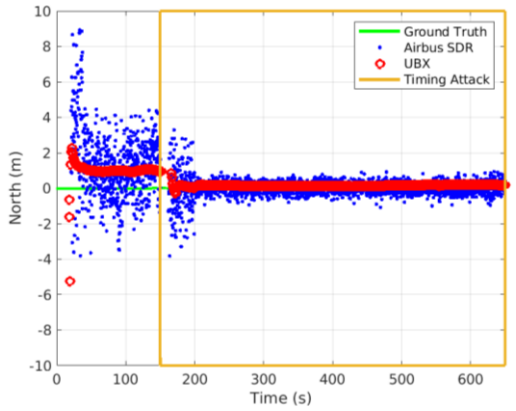
Comparison between mitigated unspoofed, mitigated CA and mitigated MA, and the CA and MA without mitigation.

Results: Overview

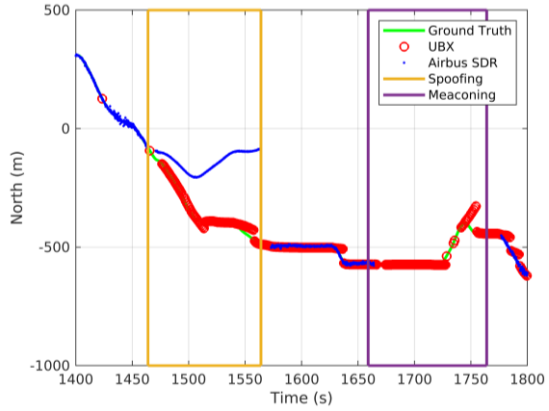
- Data Collection and Data Generation
- **Anti-Spoofing Techniques Results**
  - Anti-Spoofing Sensor Fusion based on Machine Learning
  - **GNSS SW Receiver vs. COTS Receiver**

Results: GNSS SW Receiver vs. COTS Receiver

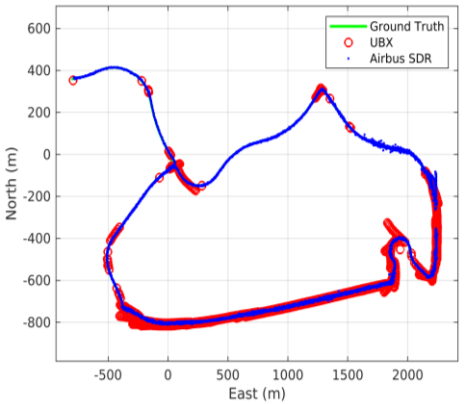
- Classical AS techniques of SW-receiver not effective against simulated spoofing attacks (a,b)
- COTS receiver was resistant against coordinated and meaconing attacks, but not effective against timing attack (a,b)
- Ublox receiver shows partially very low availability (c)
- Ublox solution shows strong extrapolation artifacts, even when signal with sufficient quality are available (d)



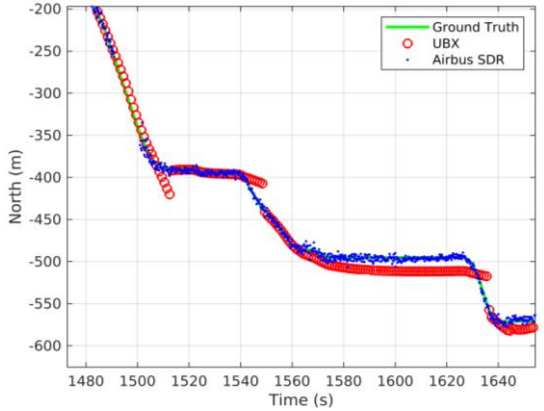
a) Timing attack fools SW-receiver and Ublox



b) Coordinated and meaconing attack affect SW-receiver, but not Ublox (in this case)



