Type of project - Type an X in the right hand column (select one only)	
Kick start	X
Feasibility study	
Demonstration project	
Demonstration from Feasibility study	

Theme - Type an X in the right hand column (select only those which truly apply)	
Aviation	
Health	
Infrastructure & smart cities	
Media, culture & sport	
Transport & Logistics	X
Safety & security	
Energy	
Education & Training	
Food & Agriculture	
Finance, Investment & Insurance	
Tourism	
Environment, wildlife & natural resources	
Maritime & Aquatic	

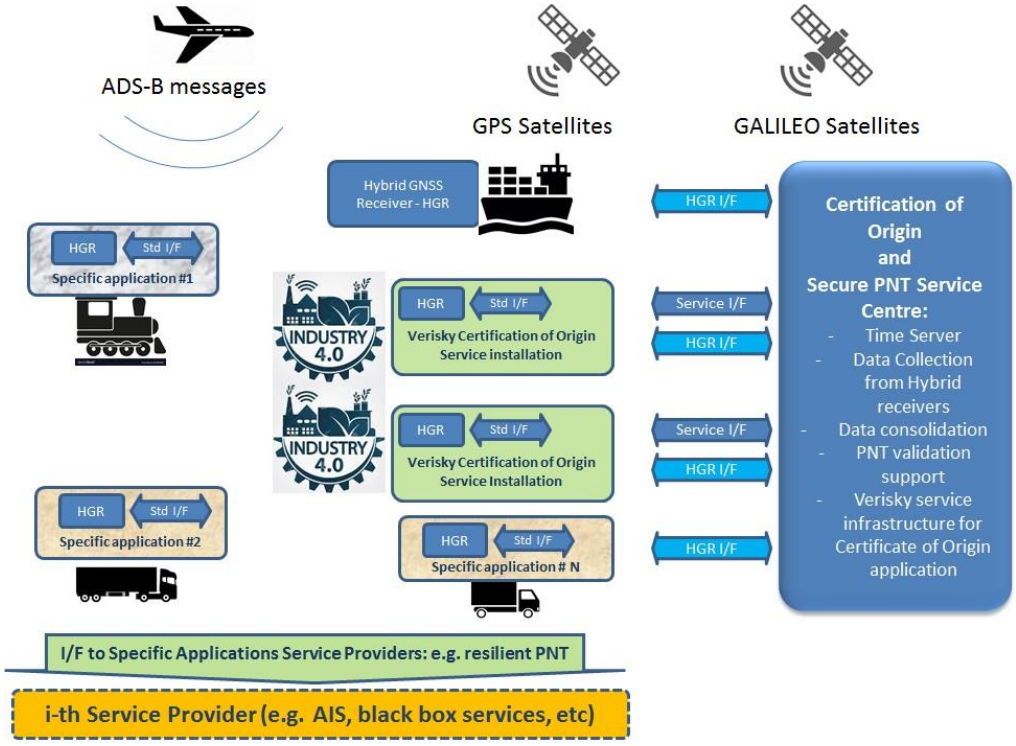
Space Assets - Type an X in the right hand column (select those that are used)	
Satellite communications	
Satellite navigation	X
Earth Observation	
Satellite AIS	
Human spaceflight technologies	

