The slides present the project submitted by GMV under the GSA Call for proposals GSA/GRANT/02/2019, Shipborne double frequency multi-constellation receiver (E1/E5).

Such project has been awarded by the GSA. However no grant agreement has been signed yet with the GSA and the award does not imply any commitment on the part of the GSA. The project will be implemented only if the grant agreement will be signed with the GSA.
ASGARD

- Founded by GSA (GRANT/02/2019, Fundamental Elements)
- Two years development: 2021-2022.
- **Scope of the project:** design, integration and V&V of a shipborne Dual-frequency Multi-constellation Galileo OS enabled including **OS-NMA authentication** and IEC GNSS approval.
- Consortium: GMV & SAAB.
ASGARD Project activities

• ASGARD shipborne receiver will take benefit of all Galileo OS features (improved performance and robustness thanks to dual-frequency and OS-NMA capabilities), in compliance with the corresponding legal framework for maritime equipment at both EU and IMO level.

• A set of activities will also be carried out in the frame of the project to test and demonstrate the capabilities of the product, enabling the dissemination and business plan activities required to maximize the penetration of shipborne Galileo receivers in the corresponding market.
Objectives of ASGARD

1. Development of a **double-frequency** (E1/E5a) shipborne **multi-constellation** Galileo OS & GPS shipborne receiver compliant with IMO resolutions **MSC.401**, **MSC.432** and **MSC.233**.

2. **Type approval** for Galileo receiver following **IEC standard 61108-3**.

3. Implement the algorithms to use the **OS-NMA** to support Resilient-PNT in maritime navigation, following GSA specifications.
Objective 1: Development of DFMC Galileo shipborne receiver

- Design and integration of the shipborne receiver, starting point:
  - SAAB R5 Navigation System
  - GMV PRESENCE2 GNSS OEM receiver
Objective 1: Development of DFMC Galileo shipborne receiver (Cont.)

• Main drivers of ASGARD shipborne receiver design
  – Take benefit of Galileo OS features (improved performance, dual-frequency capabilities) and also of Galileo OS-NMA to support resilient PNT
  – Aligned with maritime standards and applicable EU regulation (MED): TRL-7 project target
  – Compliant with IMO resolutions MSC.401, MSC.432 (Multi-system shipborne radionavigation receivers)
    – Two independent GNSS recognised by IMO (WWRNS): Galileo + GPS
    – Dual frequency in L1/L5 and E1/E5a
    – Compliant with IEC 61108-1 and IEC 61108-3 specifications (includes DGNSS augmentation, RAIM)
Objective 2: Type approval IEC 61108-3

- Static and dynamic laboratory test campaign in the laboratory following IEC 61108-3 (Galileo) and IEC-61108-1 (GPS): Type approval.
- Planned dynamic test campaign on a vessel
Objective 2: TRL-7 & 61108-X vs MED

<table>
<thead>
<tr>
<th>IMO</th>
<th>IEC</th>
<th>Description</th>
<th>MED</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSC 112 (73)</td>
<td>61108-1</td>
<td>GPS receiver equipment: performance standards, methods of testing and required test results.</td>
<td>Into 4.14</td>
</tr>
<tr>
<td>MSC 233</td>
<td>61108-3</td>
<td>Galileo receiver equipment: performance requirements, methods of testing and required test results</td>
<td>Into 4.56</td>
</tr>
<tr>
<td>MSC 401 (95)</td>
<td></td>
<td>Performance standards for multi-system shipborne radionavigation receivers</td>
<td></td>
</tr>
<tr>
<td>MSC 432</td>
<td></td>
<td>Amendment to MSC 401</td>
<td></td>
</tr>
</tbody>
</table>

### MED European WheelMark

**Type approval requirements & methods of testing and performance requirements**

- **SOLED 4 Reg V18**: EN 60945-2002, IEC 60945
- **SOLED 4 Reg V/X**: EN 60945-2002, IEC 60945
- **SOLED 4 Reg V19**: EN 60945-2002, IEC 60945

**Testing standards**

- **Mandatory**: Required tests at very different level: electromagnetic radiation and immunity, power supply, environment (temperature, vibration, rain, corrosion, others).
- **High Speed Craft**: Required tests at a level of information to crew
- **Galileo maritime receivers**: Required tests at a level of information to crew

**IEC Formal laboratory testing**

- **MSC 112 (73)**: IEC 60945-2002, IEC 60945
- **MSC 233 (95)**: IEC 60945-2002, IEC 60945

**IMO Performance requirements**

- **MSC 112 (73)**: EN 60945-2002, IEC 60945
- **MSC 233 (95)**: EN 60945-2002, IEC 60945
Objective 3: Galileo OS-NMA implementation

• First, what Galileo OS-NMA is NOT:
  – A checksum to validate navigation data integrity
  – Secret encryption of Navigation signal “for your eyes only” (i.e.:PRS)

• OS-NMA verifies the **authenticity** of the Galileo navigation message
  – To confirm the message received has been **transmitted by Galileo** OS System.
  – High level of **robustness** against simplistic and intermediate **spoofing/meaconing** attacks.

• Tests campaign in the **laboratory**, including a spoofing attack.
Objective 3: Galileo OS-NMA implementation - system level point of view

- NMA MACs are generated using **symmetric key encryption**, being the symmetric key disclosed **AFTER** the navigation message has been signed and broadcast. Such keys belong to a **TESLA chain**, in which each key can be used to derive a previous one.

- The **TESLA root key** is signed with an **asymmetric signature**. The public key involved in the TESLA root key validation can be obtained either from the OS SIS (verification required) or from the European GNSS Service Centre.

- If the locally computed MAC matches the broadcast one, the navigation message is considered to be authentic.
Objective 3: Galileo OS-NMA implementation - user level point of view

• By using reserved fields of the I/NAV, OS-NMA broadcast does not introduce extra overhead to the system. Standard OS receivers can ignore the dedicated NMA fields and keep functioning with the same level of performance (fully backwards compatibility).

• As showed in the figure on the right, an OS-NMA capable receiver differs from a generic OS receiver only by the additional firmware/software required to:
  – Retrieve the OS-NMA related fields from the navigation message;
  – Locally compute the MAC corresponding to a particular navigation message (using the information provided by the NMA field) to confirm whether this is authentic, matching in this case the broadcast one.
Thank you

Q&A
Linking space to user needs

How to get in touch:

European Global Navigation Satellite Systems Agency

www.GSA.europa.eu

EGNOS-portal.eu

GSC-europa.eu

UseGalileo.eu

The European GNSS Agency is hiring!

Apply today and help shape the future of satellite navigation!