GSTA: Final Presentation

18 December 2024

ESA Contract 4000131698

NAVISP2-HO-ORIGO-078-24

GSTA
GNSS
SMART TRACEABILITY
AND ANTI-SPOOFING

Introduction by the TO

- GNSS Smart Traceability and Anti-spoofing.
- The objective of this activity is to design and prototype a relatively simple HW that is able to provide a reliable position information and detect spoofing attacks.
- Motivation: threats to GNSS systems are pervasive in the modern society and systems are depends on PNT services. There are robust and complex techniques that can detect and mitigate Jamming and spoofing to GNSS signals.
- This activity look at a market sector that cannot afford complex and expensive solutions, yet it requires a guarantee PNT service.
- The GSTA project addresses these challenges by integrating multiple technologies: GNSS, ADS-B, and secure network-based timing synchronization into a portable/cheap HW that is able to detect and mitigate spoofing attacks, leveraging real-time, non-predictable data sources.

Who is Origosat

Introduction to the GSTA Project

Origosat has operating in the satellite PNT sector (positioning, navigation and timing) in the downstream segment.

Thanks to collaborations with ESA, European Space Agency, ASI, Italian Space Agency, INRiM (formerly Galileo Ferraris) and Links Foundation, our team has developed two patents in the Cybersecurity field of GNSS signals that mitigate threats of spoofing, jamming and meaconing.

Spoofing of satellite signals: an unresolved problem

- The spoofing of satellite signals:
  - Many spoofing events actually caused the shifting of the returned position by receivers;
  - Spoofing events also interfere with time measurement based on atomic clocks on satellites.
  - Spoofing of GNSS signals is adding risks to a wide range of applications, mostly unaware of this vulnerability;
- The availability of low-cost spoofing systems results in an underestimated risk, exposing any GNSS user to spoofing actions, especially since adequate countermeasures do not yet exist.
- **The object of the GSTA is to design, implement and demonstrate an innovative system able to support enhanced jamming, spoofing and meaconing detection.**
- The system concept has been applied to two different platforms, as follow:
  - Software Defined Radio and microcomputer – this configuration allows maximum design and implementation flexibility
  - Smartphones with ANDROID OS, through the use of GNSS RAW measurements provided by the OS

Intentional interfering attacks to GNSS

- The study of intentional interference and suitable countermeasures addresses the analysis of the likelihood, which encompasses:
  - complexity and cost of the attack
  - objectives and potential gain of the attacker
  - practical implementation constraints related to the target application
  - willingness of the final user to conduct self-spoofing
  - cost associated to the effective countermeasures
  - other aspects of non-technical nature
- Until a few years ago, a GNSS spoofing attack would require expensive, high-end equipment in the 50-500 k€ range (e.g. Spirent, IFEN, Rohde Schwarz, Spectracom, etc.)
- Today, SDR and open source software allow anyone to spoof for 5-400 €

	Cost at the attacker side		
Attacks	**Developing or buying the HW**	**Required expertise**	**Complexity of operation**
Jamming	VL	L	VL
Meaconing	VL	M	VL
Meaconing with variable delay	L	M	L
Meaconing with modem	L	M	M
Simplistic spoofing (custom low-cost HW)	L	H	M
Simplistic spoofing (HW simulator)	H	M	M
Intermediate self-spoofing	M	H	M
Intermediate spoofing	M	H	H
SCER – security code estimation and replay	M	VH	H
Meaconing/spoofing with high gain antennas	VH	H	H
Nulling attack	M	VH	VH
Sophisticated spoofing	VH	VH	VH

VH: very high – H: high – M: medium – L: low – VL: very low

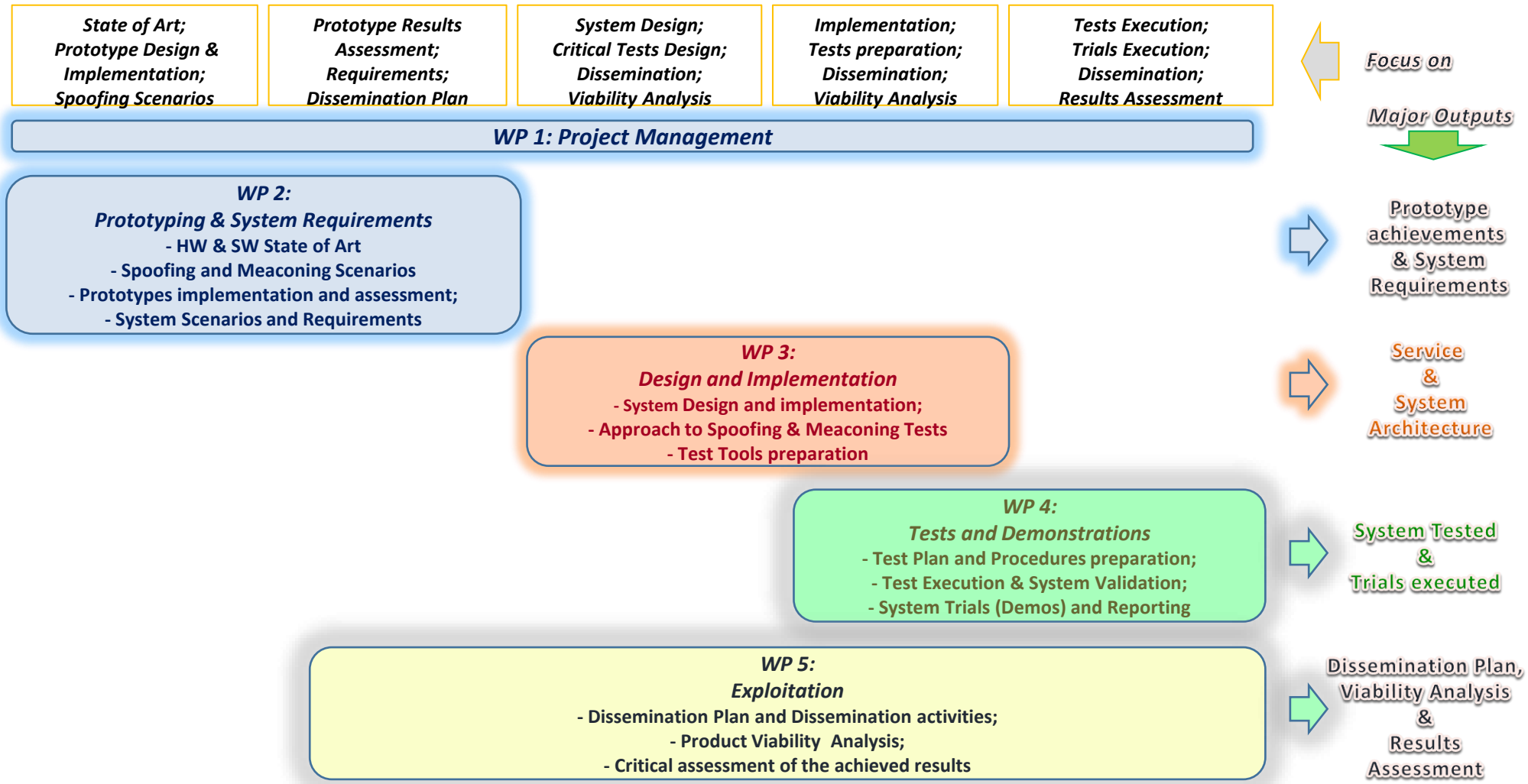
These facts provide a strong selling point for meaconing and spoofing protection services, demonstrating that spoofing is no more a diversion for GNSS engineers, but a real fact that can enable illicit behaviors or even put human life in danger

System's concept

- The system architecture is based on a set of Hybrid GNSS Receivers (HGRs) connected to a server which performs data consolidation and distribution. The system exploits the use of three sources of information, as follows:
  - **The GNSS, for continuous, accurate and worldwide available timing and positioning services**;
  - **The ADS-B, as source of a priori unknown messages** in terms of **content**, signal **characteristics** (e.g. the actual bits of the message) and emission **time**. By design, in fact, ADS-B messages are transmitted by each airplane at random times, in order to avoid message conflicts in accessing the shared ALOHA channel at 1090 MHz (ADS-B is based on a pure ALOHA access);
  - **A secure synchronisation mechanism based on a communication network**, to provide alternative timing through a secure channel.