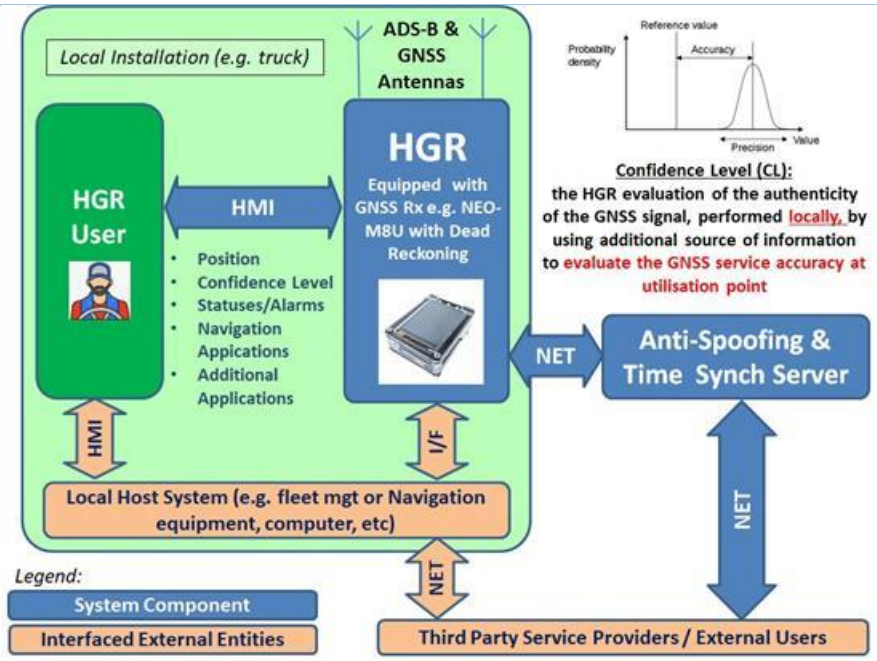
→PROJECT WEB PAGE TEMPLATE

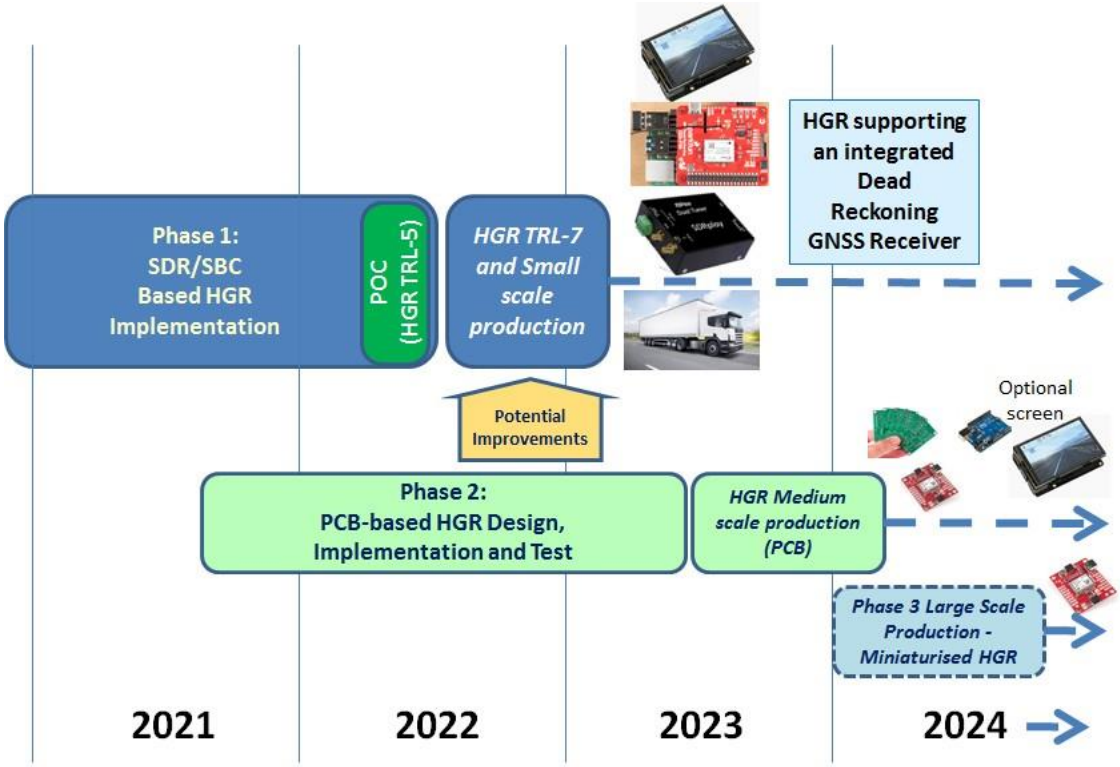
Header Information	
Project short name	HGR
Project full name	Hybrid GNSS Receiver
Project logo	
Teaser	The project designed a hybrid GNSS receiver (HGR). The HGR provides innovative time and position certification services for smart transportation applications. HGR has the ability to detect spoofing and meaconing attacks, therefore validating the authenticity of the location-related data. The HGR combines GALILEO OSNMA service, ADS-B data from aircrafts and Network timing information

Project web page	
Objectives of the service	 The HGR receiver and its technology is an economic solution that integrates various sources of information ensuring accuracy, sturdiness and precision that currently no other receiver can provide. The key driver for HGR application class is the ability to detect spoofing and meaconing, therefore determining the authenticity of the location-related data. 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".**
Users and their needs	The target user can be resumed in three different categories: 1. Consortia and logistics and transport companies 2. Industries producing Black Boxes and GNSS Receivers. 3. ISVAP (Institute for the supervision of private and collective interest insurance) and some insurance companies, always in the capacity of stakeholders. The users engagement envisaged in the project are 4 transport and logistics companies. Through interview and questionaries' it seems an important security insight emerged about special on road transport categories (i.e. electronics, jewellery, money transport etc). In reality there seems no great interest in solving these illegal activities because they make transport regulations less rigid by the sector's operators. In any case, to monitor the transports in real time, the means are often

	connected via geolocation services that exploit GPS signals and web connectivity despite there being signal interruption problems.
	
