Cybersecure GNSS for Autonomous Mobility

ESA NAVISP-EL2-109 **CECIL**

Final Presentation
09/10/2025

Dr. Bertalan Eged, CEO

Sagax Communications, Ltd.

www.sagaxcommunications.com

www.linkedin.com/company/sagaxcommunications

Agenda

- Company introduction
- Problem statement and mitigation
- System architecture HW and SW
- Project introduction WBS and Timing
- Designed and manufactured components
- Laboratory and field validation and demo (video)
- Summary of experiences
- Future outlook

Company introduction: fields of play

Aerospace and Defense	Test and Measurement	Scientific Research
Signal and Communications Intelligence	Spectrum monitoring systems and radiated measurements	High channel count transceivers and antenna systems

Sagax Communications **deliver** advanced radio electronic **solutions** with mature mainstream commercial technology.

Subject matter expertise:

- Electromagnetic simulation and antenna element and array design
- Analog signal conditioning with high dynamic range multiple source and sink analog connectivity
- Wide-bandwidth and high-frequency multi-channel conversion of analog signals (ADC/DAC)
- High-throughput data acquisition and generation with record and playback (RnP)
- Off-line and real-time digital signal processing with parallel processing resources (GPP, GPU, FPGA)

System integration

Stand-alone operation | Integrated operation | Integrated systems

Receiver and test systems integration
From man-portable receiver to integrated site
With direction finding and record-playback-delay


Portable


Desktop


Connected


Extended


Station


Work-post


Operation-site

Problem statement

- Industry and society have embraced and **depend on** the space/satellite based navigation systems. (GNSS)
- These systems are target of **electromagnetic and cyber-attacks** which are recently proved to be existing threat to our community.
- Jamming and **spoofing of GNSS systems** are real danger and can block lot of mission critical infrastructure and day by day activity

GPS

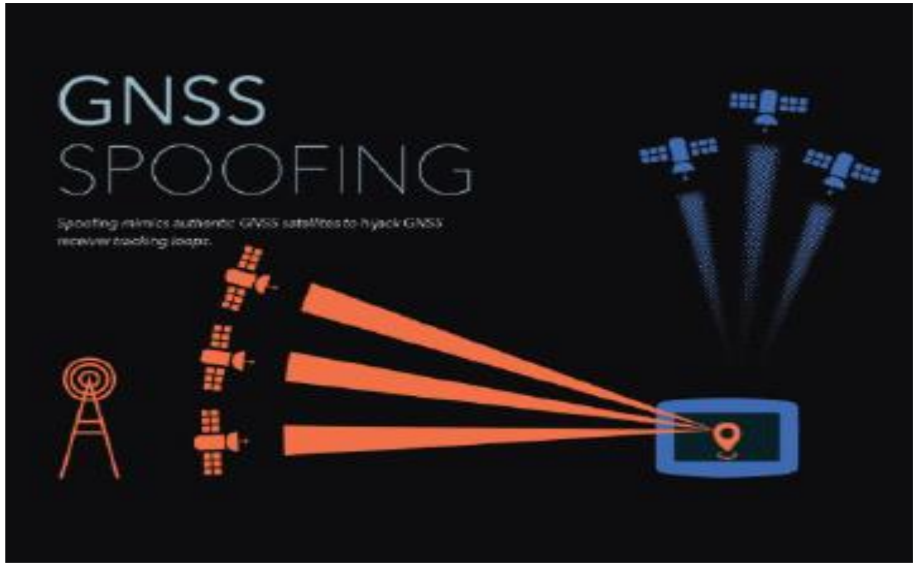
Glonass

Galileo

BeiDou

Spoofing mitigation in the antenna domain

The physical source of the signal is different for original and spoofing signal



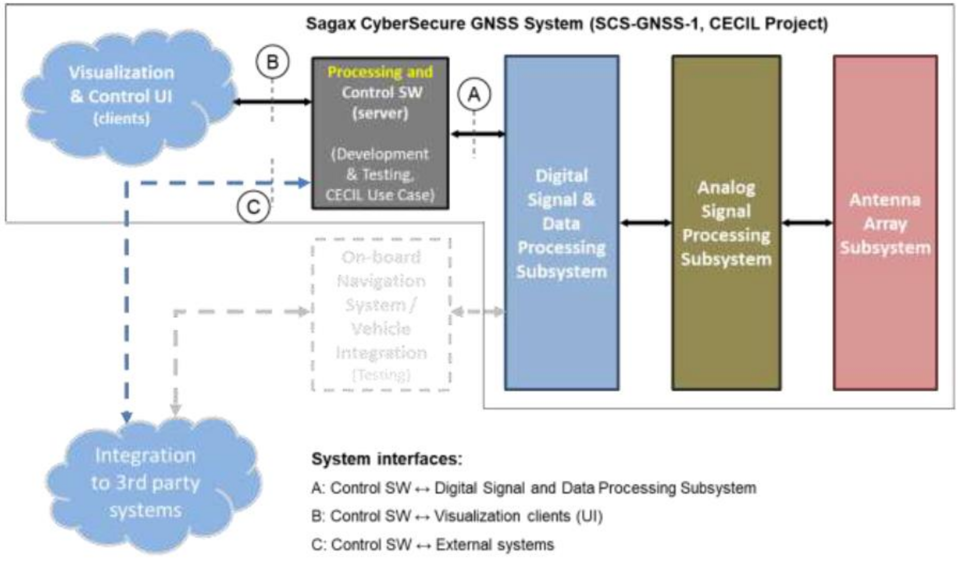
GNSS Spoofing Mitigation technic based on special antenna sensor