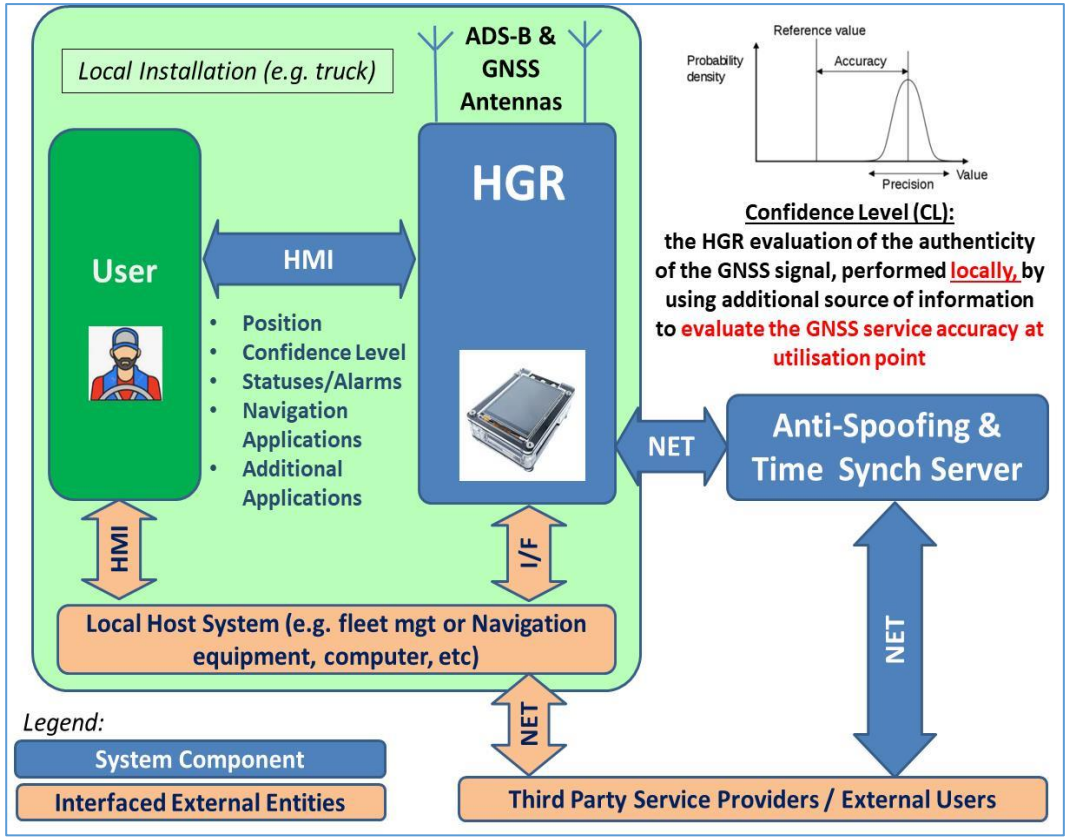
The unique combination of the three elements above, or part of them when not all contemporary available, provides capabilities to detect the most likely spoofing attacks, i.e. those based on "signal retransmission" (meaconing) and even those based on "signal simulation".

Study Logic


State of Art;
Prototype Design & Implementation;
Spoofing Scenarios
Prototype Results Assessment;
Requirements;
Dissemination Plan
System Design;
Critical Tests Design;
Dissemination;
Viability Analysis
Implementation;
Tests preparation;
Dissemination;
Viability Analysis
Tests Execution;
Trials Execution;
Dissemination;
Results Assessment
Focus on
Major Outputs
WP 1: Project Management
WP 2:
Prototyping & System Requirements
- HW & SW State of Art
- Spoofing and Meaconing Scenarios
- Prototypes implementation and assessment;
- System Scenarios and Requirements
Prototype achievements & System Requirements
WP 3:
Design and Implementation
- System Design and implementation;
- Approach to Spoofing & Meaconing Tests
- Test Tools preparation
Service & System Architecture
WP 4:
Tests and Demonstrations
- Test Plan and Procedures preparation;
- Test Execution & System Validation;
- System Trials (Demos) and Reporting
System Tested & Trials executed
WP 5:
Exploitation
- Dissemination Plan and Dissemination activities;
- Product Viability Analysis;
- Critical assessment of the achieved results
Dissemination Plan, Viability Analysis & Results Assessment

System design

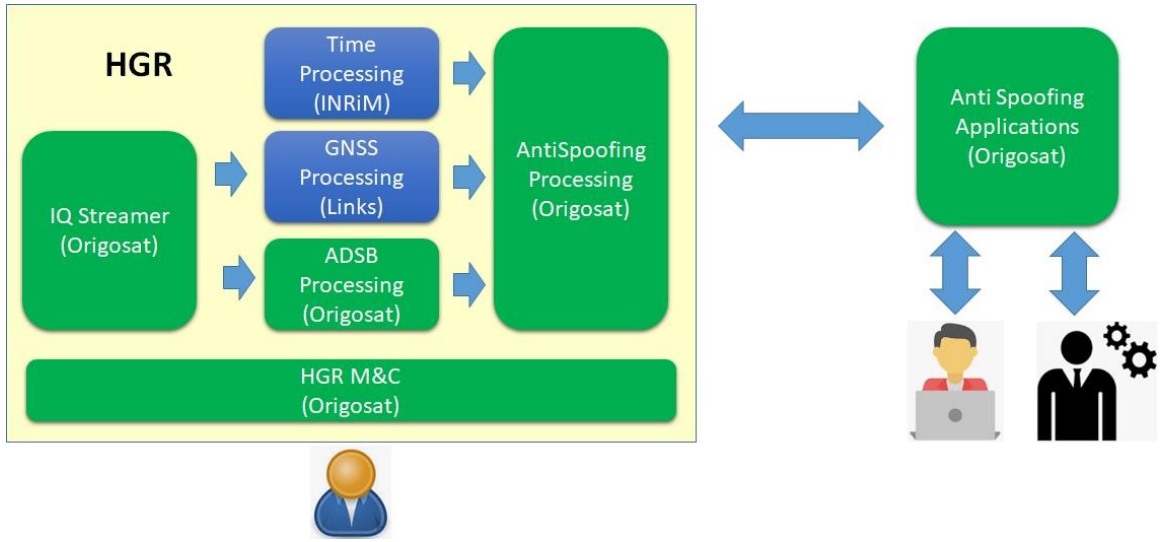
- The system is composed by a set of Hybrid GNSS Receivers (HGRs), in its various configurations and operational modes, connected to a service center.
- The HGR provides Position Velocity and Time information to users and to the server. The HGR has two major configurations, as follows
  - The **HGR "basic"** (RSPduo and Raspberry Pi4)
  - The **HGR "+"** which is based is a customised Pi4 where the quartz has been replaced with an external Local Oscillator which is also connected to the RSPduo SDR-FE
- The Anti-Spoofing Application Server (ASAS) provides the services as well as valuable information to authorised users



The system provides the LOCAL evaluation of the authenticity of the GNSS signal, as well as the confidence level on the GNSS information provided by constellations

