



# Contribución de Galileo y SBAS a autenticación e integridad en los servicios de posicionamiento y navegación

*Prof. Dr. Manuel Lopez,  
Sr. Market Development Technology Officer*



# IMO warns against deliberate GPS, GNSS interference – MSC.1/Circ.1644 (Oct'21)



The Maritime Safety Committee noted that the deliberate interference with satellite navigation system signals poses a substantial risk to the safety of navigation, the safety of life and property, and the protection of the marine environment.

The Committee urged Member States to:

1. take actions necessary to minimize interference coming from their territory, as required under the International Telecommunication Union Radio Regulations;
2. consider **issuing warning notices or advisories to mariners** specifying the time periods and areas impacted by any known interferences to minimize negative effects upon maritime operations; and
3. consider enacting measures that prevent unauthorized transmissions on recognized satellite navigation system frequencies.

# European GNSS enable new applications and resilient Maritime Navigation

## Availability

Enhanced **performance** in challenging environments, thanks to more satellites in view

## Accuracy

Increased **accuracy** thanks to Dual Frequency and High Accuracy Service

## Integrity

## Authentication

Increased **safety and security** thanks to contribution to integrity provided by EGNOS and Galileo Authentication



Contribution to resilient position for vessels monitoring, e.g. fishing and merchant vessels

# Outline

- Galileo Open Service – Navigation Message Authentication (**OS-NMA**)
- **SBAS** contribution to integrity

# Galileo is the European GNSS offering a wide range of services



## Open Service (OS)

Galileo open and free of charge service set up for positioning and timing services. It is plan to deliver navigation message authentication (OS-NMA, 2023).

## Search and Rescue Service (SAR)



Europe's contribution to COSPAS-SARSAT, an international satellite-based search and rescue distress alert detection system



## High Accuracy Service (HAS)

A service complementing the OS by providing an additional navigation signal and added-value services in a different frequency band. The HAS signal can be encrypted in order to control the access to the Galileo HAS services (HAS, 2023)

## Public Regulated Service (PRS)



Service restricted to government-authorized users, for sensitive applications that require a high level of service continuity

Galileo was recognised by IMO in 2016 as part of the World Wide Radionavigation System, allowing for its use in Merchant Shipping (IMO SN.1/Circ.334)