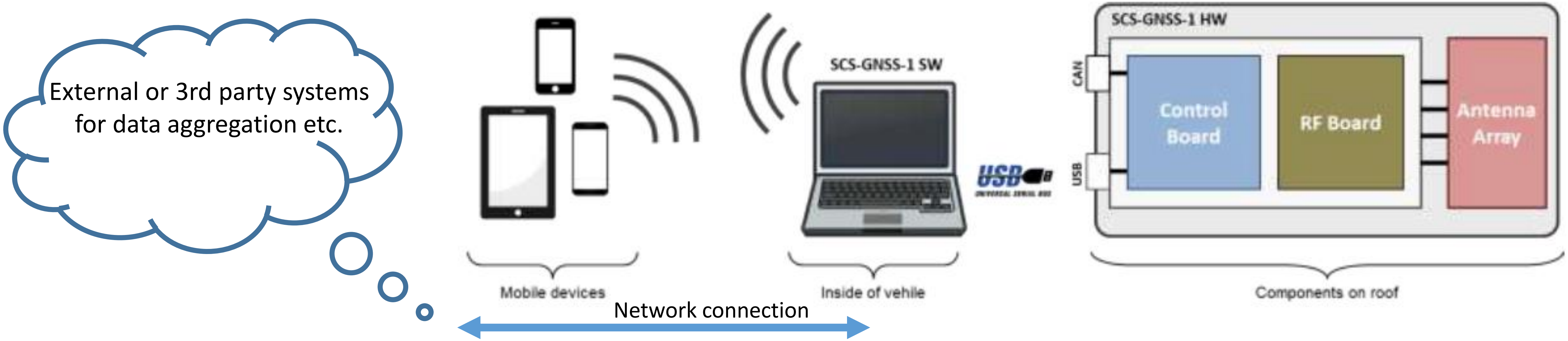
esa NAVISP

ESA NAVISP-EL2-109 CECIL

CECIL System Architecture

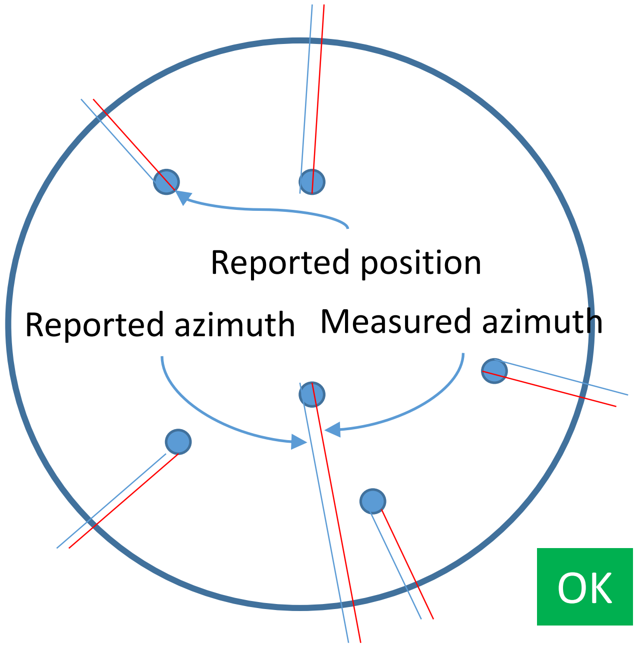
- CECIL consists of a 4 antenna array and connected analog-to digital, processing and control board
- The control board is connected to and external computer running the data processing, visualization and external connectivity software