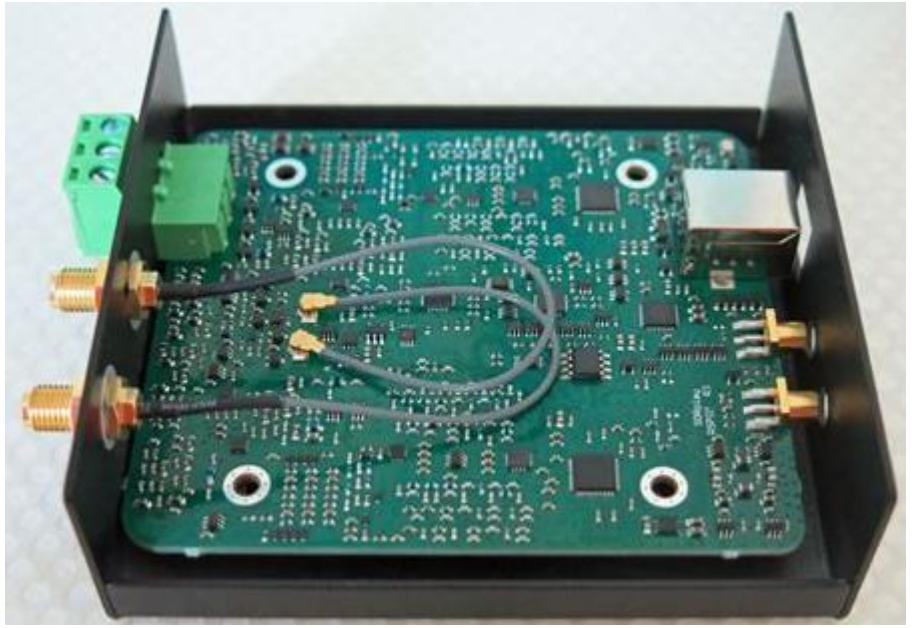
HGR Design

- The HGR is based on SW Defined Radio (RSPDuo SDR) and SBC (Raspberry Pi4) technologies and is composed by:
  - An IQ streamer, in charhge of collecting the samples from the dual channel SDR
  - a GNSS Processor
  - a Time Processor
  - an ADS-B Processor
  - An Anti-Spoofing Processor



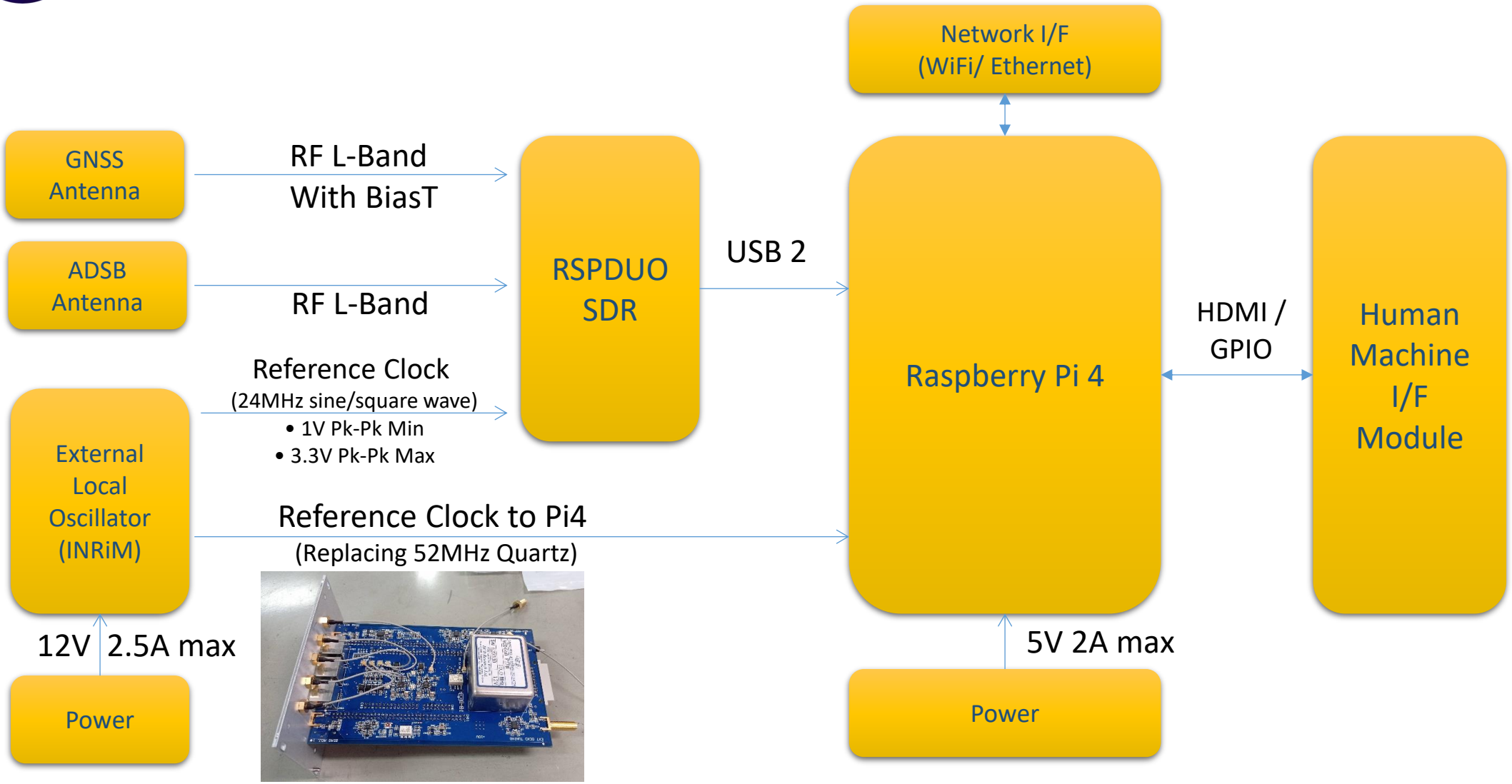
SDR selection: RSPduo

- The HGR is based on the **RSPduo SDR** which offers, at reasonable cost, synchronous dual channel acquisitions at GNSS L1 and at ADS-B bands.
- The HGR based implements the following alternative modes of operation, which are SW selectable:
  - **Single tuner at GNSS L1** frequency (6 MSPS – 12 bits) for GNSS processing, including **GALILEO OSNMA services**
  - **Dual tuner synchronous at GNSS L1 and ADS-B frequencies** (2 x 2MSPS I&Q stream), for the dual channel HGR receiver; the dual channel mode suffers of limited performances due to the BW provided by the RSPduo (1.536 MHz in dual mode)



Despite the limitation of the device, selected to meet cost requirements, the system works with GPS, Galileo and ADS-B in parallel, including OSNMA

HGR Design – Physical view



OCXO Oscillator for HGR+

HCD660

High Performance OCXO with Sine Output and European pin-out

- Temperature stability down to 1ppb
- Single 12V supply (12V ~ 30V optional)
- Standard European pin-out
- Custom options available