# Galileo Navigation Message Authentication (OS NMA)



## GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA)

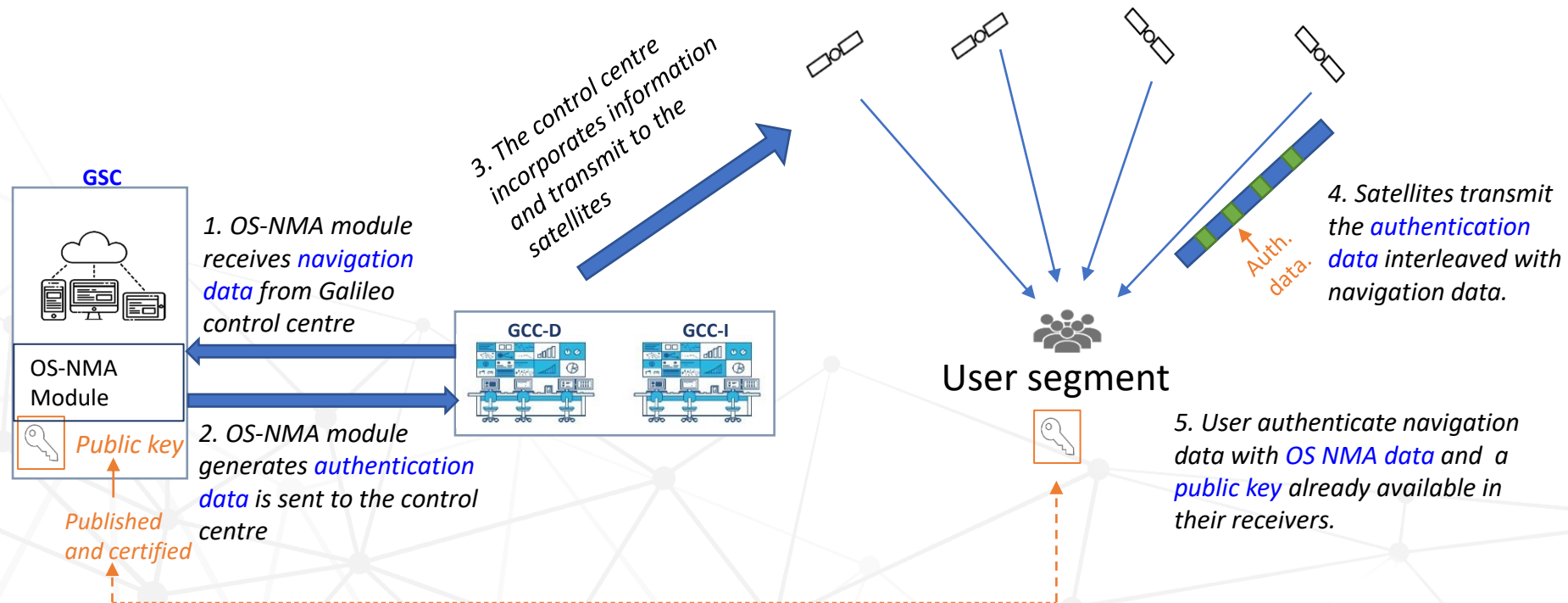
INFO NOTE

- Galileo OS NMA is a new public and free of charge anti-spoofing service within Galileo that:
  - will **authenticate the Galileo data** using the navigation message
  - will allow to **detect certain spoofing attacks**
  - will be **free of charge** to Galileo Users
- This mechanism provides users with an additional security layer so that to be reassured about the authenticity of the information received from Galileo satellites.
- Initial OS-NMA Signal-in-Space transmission in test mode is on-going in 2021 while service provision phase will start in 2023.
- [OS-NMA infonote](https://www.gsc-europa.eu/electronic-library/programme-reference-documents#OSNMA), ICD and Guidelines for manufacturers available at <https://www.gsc-europa.eu/electronic-library/programme-reference-documents#OSNMA>

# Galileo Navigation Message Authentication (OS NMA)

OS-NMA is based on:

- 1) the publication of **public keys**, to be stored in GNSS receivers, allowing the authentication of the Signal In Space E1 I/NAV data; and
- 2) the transmission of **data to authenticate** the Galileo OS navigation message (e.g. Digital Signatures, Message Authentication Codes and associated Keys) through the E1B I/NAV navigation message



# Overview of OS-NMA Features

CHARACTERISTIC	OSNMA
GNSS RECEIVER MINIMAL CAPABILITIES	Single frequency E1
OBJECT OF AUTHENTICATION	Nav Data (E1B I/Nav and E5b I/Nav and capability for E5a F/Nav if required)
REQUIRED COMPONENTS	E1B
NEED OF RAW GNSS SIGNAL STORAGE AT RECEIVER SIDE	No
NAVIGATION SIGNALS DECRYPTION BY GNSS RECEIVER	No
NEED OF A NETWORK CONNECTION	No <sup>4</sup>
AUTHENTICATION	Clock & Ephemeris Data (CED) and timing parameters (GGTO and UTC), delayed
TIME TO FIRST AUTHENTICATION	One to few minutes
AUTHENTICATION AVAILABILITY	High, expected above 95%
ANTI-TAMPERING FEATURES	Light, as the receiver only stores a public key. To be considered depending on the specific application threats.
OTHER REQUIREMENTS	Time synchronisation <sup>5</sup>





# Project: Blue Box Porbeagle VMS



## Summary

**Contract:** GSA/GRANT/02/2019/Bluebox

**Title:** Shipborne double frequency multi-constellation receiver (E1/E5a)

**Website:** <https://blueporbeagle.eu>

**Implementation period:** 01/01/2021 to 31/12/2022. First tests planned for 2022.

**Goal:** Develop a close-to-market complete shipborne integrated equipment, compliant with regulatory standards for Vessel Monitoring Devices required by EU and countries regulations, and that will disrupt current market solutions through the first use of **anti-spoofing cybersecurity protection technology and improved accuracy with dual frequency, enhancing the fishery VMS with E-GNSS Galileo Open Service (OS), including the navigation message authentication (NMA).**

### Beneficiaries:

- Cooperative of Fishing Vessels' owners of the Port of Vigo (ArVi)
- ArXitEC Critical Systems (Coordinator)