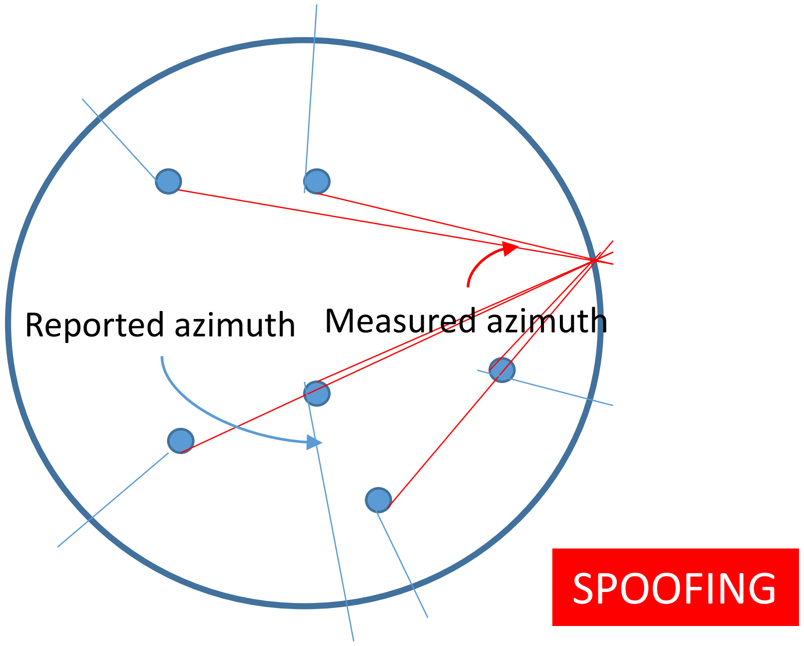


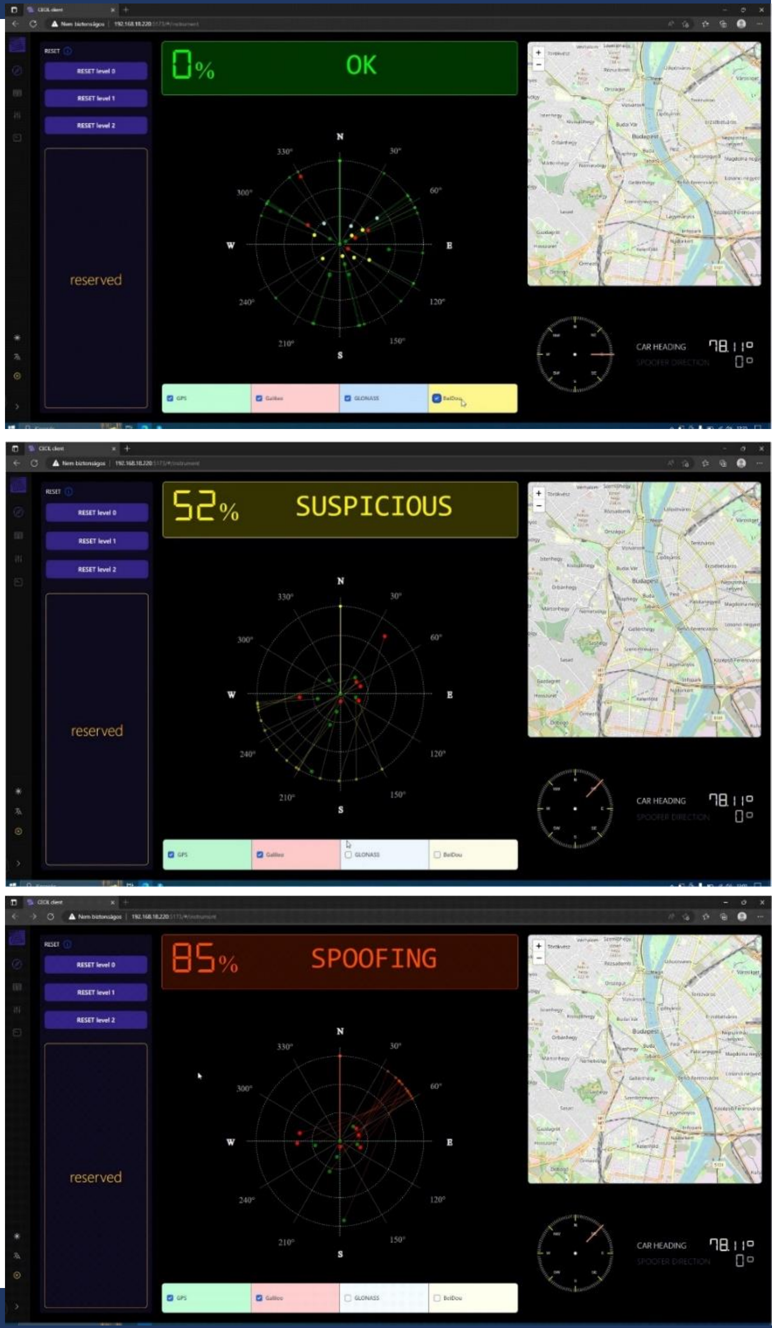


CECIL software functions

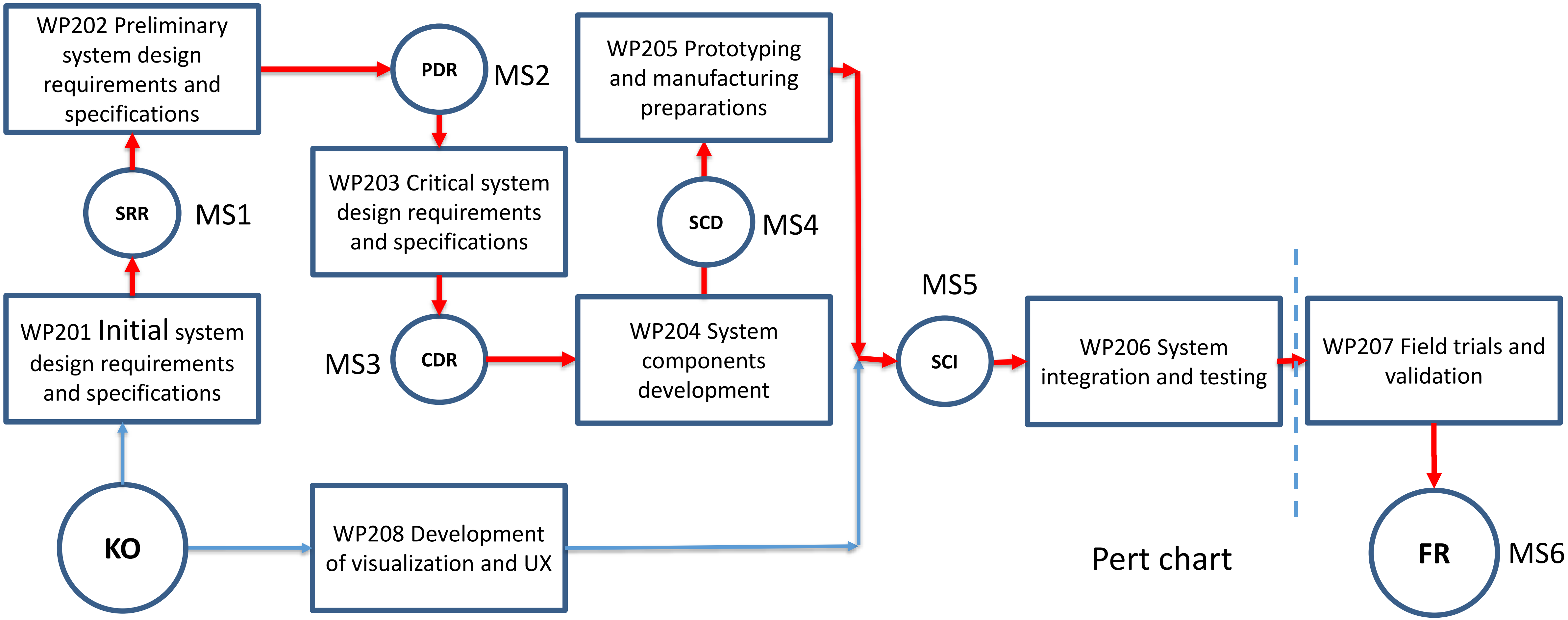
- Calculating the reported azimuth of the reported satellite position
- Compare the reported and measured azimuth by the sensor
- Non-aligned signals where azimuths different are likely spoofed
- Calculate the alignment level and compare the preset thresholds