	The relevant applications and user needs for Road Domain:
	
	• **Safety-Critical Applications (SCA)**
	  ○ Fleet Management – enhanced (HMT)
	• **Payment-Critical Applications (PCA)**
	  ○ Location-based charging (RUC)
	  ○ Pay-As-You-Drive
	• **Regulatory-Critical Applications** (RCA)
	  ○ Emergency Services – eCall
	  ○ Road Navigation – supporting emergency
	  ○ Vehicle Tracking – DT
	• **Smart Mobility Applications (SMA)**
	  ○ Road Navigation
	  ○ Fleet, asset and freight monitoring

Service/system concept	The key driver for HGR application class is the ability to detect spoofing and meaconing, therefore determining the authenticity of the location-related data. The system concept is to acquire the same signals from different sites by means of collaborative receivers and/or reference receivers managed by the service owner. Every receiver, knowing its **presumed position by using GNSS**, is able to infer the emission time of a message, which can be compared with the similar evaluation made from all receivers who decoded the same message. At this point, the system is able to verify the trueness of the presumed position of each receiver by using a voting mechanism (with reference receivers having very large weight in the evaluation). The comparison with GNSS derived position shall allow to validate and to certify GNSS positioning against spoofing. The proposed architecture considers the possibility to interoperate with Service Providers already supporting the Transportation Chains (e.g. fleet management systems).  The HGR will provide two sets of information, as described below: • The position, as any GNSS receiver (e.g. using NMEA protocol) • The level of confidence associated to the information reported, including alarms when a spoofing, meaconing or jamming attack is detected, e.g. extending the NMEA protocol.

	 The system is composed by: • A set of HGR equipment, installed on the transportation platforms for rail, road and maritime smart transportation (respectively on trains, trucks or vessels) • The Anti-spoofing and the time synch server(s) to manage the systems and services
Space added value	The proposed application/service takes advantage of GNSS signals, especially **Galileo**, the Europe's own global navigation satellite system. Currently providing Initial Service, Galileo is designed to be interoperable with GPS and GLONASS, the US and Russian GNSSs. In detail, Galileo is introducing a new service, referred to as Open Service Navigation Message Authentication (**OSNMA**), designed to be disseminated over the E1 band. This functionality contributes significantly to mitigate the simplest forms of spoofing attacks, which are also the most likely. Whereas GNSS remains the principal mean for positioning, especially in outdoor scenarios, highlight risks related to GNSS spoofing and jamming. The HGR is based on the exploitation of a patented anti-spoofing algorithm based on the integration of data coming from three different sources of information: positioning technology (GNSS), Signals of Opportunity (SoO) (ADS-B) and a satellite-independent timing source. This unique combination of the three elements above, or part of them when not all simultaneously available, provides capabilities to detect the most likely spoofing attacks, i.e., those based on "signal retransmission" (meaconing) and those based on "signal simulation". Such a combination grants benefits against intentional spoofing attempts.
Current status	



The HGR development status in March 2021 is the following:

- Consolidated user requirements
- Consolidated HGR design baseline
- Started HGR prototyping activities with the support of strategical partners: LINKS Foundation, a research centre, and INRiM, a public research centre and Italy's national metrology institute (NMI)
- Started simulations to determine expected performance. Initial results shows very good performances, in line with the requirements, achieved with margin
- Prototype results are consolidated within June 2021
- Implementation is planned to be completed by spring 2022
- Proof Of Concept with installations on vehicles are scheduled, using the implemented system, in Summer 2022. The POC are organised with the involvement of target users and stakeholders

Please continue to the page below ↓

→PROJECT WEB PAGE TEMPLATE

Prime Contractor	
Logo	
Company Name	ORIGOSAT S.r.L
Country	Italy
Website URL	http://www.origosat.com/

Sub Contractor 1	
Logo	
Company Name	Fondazione LINKS Leading Innovation & Knowledge for Society
Country	Italy
Website URL	https://linksfoundation.com/

Project Managers		
	Contractor project manager	ESA project manager
Name	Ibrahim Osmani	Christopher Frost-Tesfaye
Postal Address	*Corso Barolo 47* *12051 Alba (CN)* Italy	Fermi Avenue, Harwell Science & Innovation Campus Didcot, Oxfordshire OX11 0FD, United Kingdom
Email	ibrahim.osmani@origosat.com	Christopher.Frost-Tesfaye@esa.int
Phone	+39 349 2353244	+44 (0) 12354 44 316

Realated links – links to your product web page, news items or to ESA feasibility or Demo Project			
Title	Origosat WEB Page	URL	http://www.origosat.com/