OL: OCXO QUARTZ

52 MHz

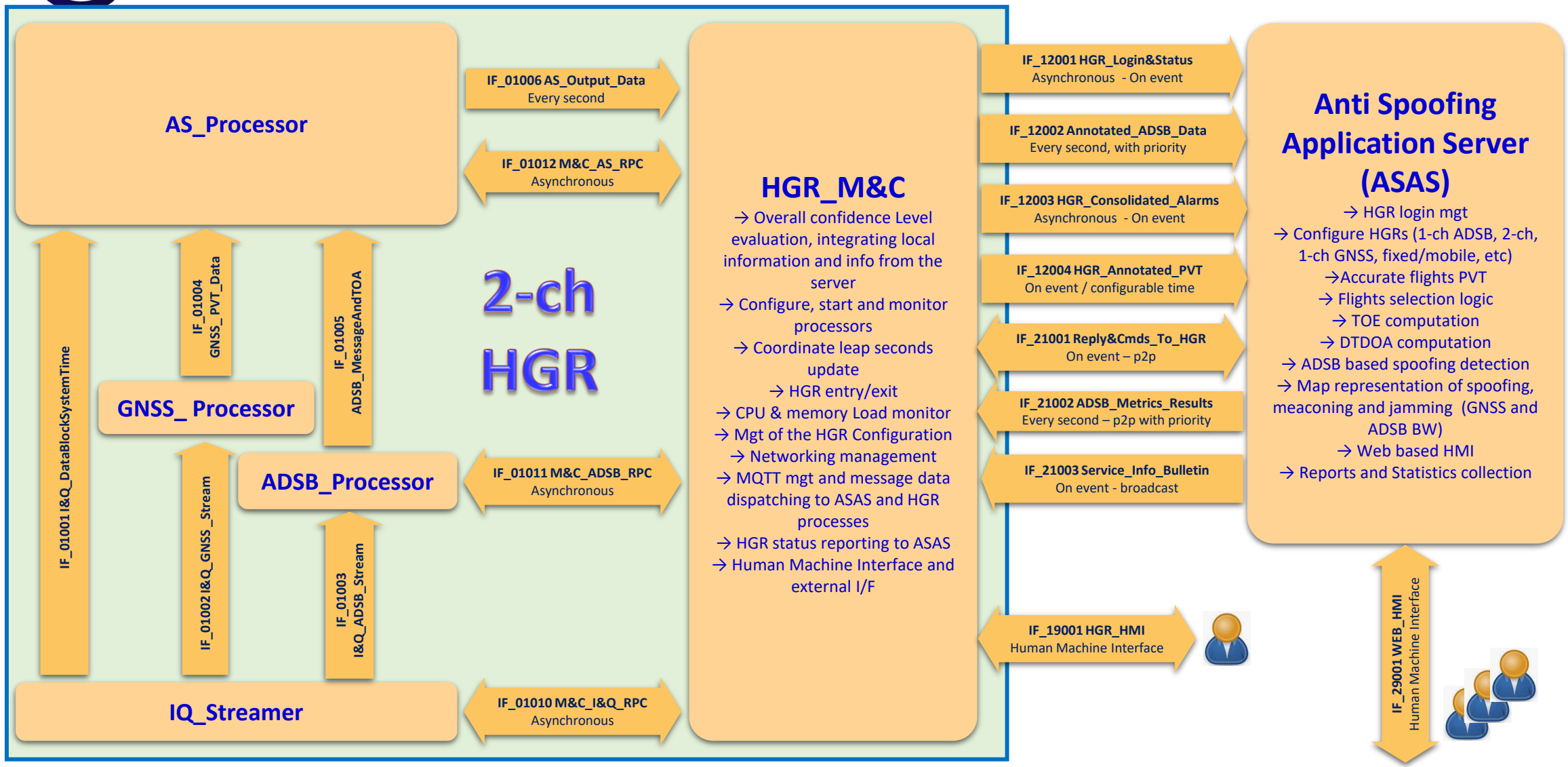
SBC: Raspberry Pi4

24 MHz

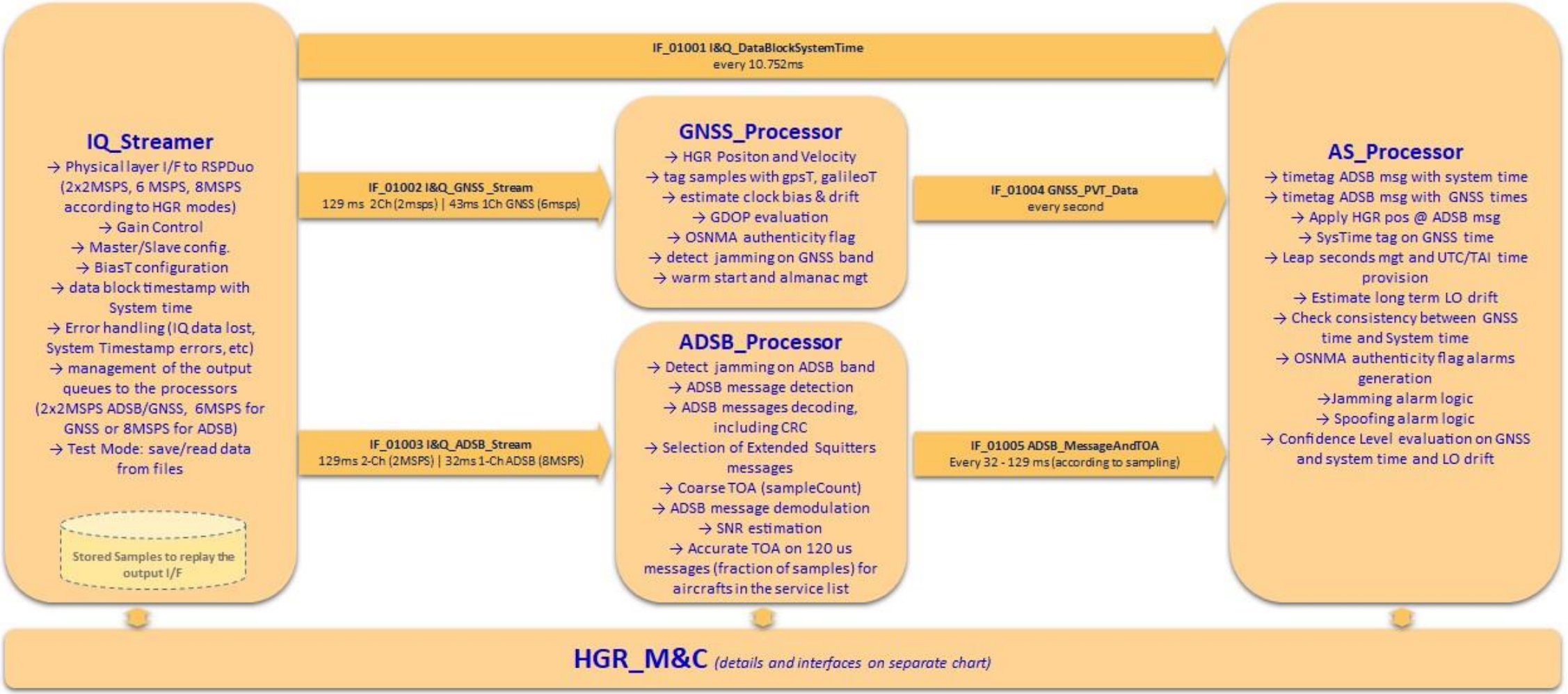
SDR - Front End: RSPDuo

- The OL is a OCXO Quartz @10 MHz
- It is the local reference
- From the OL, generation of 24 MHz, for RSPDuo
- From the OL, generation of 52 MHz, for SBC Raspberry Pi4
- NTP Chrony release on R-Pi4