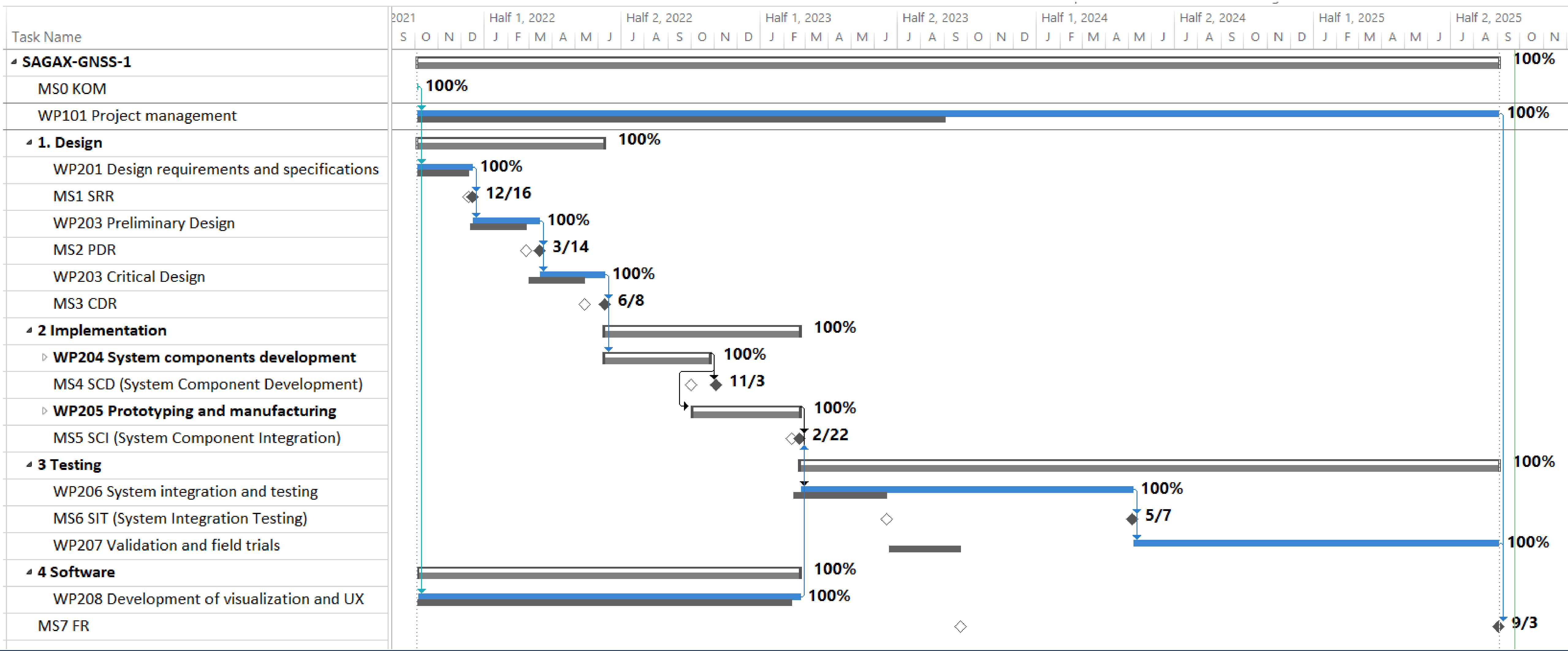




Project outline: WBS on Pert chart

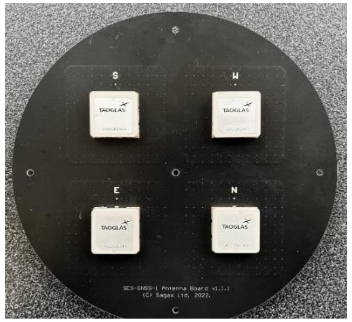


Project outline: tracking-Gantt

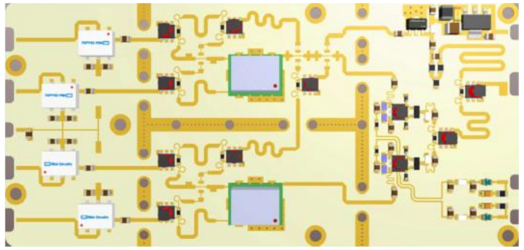


Manufacturing and integration

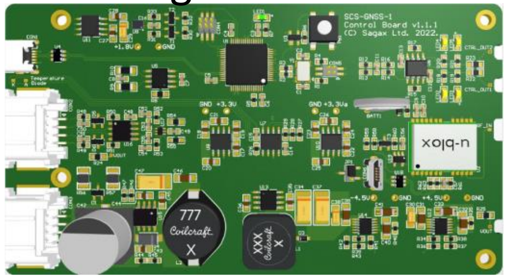
Antenna board



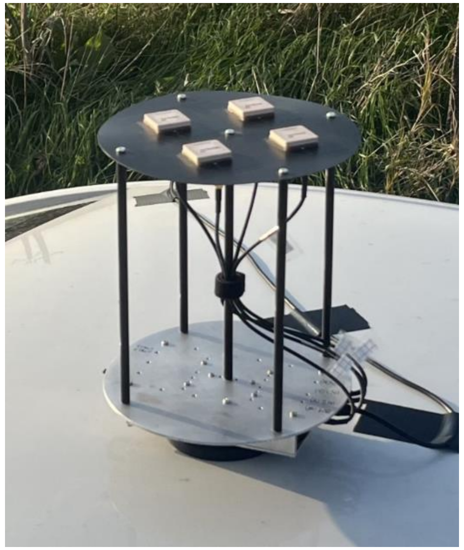
Analog/RF board



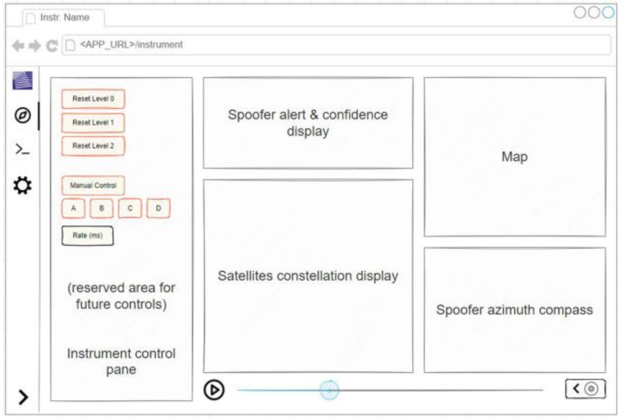
Digital board



Antenna and sensor assembly

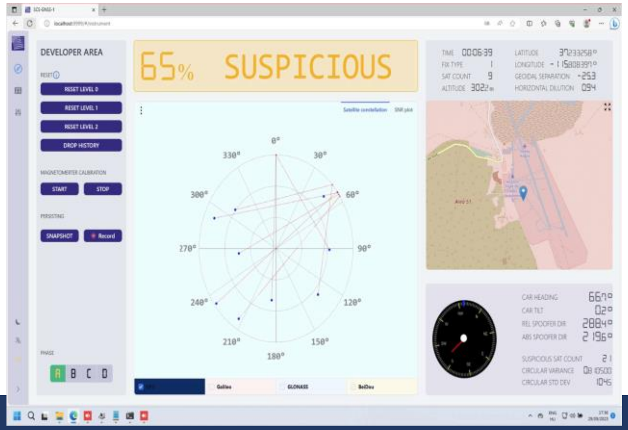


UI software design



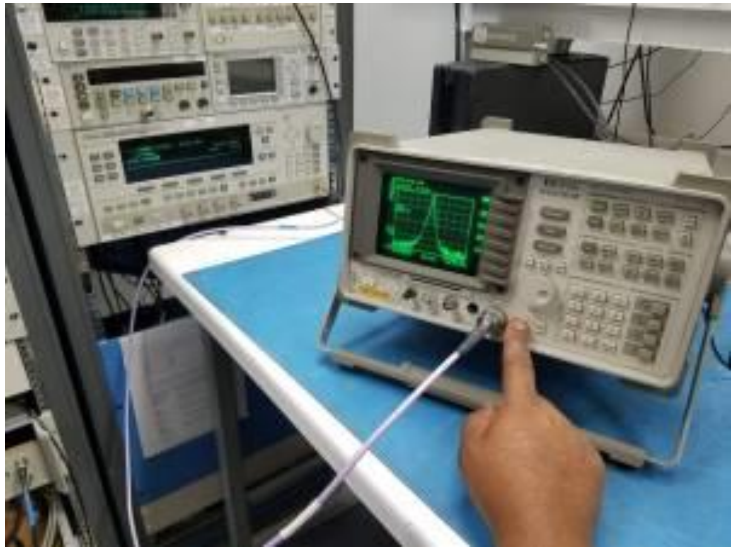
Circuits box

Control and UI software