# Project: Asgard



## Summary

**Contract:** GSA/GRANT/02/2019/ASGARD

**Title:** Shipborne double frequency multi-constellation receiver (E1/E5a)

**Website:** <https://asgard.gmv.com/>

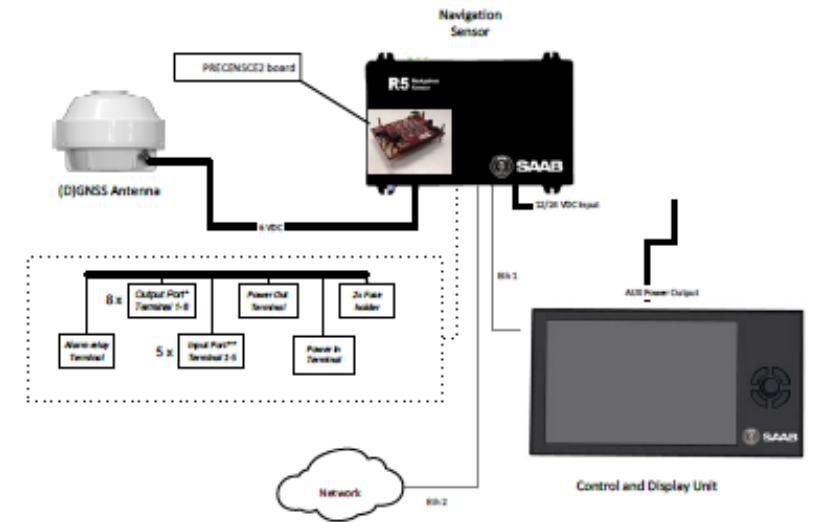
**Implementation period:** 01/01/2021 to 31/12/2022. First tests planned for 2022

**Goal:** Design, development and type approval of a shipborne dual-frequency multiconstellation **shipborne** receiver implementing **OS-NMA authentication**.