GSTA Interfaces Summary



HGR SW Components and major HGR internal interfaces



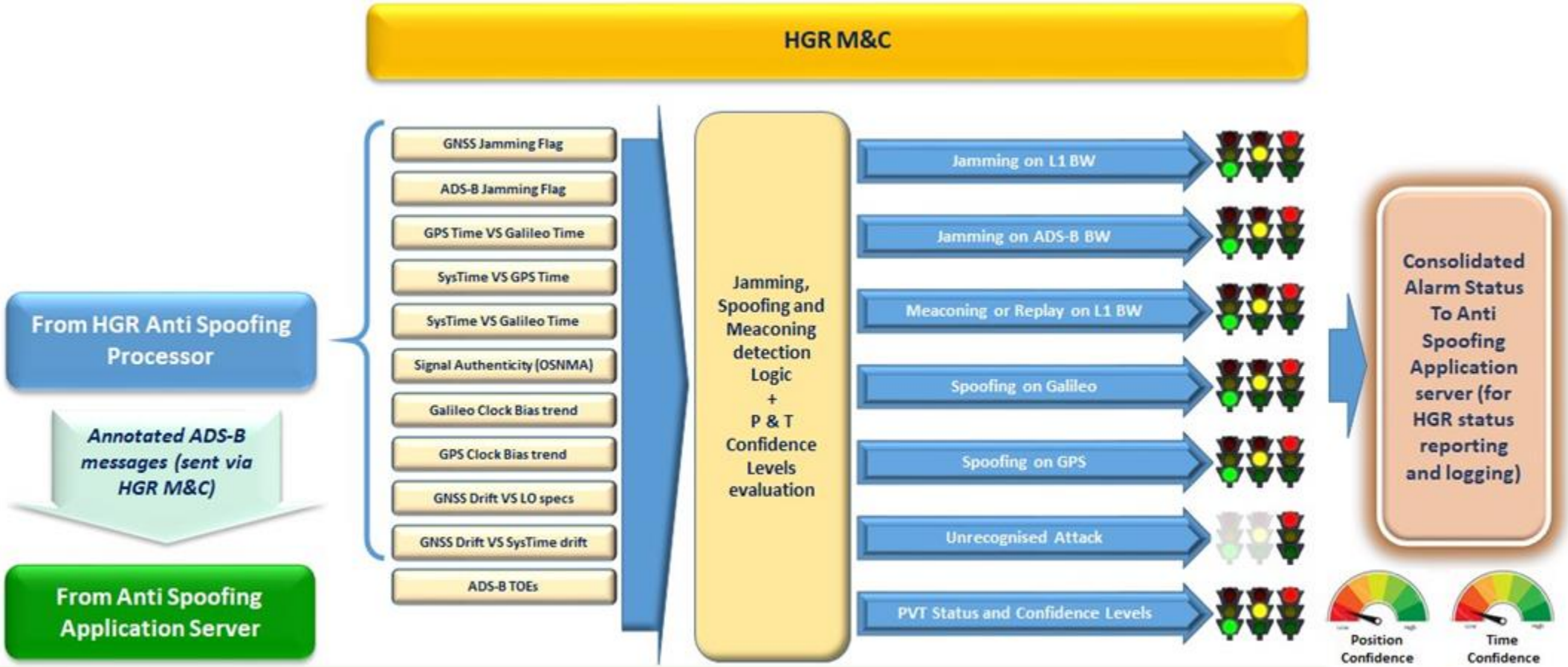
HGR for mobile applications

- The HGR support a very easy installation and use:
  - car lighter socket 12V
  - Automatic power-on (when connected to lighter)
  - No buttons
  - The HGR is fully autonomous, also for networking (LTE)
- The packaging includes LEDs (automatically commanded by the HGR SW in the raspberry Pi4) used to report to the user the status of the main topics, as follows:
  - RUN (green LED): flash during boot, fixed when HGR is ready and operational
  - GNSS / ADS-B (yellow LED): flash when GNSS fix are available, fixed when also ADS-B data is received
  - NETWORK (blue LED): fixed when LTE network is available, flash when TX/RX packets from/to the server
  - ERROR (red LED): different flash sequences to notify attacks

HGR for fixed installations

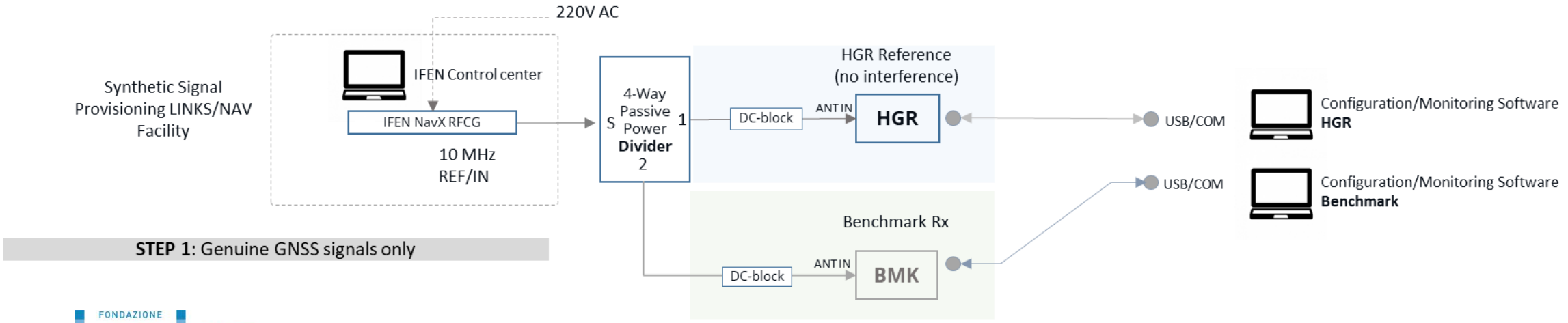
- A specific boxing has been prepared to support fixed installation, including
  - Waterproof boxing
  - DC power supply and switch
  - Antenna connectivity
  - Network connectivity

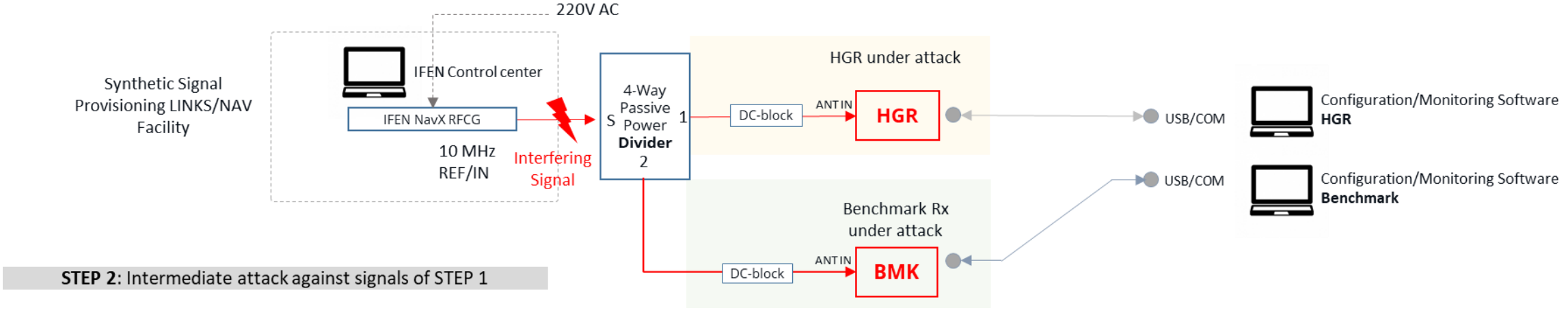
Anti Spoofing logic summary



The system implements a quite complex decision logic and leverages the features provided by the available information sources

Intermediate spoofing





System tests

- The system passed all the tests, detecting all the types of attacks generated in laboratory. An example of test result is shown in the following figure, where a signal generator force a generic GNSS receiver to report erroneous position. The system immediately detects the anomaly and report a red flag

The system has been tested in several attack conditions, including intermediate spoofing where the signal emulates position or time shift [in the range 1-5 ns/sec] on the GNSS fix

1. the GNSS signal generator alters the position estimation through the counterfeit signal

The position is moved according to the spoofing scenario (red marker shows attack detection)

Intermediate spoofing detected

10-day demonstration

TECHNOLOGICAL LEADER IN OPERATING MACHINES

Merlo is a family-run industrial group that designs, produces and markets its own products under the “Merlo” and “TreEmme” brands. People are at the centre of the project; the Merlo Group is committed to respecting the environment and making the work of the operator (and everyone who is passionately dedicated to constantly improving the efficiency and performance of its products) more functional, safe and comfortable.