c) Low availability of COTS solution

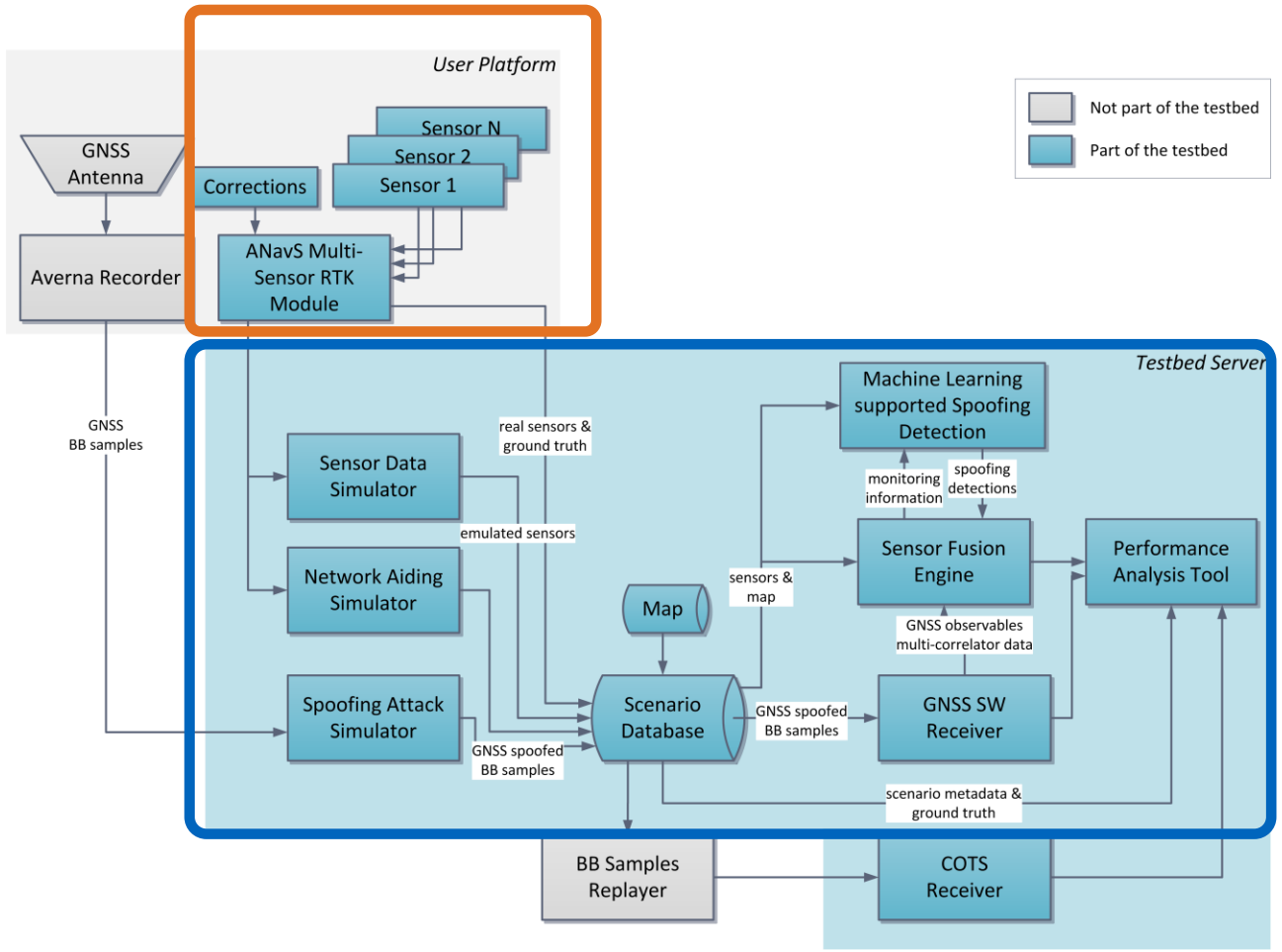


d) Strong extrapolation of COTS receiver

Outline

- Motivation
- **Innovative Anti-Spoofing Testbed with Sensor Fusion and Machine Learning**
  - Design
  - Results
  - **Software and Hardware**
- Summary
- Next Steps

Software and Hardware – Overview



High-level testbed architecture

- **Hardware Modules**
  - Multi-Sensor RTK Module
  - Computer Vision Module (NVIDIA Jetson embedded platform)
- **Software Modules**
  - Sensor Data and Network Aiding Simulator
  - Spoofing Attack Simulator
  - GNSS SW Receiver
  - Anti-Spoofing Sensor Fusion based on Machine Learning
  - Performance Analysis Tool