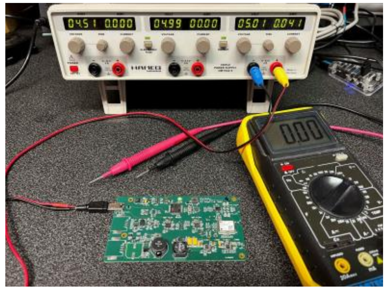
Laboratory and field validation

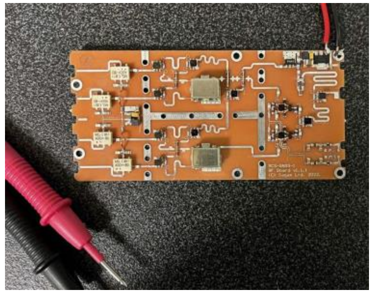
Lab validation



Field validation

Test drive demos

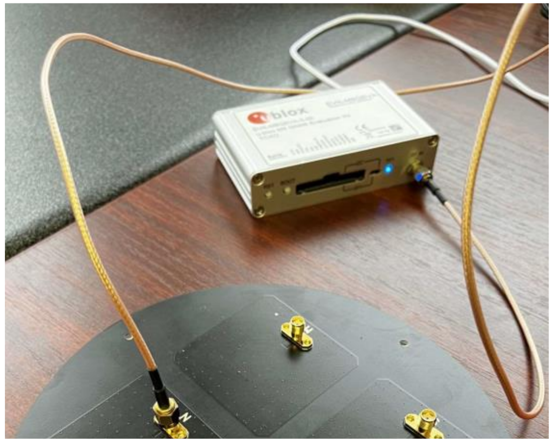


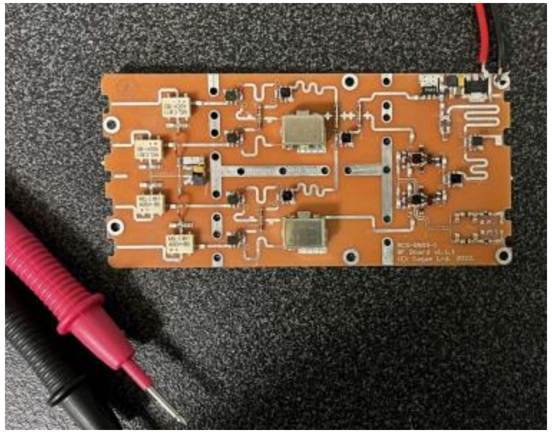


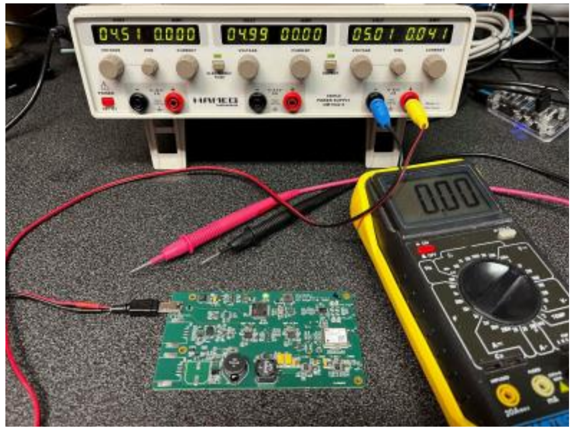
EMC Lab ≠ Antenna Lab

Laboratory test and integration

- Evaluation of the Production of the Components
  - Antenna Boards
  - Analog RF Boards
  - Control Boards
  - Aluminum cages
  - Control and visualization software
- Integrate the overall system raedy for field validation and trials