Annual Revenue > 420 Ml €

People > 1400

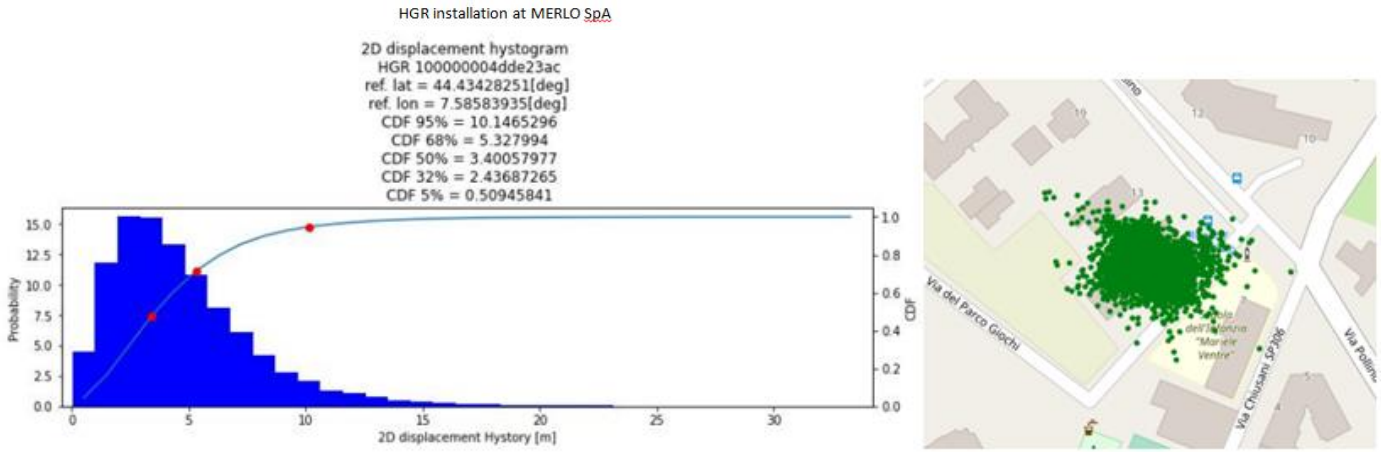
The system has been demonstrated on field with different configurations and use

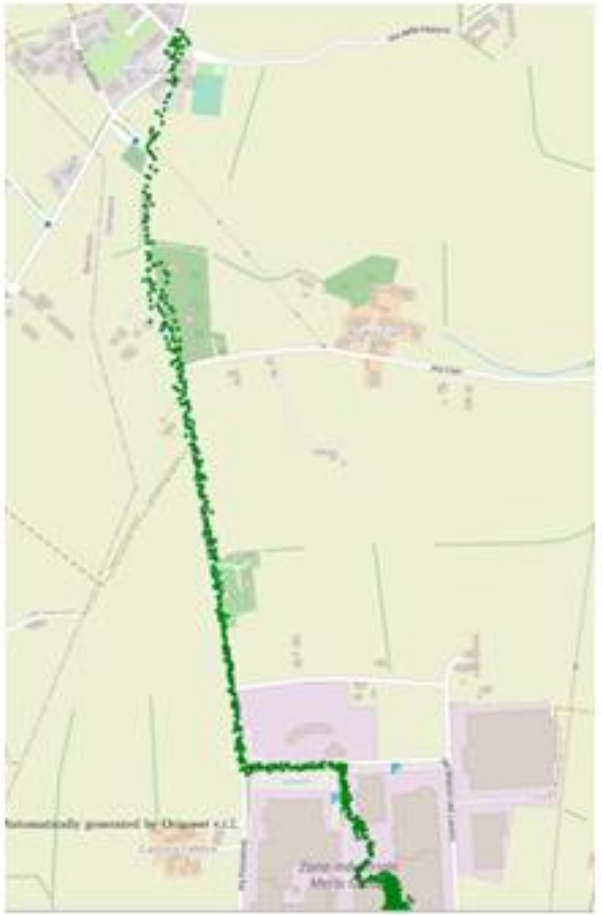
https://www.merlo.com/

10-day Demonstration







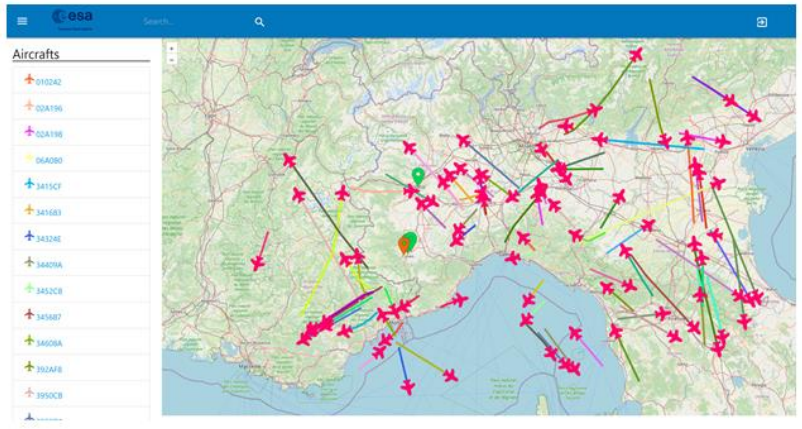


Typical HGR demo in mobility

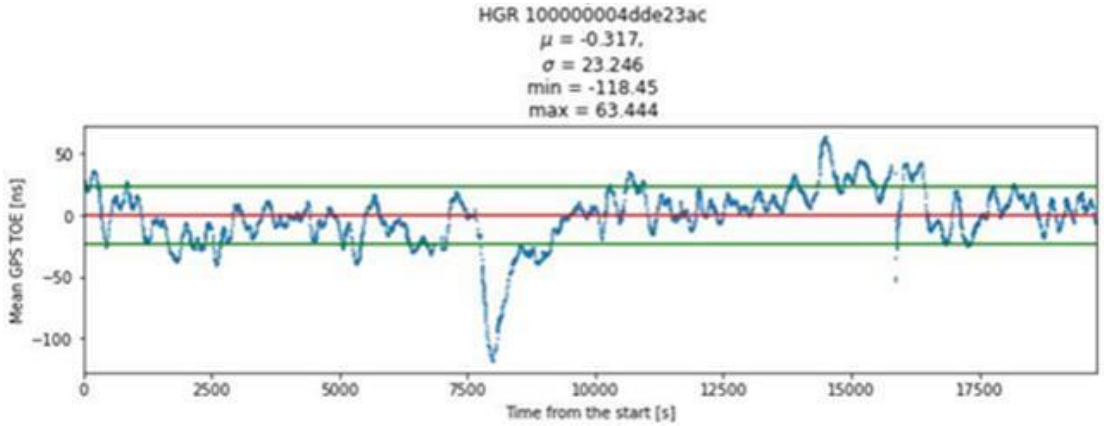
Despite the limited BW for GNSS and for ADS-B (1.56MHz), the HGR showed reasonable accuracy for the application

10 day demo: ADS-B processing for dual channel HGR

- The ADSB processing for the HGR resulted in a continuous processing of ADS-B data supporting the evaluation of two metrics:
  - **Mean TOE metrics** demonstrated to be very stable and shows high sensitivity to potential spoofing and meaconing attacks. **A few ns delay on the GPS/GALILEO signals w.r.t. the authentic signal can be detected as depicted in the following chart**.
  - **StDev TOE metrics** is very sensitive to **position displacement**, independently on the time offset which is potentially caused by an attack. The metric, with the HGR configuration (2MSPS dual channel), is sensitive to **100ns** approximately, which is equivalent to **30m displacement**