Hardware Deliverables – Overview

Advanced Navigation Solutions

MSRTK Module

- Industrial Casing (with Touchscreen)
- 3x Ublox Dual-Frequency GNSS Receivers
- 3x Survey-grade GNSS Antennas
- High-grade MEMS IMU (Epson-MG370)
- Interfaces:
  - Ethernet
  - Wi-Fi
  - CAN
  - LTE

Multi-Sensor RTK Module

NVIDIA Jetson Xavier NX

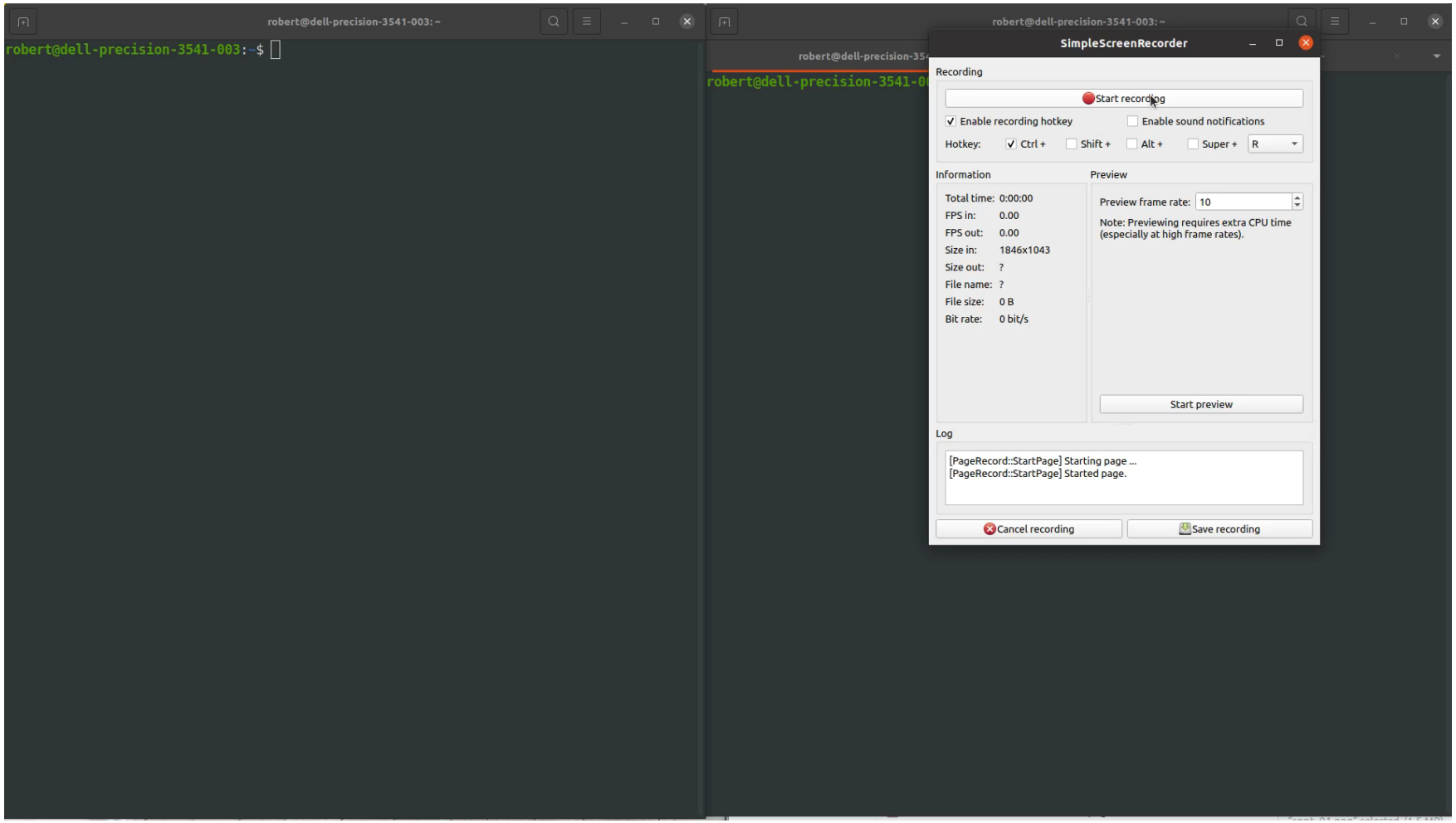
- AI-power: 21 TOPS
- GPU: NVIDIA Volta™-GPU mit 384 Cores und 48 Tensor-Cores
- CPU: NVIDIA Carmel ARM® v8.2 64-Bit-CPU, 6 Cores
- RAM: 16 GB
- Interfaces:
  - Ethernet
  - USB
  - MIPI/CSI
  - HDMI