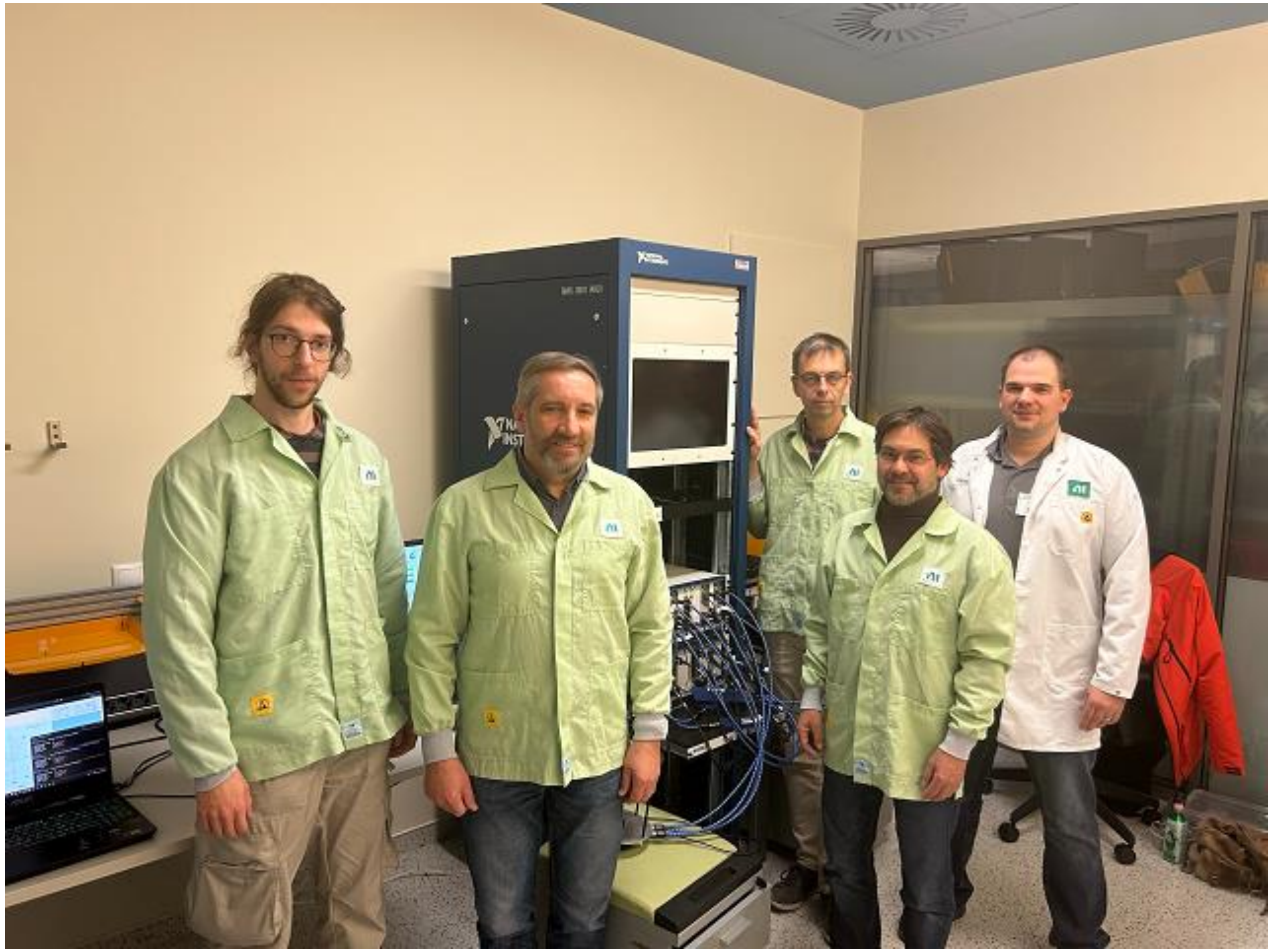


Testing with recorded signals

OPEN INNOVATION LAB NAVISP-EL3-027

https://navisp.esa.int/project/details/261/show

- 4ch coherent record and playback system by NI was used
- Recorded signals during the 2024 Jammertest (Norway) with 4 antennas
- Phase coherent playback of the 4 antenna signal connected to the input
- Spoofer well detected ☺



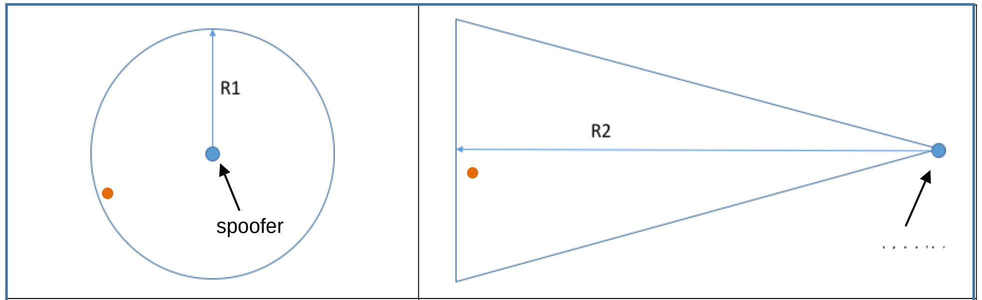
Field validation tests and demonstration

- The scope and criteria
  - To **test and validate the entire prototype system** developed in the SCS-GNSS-1 project in order to ascertain its behavior in a quasi-real life environment
  - Learn about its potential shortcomings in various scenarios.
  - The validation has to show weather if the system fulfils the *User Requirements*
- Types and number of test cases
  - Under ***static conditions*** in order to determine certain operation parameters, like spoofer range, and the required minimum interaction time.
  - Several ***dynamic*** **real-life operating** environments with *moving vehicle* resulting in *pass/fail results* and/or *likelihoods* on missed detections and false alarms.

The spoofer device and antennas

HackRF One with Portapack H2 and accessories

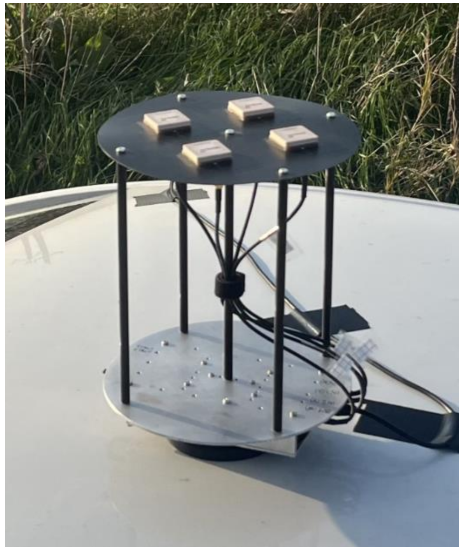
Omni- and directional antenna used by the spoofer



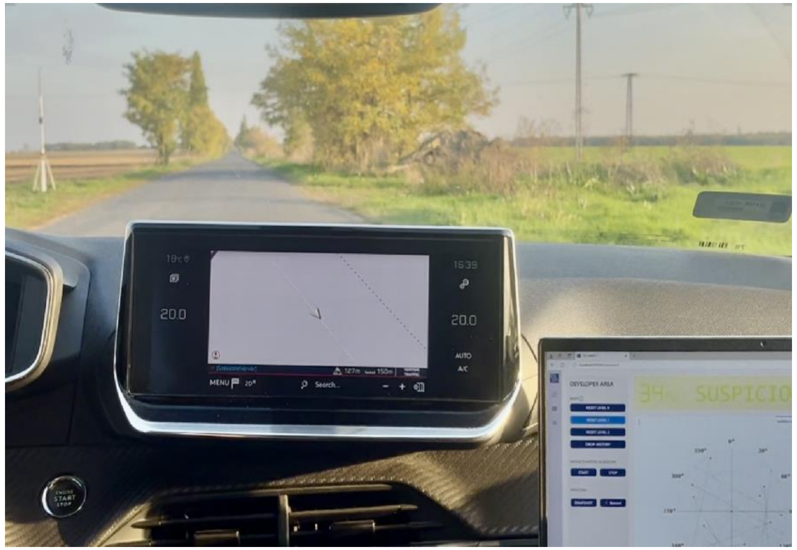
Spoofer coverage with *omnidirectional* antenna (no directional gain)	Spoofer coverage with a *directional* antenna (directional gain)