Typical ADSB coverage with the daily HGR configuration

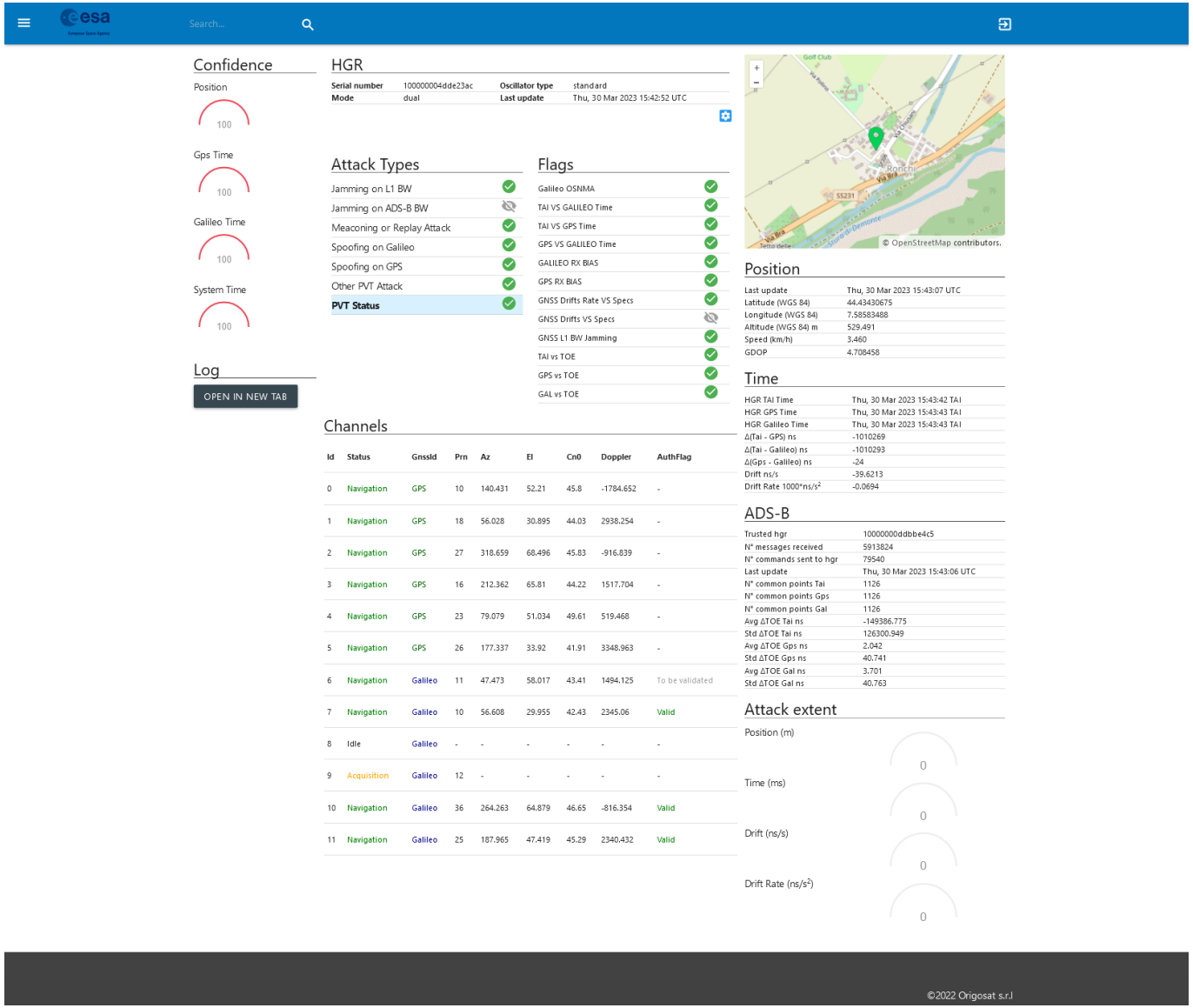


The conceived metrics allows to discriminate attacks on the position, on the time and time drift, evaluating their intensity (meters , ns and ns/s)

Web server

- The system provides significant information such as:
  - **General information** of the HGR device
  - The **alarm flags**
  - The **attack types**
  - **OSNMA information** on a single GALILEO satellite and overall
  - The **Position and Time information**, also provided with a map view
  - The **attack intensity** information
  - The **level of confidence** on the information provided (position and times).
  - The information of the **status of the channels of the GNSS processor**

The system provides significant results to detect and quantify the effects of attacks to GNSS



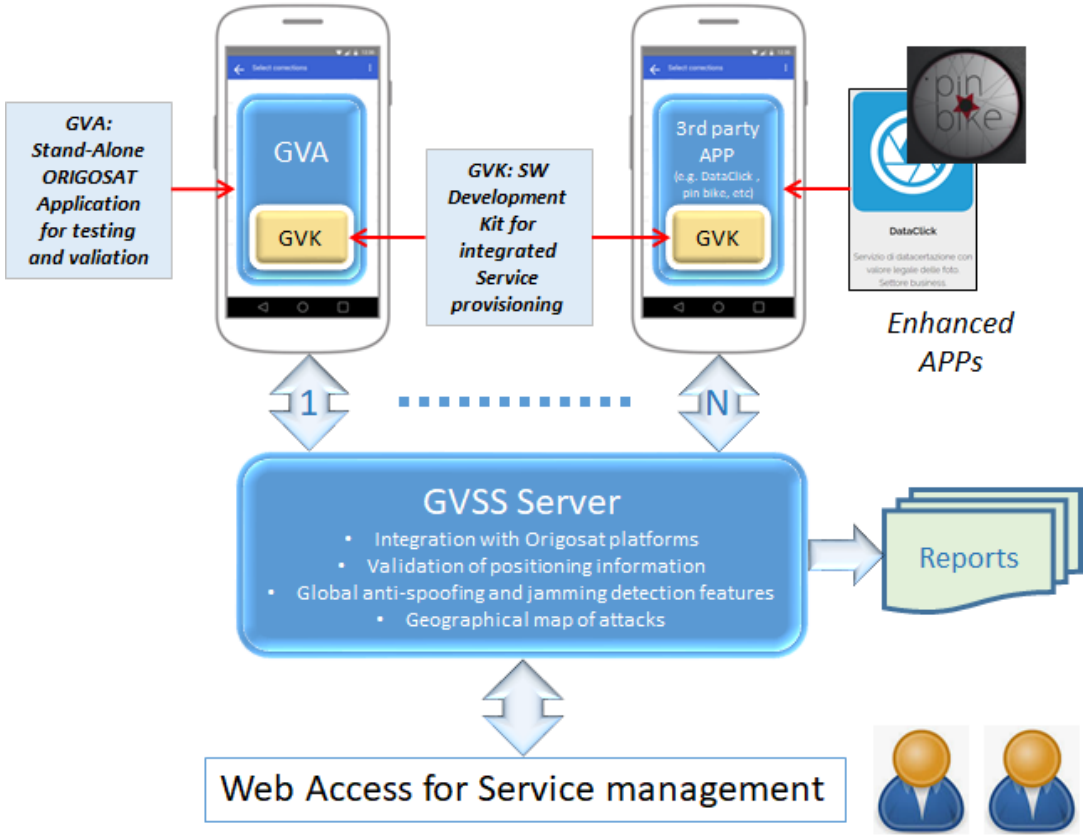
Application for ANDROID smartphones

- The **GNSS Anti-Spoofing and Anti-Counterfeiting System for smartphones (GASACS)** implements several countermeasures to detect, and when possible survive, to P&T attacks. The solutions implemented are partially derived from the algorithms conceived for the HGR, namely:
  - Processing of GPS and GALILEO raw measurements on the L1/E1 band, made available from the ANDROID API (GNSS RAW MEASUREMENTS). The system's concept includes the usage of corrections provided by a set of reference GNSS receivers
  - Take advantage from an independent timing source in order to detect spoofing and/or meaconing attacks. The timing source is integrated with the internal clock, with a solution similar to the one conceived and implemented in the GSTA HGR