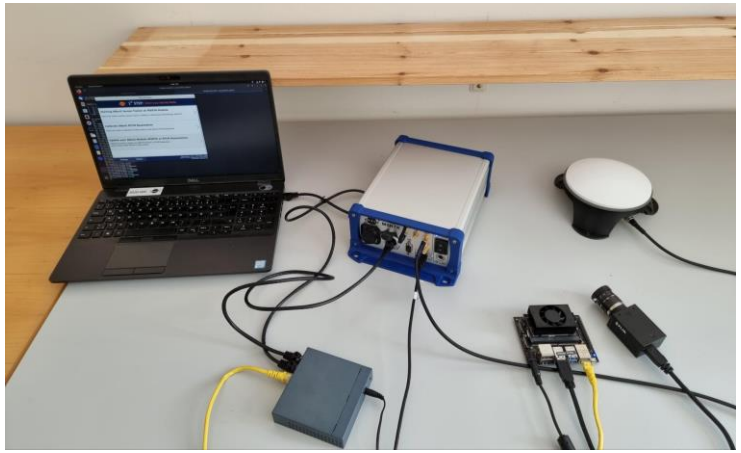
High-quality RGB camera (FLIR Grasshopper3)

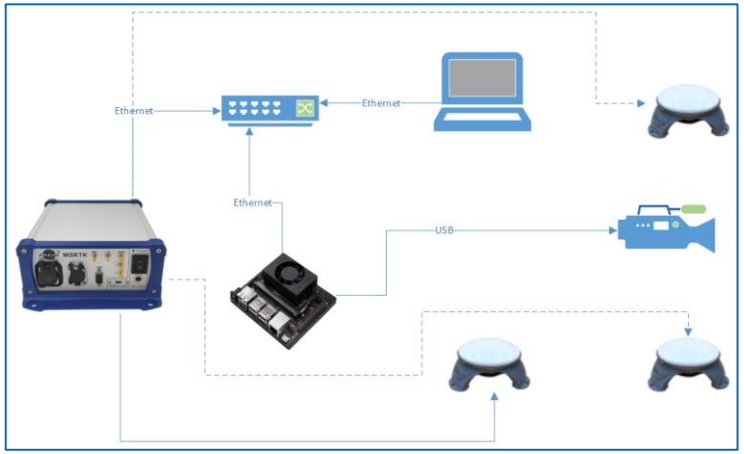
Computer Vision Module

Hardware Deliverables – Demo Video

Advanced Navigation Solutions







AIRBUS

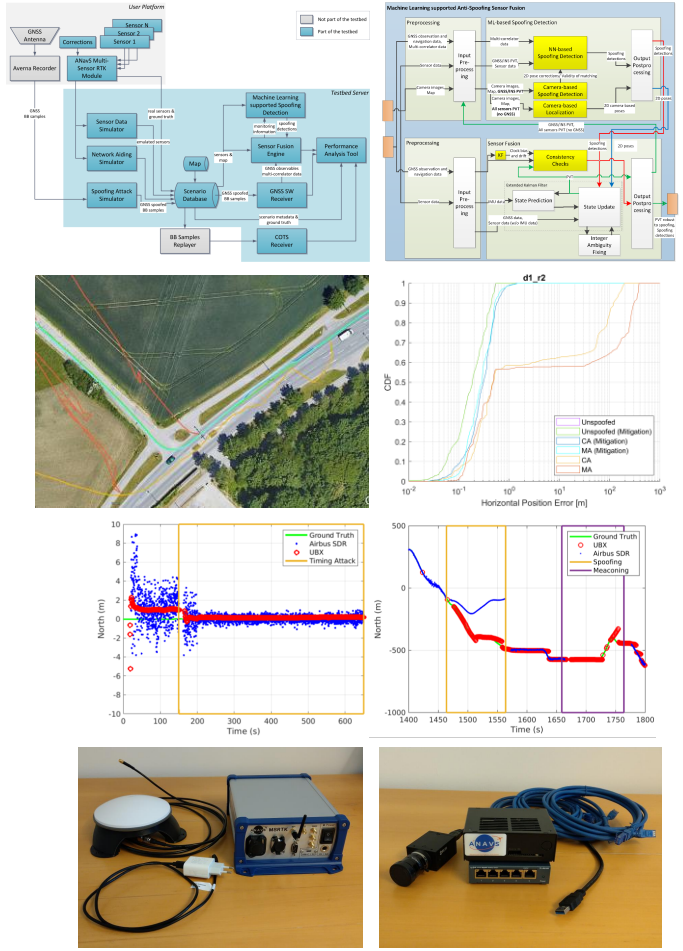
ANAVS

Outline

- Motivation
- Innovative Anti-Spoofing Testbed with Sensor Fusion and Machine Learning
  - Design
  - Results
  - Software and Hardware
- **Summary**
- Next Steps

Summary

- Flexible anti-spoofing testbed, including sensor data and spoofing attack simulation developed
- Innovative anti-spoofing sensor fusion based on machine learning developed, that achieves very promising results in all tested scenarios
- Comparison to classical anti-spoofing techniques and performance of a COTS receiver
- Testbed software and data acquisition hardware provided



Outline

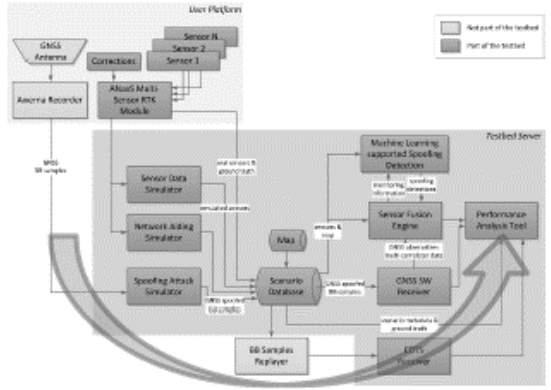
- Motivation
- Innovative Anti-Spoofing Testbed with Sensor Fusion and Machine Learning
  - Design
  - Results
  - Software and Hardware