Device under test installation

Passenger car used during the test



Antenna array on top of the car



Software on laptop near dashboard

Test drives in different environments

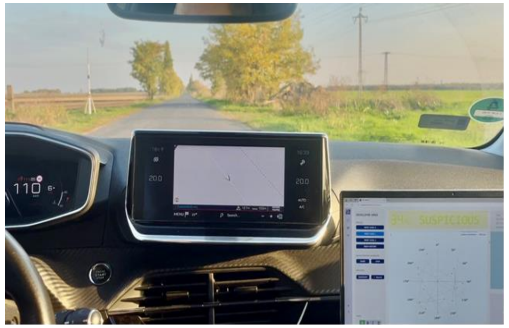
Open

Rural

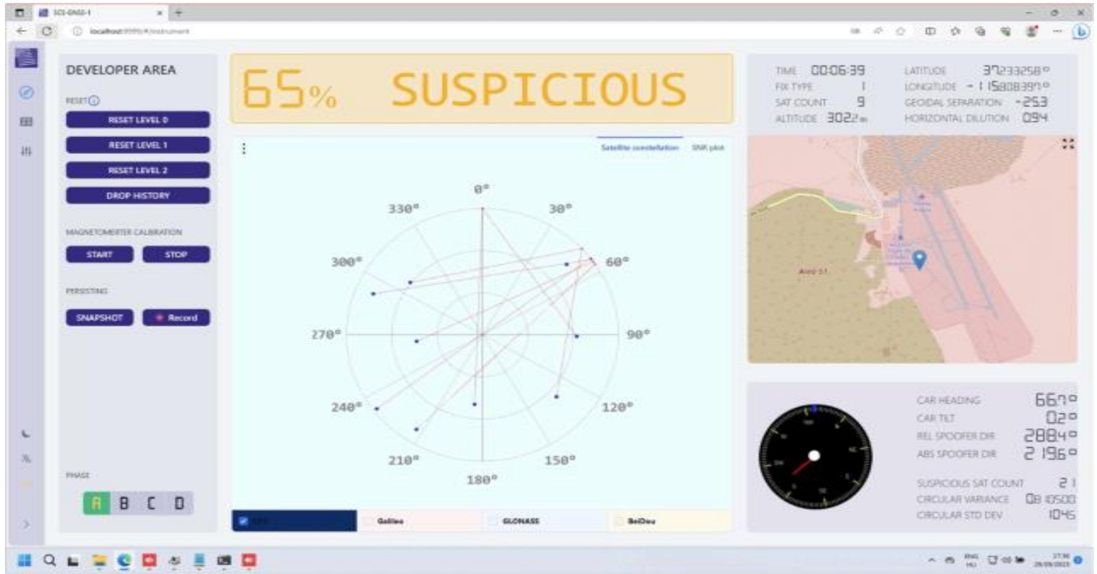
Urban

Antenna on top of the car

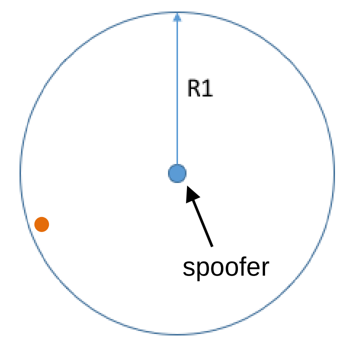
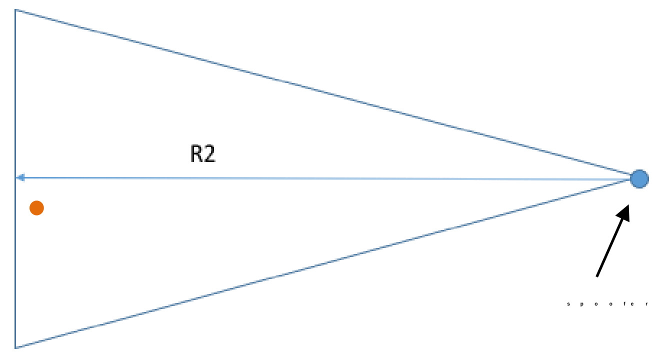
Computer next to dashboard



With control software running

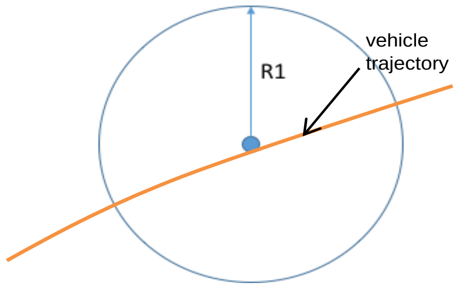
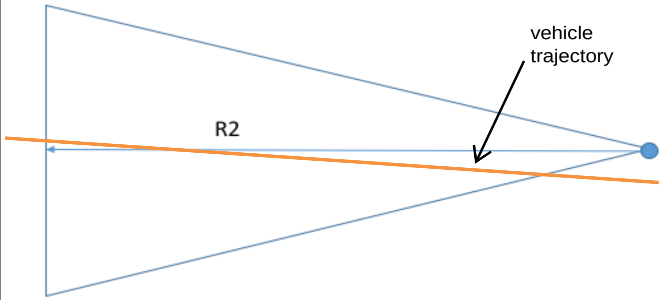


Static test results

	
Spoofer coverage with *omnidirectional* antenna (no directional gain)	**Spoofer coverage with a *directional* antenna** (directional gain)
Expected ‘low power’ coverage (R1): < 20 m Expected ‘high power’ coverage (R1): < 80 m	Expected ‘low power’ coverage(R2): < 60 m Expected ‘high power’ coverage (R2): < 240 m
Interaction time: ∞ (30 sec, max) (static situation, *distance* to be tested)	
Environment Planned: “open” (low reflections), “suburb” (mid reflections), and “urban canyon” (high reflections) Tested: “open” (low reflections) only. (*See explanation below.*)	

The sensitivity and detection speed of our SCS-GNSS1 system in a close-to-the-ideal open field (low reflection) environment					
The can lock to a typical spoofer in a distance less than 200 m. (SR#5) The system detect a typical spoofer and give an initial azimuth angle in not more than 5 sec (SR#5)		**Spoofer antenna**			
		Omnidirectional		**Directed**	
Spoofer Power	**Low** (spoofer power)	Can detect in less than 5 sec:	**40 m**	Can detect in less than 5 sec:	**60 m**
		Max detection distance (detection in 30 sec):	**120 m**	Max detection distance (detection in 30 sec):	**180 m**
	Boosted with +10 dB	Can detect in less than 5 sec:	**100..150 m**	Can detect in less than 5 sec:	**200..250 m**
		Max detection distance (detection in 30 sec):	**250 m**	Max detection distance (detection in 30 sec):	**250..300 m**

Dynamic results

	
Spoofer coverage with omnidirectional antenna (no directional gain)	**Spoofer coverage with a directional antenna** (directional gain)
Originally expected 'low power' coverage (R1): < 20 m Originally expected 'high power' coverage (R1): < 80 m	Originally expected 'low power' coverage (R2): < 60 m Originally expected 'high power' coverage (R2): < 240 m
Interaction time (to be tested) 40 sec, 20 sec, 10 sec, 5 sec, 2 sec (moving, dynamic situation)	
Corresponding speed ranges: (not all are feasible!)	
Low power: ~ 1.8 km/h … 36 km/h **High power:** ~ 7.2 km/h … 144 km/h	**Low power:** ~ 5.4 km/h … 108 km/h **High power:** ~ 21.6 km/h … 432 km/h
Environment Planned: "open" (low reflections) and "urban canyon" (high reflections) Tested: "open" (low reflections), 'suburb' (mid reflections), and "urban canyon" (high reflections)	