A subset of the GSTA project findings has been applied to ANDROID smartphones , tailored for the different platform to which are applied

System architecture to support ANDROID smartphones

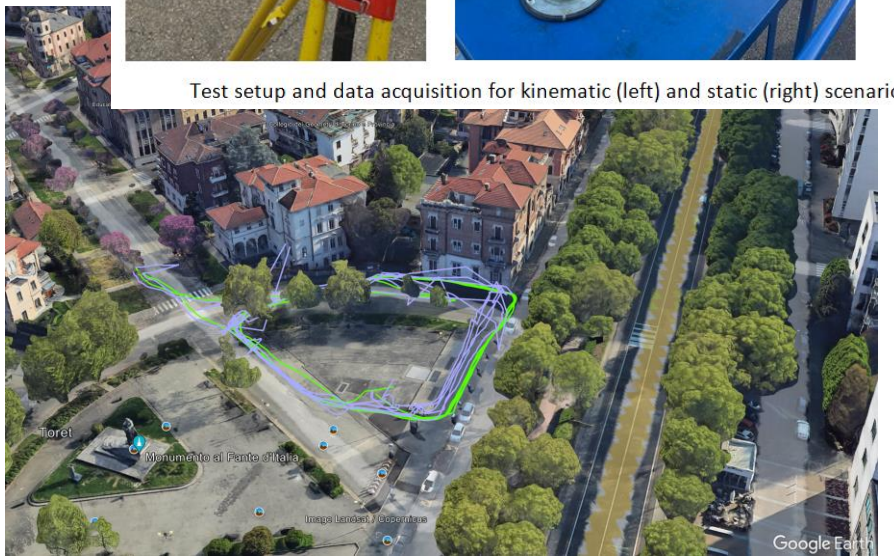
- The **GNSS Validator Software Development Kit (GVK)** is the ANDROID compatible kit suitable for integration with third party APPs. Well documented interfaces will be defined in the frame of the study. The GVK interacts with the GNSS chip (e.g. GNSS RAW MEASUREMENTS) via APIs provided by ANDROID OS and supports full integration of the Anti Spoofing functionalities in the cooperating APP.
- The **GNSS Validator App (GVA)** aims at supporting system tests and validation. The GVA implements the interfaces to the GVK, i.e. using the same interfaces and paradigm of the integration of a third party APP on ANDROID
- **GNSS Validator Server SW (GVSS)**, the server SW supporting the service provisioning and the position and time validation workflow



Tests

- The measurement campaign was held in Turin, in a public area in front of Politecnico di Torino University.
- The campaign was performed by considering two different operational scenarios:
  - Static GNSS acquisition in open-sky condition
  - Kinematic GNSS acquisition seamlessly moving from open-sky to partially covered condition
- For both scenarios, the GASACS system, implemented as an Android app in several new-generation smartphones, has acquired dual-frequency signals from all the visible constellations in a 30-minute-long acquisition campaign.

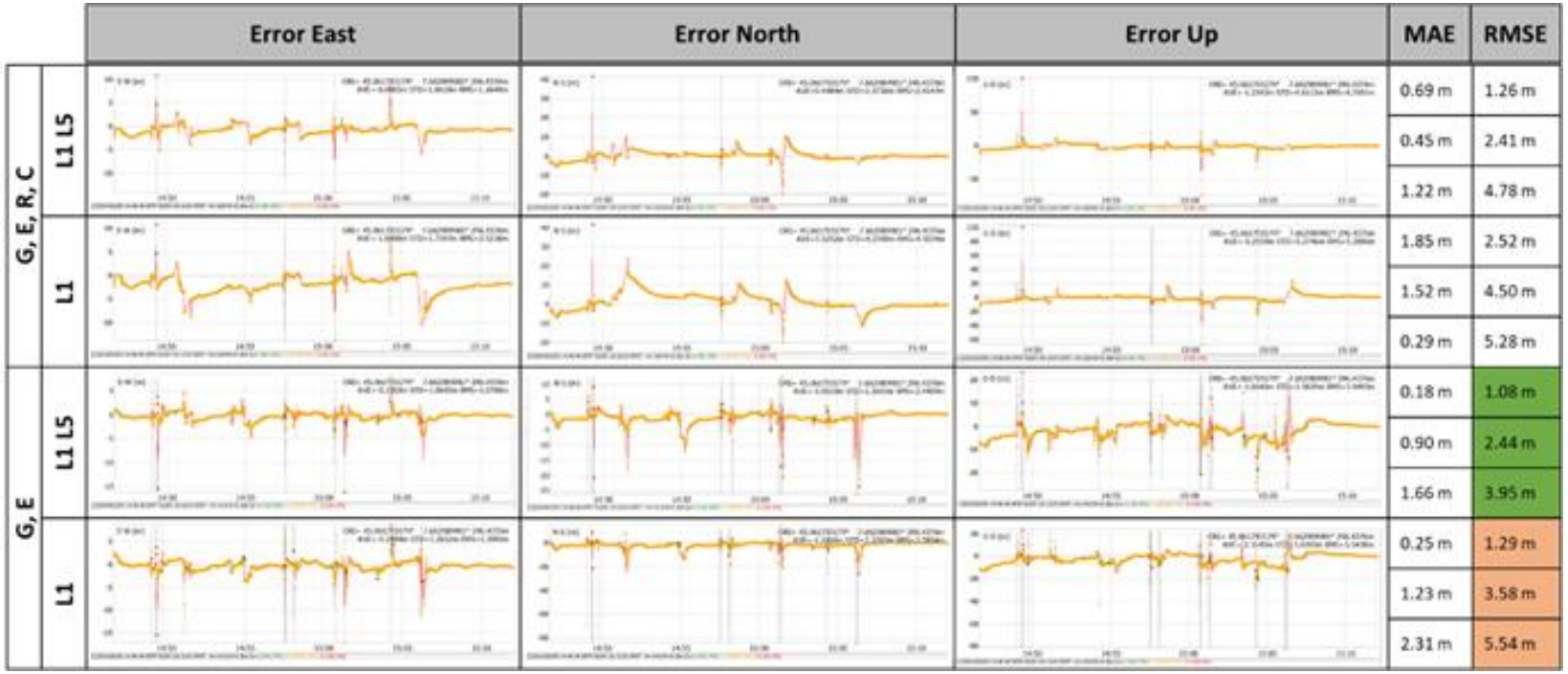
Test setup and data acquisition for kinematic (left) and static (right) scenarios



Tests on the application have been performed with comprehensive test set-up, and showed very good results

Accuracy

- The overall accuracy is higher in the GPS+GAL case
- It is observed that there are many more 'spikes' in this solution compared to the solution with all the constellations (GPS+Glonass+GAL+BeiDou).
- Such spikes, are due to the combined effect of DOP and satellite visibility



		Error East	Error North	Error Up	MAE	RMSE
G, E, R, C	L1 L5				0.69 m	1.26 m
					0.45 m	2.41 m
					1.22 m	4.78 m
	L1				1.85 m	2.52 m
					1.52 m	4.50 m
					0.29 m	5.28 m
G, E	L1 L5				0.18 m	1.08 m
					0.90 m	2.44 m
					1.66 m	3.95 m
	L1				0.25 m	1.29 m
					1.23 m	3.58 m
					2.31 m	5.54 m

It is possible to conclude that the GASAC system, implemented in commercial smartphones, has the capability to estimate metric or sub-meter level accurate positioning in both kinematic and static acquisition, as well as in challenging situations like urban areas.