- Summary
- **Next Steps**

ENABLING TECHNOLOGIES FOR SECURE POSITION-NAVIGATION-TIME USER SEGMENTS

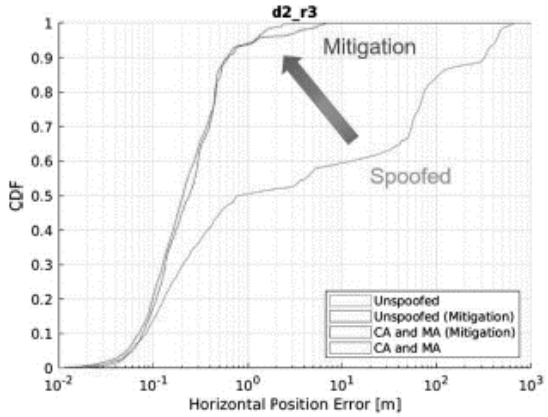
Contractor(s): ANavS (DE), Airbus Defence & Space (DE)		ESA Budget:	600k€
TRP T606-606ES	Contract 4000129660	YoC: 2023	TO: Gianluca Caparra (TEC-ESN)
TRL Initial: 2	Achieved: 4	Target TRL: 3 Date: Q4 2022	

Next Steps

- Secure, robust and accurate positioning enabled by camera-, LiDAR- and/or RADAR-based localization on custom and publicly available maps.
- General purpose flexible machine learning techniques for multi-sensor data anomaly detection.
- → D501: TN – Guidelines for Sensor fusion-based GNSS AS and Potential System Evolution



Testbed architecture



Spoofing mitigation performance

Thank you for listening!

Questions?

Contact information

www.anavs.de

Managing director:	Dr. Patrick Henkel
Phone:	+49 (0) 89 890567-21
Fax:	+49 (0) 89 890567-20
Email:	patrick.henkel@anavs.de

Address:

ANavS GmbH
Gotthardstraße 40
80686 München

Advanced Navigation Solutions