**Beneficiaries:**



**SAAB**

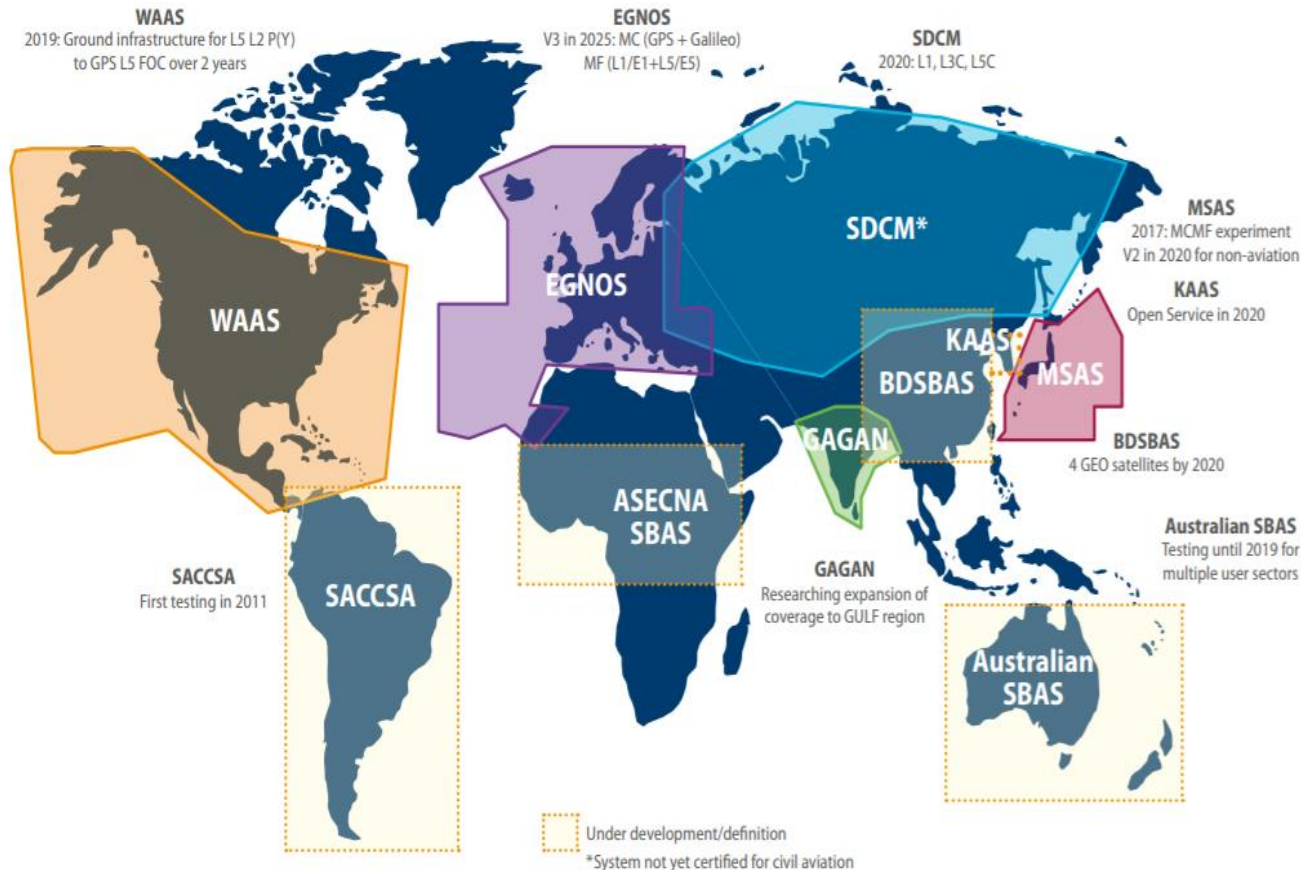


# Outline

- Galileo Open Service – Navigation Message Authentication (**OS-NMA**)
- **SBAS** contribution to integrity

# Satellite-Based Augmentation System (SBAS) worldwide

## SBAS INDICATIVE SERVICE AREAS



**Existing and under definition SBAS systems (Source: GSA User Technology Report 2018)**

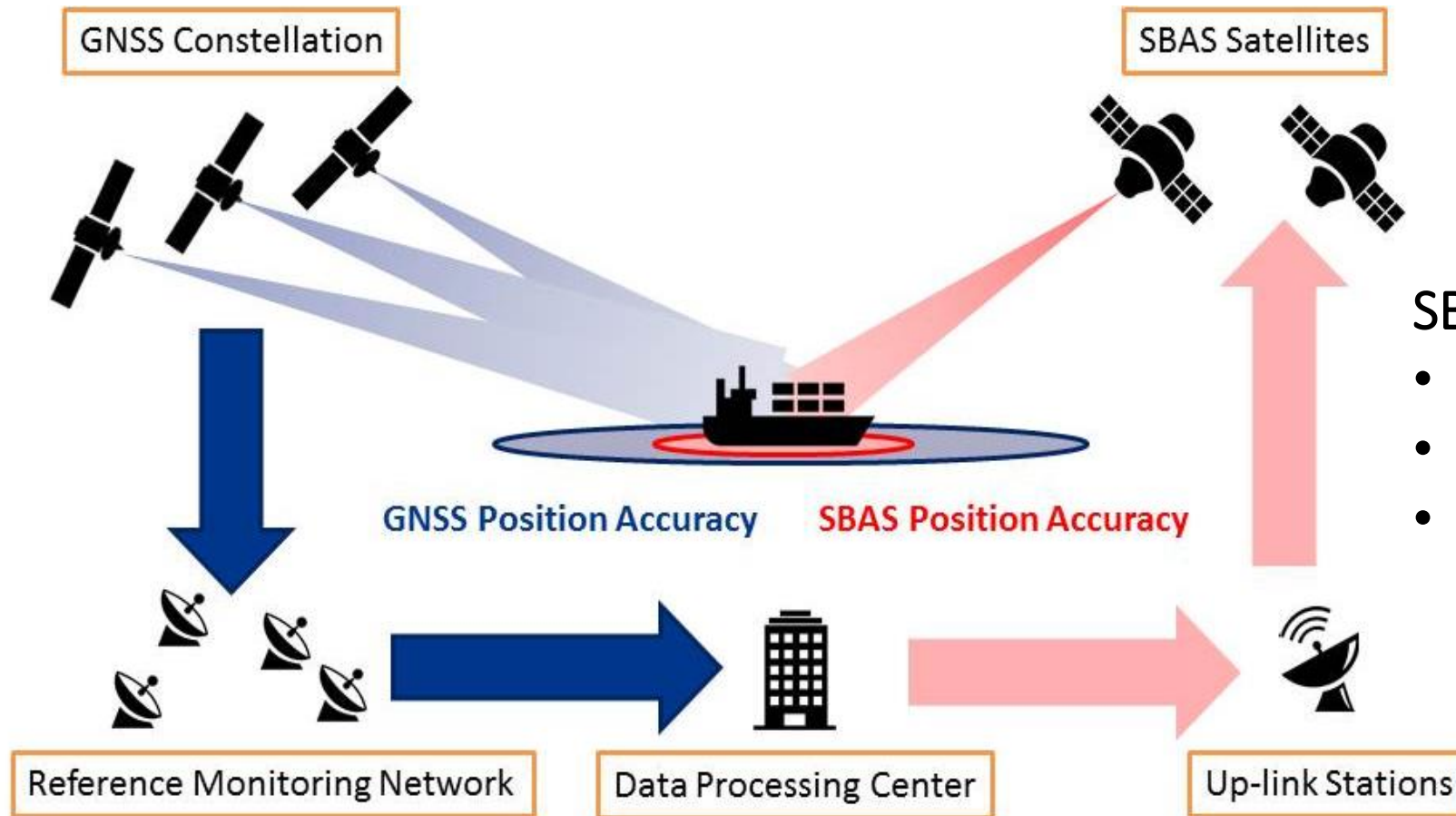
SBAS can be used in two different ways:

- Directly from SiS
- Or retransmitted from a MF Radiobeacon or AIS station

The vessels can benefit from SBAS SiS especially where there is no DGNSS infrastructure (i.e. DGPS/DGLONASS) or in poorly covered environments.

The vessels can use as well SBAS corrections retransmitted by MF Radiobeacons and AIS Stations.

# EGNOS: The European Satellite-Based Augmentation System (SBAS)



SBAS provides:

- Pseudorange corrections
- Satellite, iono & system alerts
- Better accuracy wrt GNSS standalone

# IEC Standardisation for SBAS shipborne receivers



International  
Electrotechnical  
Commission

Standards  
development

Conformity  
assessment

Where we make a  
difference

Who  
benefits

News &  
resources

Programmes  
& initiatives

Who we  
are

[Home](#) / [Standards development](#) / [Technical committees and subcommittees](#) / [TC 80](#) / PT 61108-7

## TC 80 Maritime navigation and radiocommunication equipment and systems

[Scope](#) [Structure](#) [Projects / Publications](#) [Documents](#) [Votes](#) [Meetings](#) [Collaboration Platform](#)

Subcommittee(s) and/or Working Group(s) > [TC 80/PT 61108-7](#)

[en](#) [fr](#)

### PT 61108-7 Project Leader & Members



Project Leader	National Committee
Mr Guillermo Fernandez	ES
Member	National Committee
25 experts appointed from 16 countries	

[https://www.iec.ch/dyn/www/f?p=103:14:516039640385776:::FSP\\_ORG\\_ID:27752](https://www.iec.ch/dyn/www/f?p=103:14:516039640385776:::FSP_ORG_ID:27752)

### Title & Task

## PT 61108-7

Maritime navigation and radiocommunication equipment and systems - Global navigation satellite systems (GNSS) - Part 7: Satellite Based Augmentation Systems - Receiver Equipment - Performance requirements and method of testing

[www.iec.ch](http://www.iec.ch)

# European GNSS enable new applications and resilient Maritime Navigation

## Availability

Enhanced **performance** in challenging environments, thanks to more satellites in view

## Accuracy

Increased **accuracy** thanks to Dual Frequency and High Accuracy Service

## Integrity

## Authentication

Increased **safety and security** thanks to contribution to integrity provided by EGNOS and Galileo Authentication



Contribution to resilient position for vessels monitoring, e.g. fishing and merchant vessels



# Thanks ! Questions ?

Manuel.LopezMartinez@euspa.europa.eu

[www.euspa.europa.eu](http://www.euspa.europa.eu)



The European Union Agency for the Space Programme is hiring!

Apply today and help shape the future of #EUSpace!