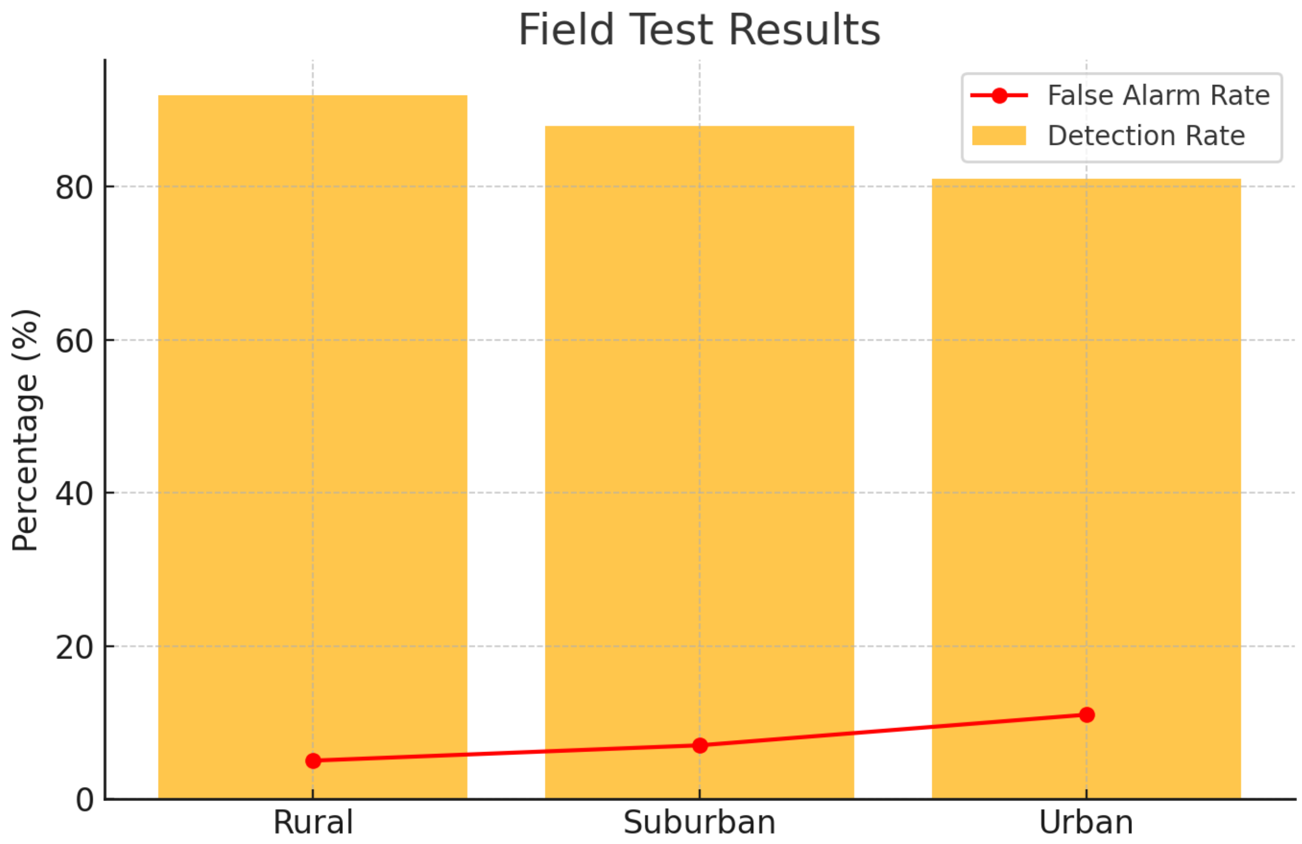
Environment	**Spoofer** (GPS)	**Spoofer location**	**Driving speed**	**SCS-GNSS-1 performance**		**Risk of false alarms**	**Fine tuning of the algorithm** (i.e. modifying the default thresholds)
				Detection rate	**False alarm rate**		
Rural / Open sky	HackRF One + 30 dB amp. + omnidir. ant	Road margin (Passing by 1..2 m)	**Up to 110 km/h**	> 95%	< 5 %	Low	Decision sensitivity can be significantly increased by lowering the alert decision threshold
Suburb	HackRF One + 30 dB amp. + omnidir. ant	3..5 m away from the road side. (Garden, balcony or window of a house.)	**Up to 45 km/h**	80-100%	< 20 %	Low /Mid	Default thresholds
					<10 %		slightly increased
Urban canyon	HackRF One + 30 dB amp. + omnidir. ant	Betw. high buildings, at ground level. (~ 20m from road and buildings)	**Up to 40 km/h**	~ 80 %	< 20 %	High	slightly increased
					<10 %		increased

DEMO VIDEO:

In vehicle at 110km/h speed

Spoofer detected on the roadside

Field test results in different environment



Summary of experiences

- Environment counts

  In urban canyon, the situation is very unpredictable, results are volatile, and hardly repeatable, *blind spots for missing detections* and *hot spots for fake alarms* are challenging phenomena.

- Power counts

  A typical low-cost, easily available spoofers (like maker-style SDR based spoofers just as the HackRF one) usually have low power to that makes the detection (but also the spoofing) difficult from a realistic, larger distance. Even relatively simple power amplifiers (e.g. 10..30 dB ones) significantly increase the coverage

- Trade-off between Sensitivity and False Alarms

  In all scenarios the fine tuning of the ‘sensitivity’ (that is, the decision making threshold) have been possible. It can be automatized based on the vehicle speed and location data.

Future outlook

https://navisp.esa.int/project/details/327/show
Interference Testbed
NAVISP-EL3-032

https://navisp.esa.int/project/details/261/show
OPEN LAB
NAVISP-EL3-027

CPRA Antenna

MIL-grade sensor

Invented, designed and

MADE IN EUROPE

Increased
European resilience
autonomy
in PNT

Dual PCBA w/ discret components

Multi-chip module

Integrated chip

CECIL

CECIL+

CECIL++

Summary

- Problem: GNSS spoofing which might be higher threat than jamming
- Mitigation: physical/antenna domain sensor
- Project: designed, manufactured, tested, validated and field demonstrated
- Further: mobile or static deployment and further developments

- Please contact:

Dr. Bertalan Eged, CEO

Sagax Communications, Ltd.

bertalan.eged@sagaxcommunications.com

www.linkedin.com/company/sagaxcommunications